Chapter 4

Local Properties

In the preceeding chapters, we developed the geometry-algebra dictionary from a global point of view, focusing on geometric questions which concern a given algebraic set A as a whole. Accordingly, we studied functions defined on all of A, the polynomial functions on A, and used the ring $\Bbbk[A]$ formed by these functions to express geometric properties of A in ring theoretic terms. Algorithmically, we computed Gröbner bases with respect to what we called global monomial orders.

In this chapter, we will be interested in geometric properties which are local in the sense that they reflect the behavior of A near a given point $p \in A$. In defining the basic local property, which is smoothness, we will rely on the concept of the tangent space. Intuitively, p is a smooth point of A if the tangent space T_pA approximates A near p (otherwise, we will say that p is a singular point of A). Here, we will define T_pA over any field in a purely algebraic way (no limiting process as in calculus is needed). We will show that the singular points form an algebraic subset of A, and we will prove the Jacobian criterion which, in many cases of interest, allows one to compute the equations of this subset, and to check whether the given polynomials defining A actually generate a radical ideal.

We will, then, describe the construction of the local ring $\mathcal{O}_{A,p}$ whose elements are germs of functions defined on Zariski open neighborhoods of p in A. It will turn out that A is smooth at p iff $\mathcal{O}_{A,p}$ is a regular local ring. Focusing on the general and purely algebraic nature of the construction of $\mathcal{O}_{A,p}$, we will be lead to the concept of localization which plays an important role in commutative algebra. In fact, localization often allows one to reduce problems concerning arbitrary rings to problems concerning local rings which are much easier. One reason why local rings are easier to handle than arbitrary rings is Nakayama's lemma. As a typical application of this lemma, we prove a special case of Krull's intersection theorem.

Returning to more geometric questions, we will use the local ring $\mathcal{O}_{\mathbb{A}^2,p}$ to define the intersection multiplicity of two plane curves at a point $p \in \mathbb{A}^2$.

Making, thus, preperations for the treatment of Bezout's theorem in Chapter 5, we will verify a number of properties of intersection multiplicities.

Algorithmically, the computation of the multiplicities is based on a version of Buchberger's algorithm for computing Gröbner bases with respect to what we will call local monomial orders.

Motivated by rationality problems which may arise in such computations, we will give an alternative definition of the multiplicities using the notion of modules of finite length. Discussing this notion, we will show that a ring R has finite length iff it is Artinian, that is, R satisfies the *descending* chain condition. Applying this fact in a localized situation (which will allow us to benefit from Nakayama'a lemma), we will prove Krull's principal ideal theorem.

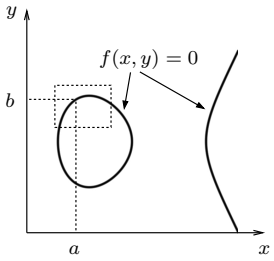
In the final section, we will treat the completion $\widehat{\mathcal{O}_{A,p}}$ of $\mathcal{O}_{A,p}$. This will help us to overcome a drawback of $\mathcal{O}_{A,p}$ which is due to the fact that Zariski open sets are rather large. Since $\mathcal{O}_{A,p}$ consists of (germs of) functions defined on such sets, it carries information on too much of A. In contrast, the larger ring $\widehat{\mathcal{O}_{A,p}}$ carries far more local information. Another topic, which we will treat briefly, is the tangent cone TC_pA which approximates A near p even if p is a singular point of A.

4.1 Smoothness

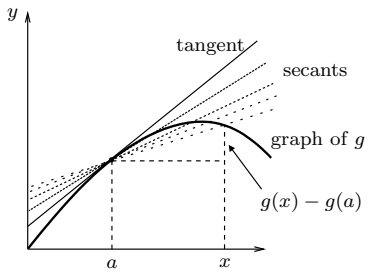
We will define smoothness such that in case $\mathbb{K} = \mathbb{C}$, an algebraic set $A \subset \mathbb{A}^n$ is smooth at a point $p \in A$ iff A is a complex submanifold of $\mathbb{A}^n$ in an Euclidean neighborhood of p. Equivalently, we will require that the hypothesis of the implicit function theorem is fulfilled. In making this precise, we will first study the hypersurface case, which is intuitively easy to understand, and where important consequences of the definition are easy to prove.

We fix our ideas by illustrating the special case of a plane curve. Let $f \in \mathbb{C}[x, y]$ be a nonconstant square-free polynomial, let $C = \mathrm{V}(f) \subset \mathbb{A}^2(\mathbb{C})$ be the corresponding curve, and let $p = (a, b) \in C$ be a point. In this situation, the complex variable version of the implicit function theorem asserts that if the gradient $\left(\frac{\partial f}{\partial x}(p), \frac{\partial f}{\partial y}(p)\right)$ is nonzero, then there is an Euclidean neighborhood of p in which C can be exhibited as the graph of a holomorphic function. Supposing, say, that $\frac{\partial f}{\partial y}(p) \neq 0$, the precise statement is that there are open neighbourhoods U_1 of a and U_2 of b in the Euclidean topology and a holomorphic function $g : U_1 \to U_2$ such that $g(a) = b$ and

$$C \cap (U_1 \times U_2) = \{(x, g(x)) \mid x \in U_1\}.$$



Reflecting this fact, we get a well defined tangent line to C at p (the linear approximation of C near p) by interpreting the existence of the differential quotient of g at $x = a$ geometrically – the tangent line is the limiting position of secant lines to C passing through p:



Since

$$g'(a) = -\frac{\partial f}{\partial x}(p)/\frac{\partial f}{\partial y}(p)$$

by the chain rule, we may rewrite the equation $y = b + g'(a)(x - a)$ of the tangent line in terms of f:

$$\frac{\partial f}{\partial x}(p)(x - a) + \frac{\partial f}{\partial y}(p)(y - b) = 0. \tag{4.1}$$

There is no algebraic geometry analogue of the implicit function theorem: Even though we are concerned with a *polynomial* f in our considerations, it is usually not possible to choose the U_i as neighborhoods in the Zariski topology and g as a polynomial function. From a topological point of view, as illustrated by the example in the following picture, the Zariski open sets are simply too big:

On the other hand, using formal partial derivatives, equation (4.1) makes sense even in case $\mathbb{K} \neq \mathbb{C}$. We, therefore, define:

Remark-Definition 4.1.1. 1. If $f \in \mathbb{K}[x_1, \ldots, x_n]$ is a polynomial, and $p = (a_1, \ldots, a_n) \in \mathbb{A}^n$ is a point, the **differential of f at p**, written $d_p f$, is defined to be

$$d_p f = \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(p)(x_i - a_i) \in \mathbb{K}[x_1, \ldots, x_n].$$

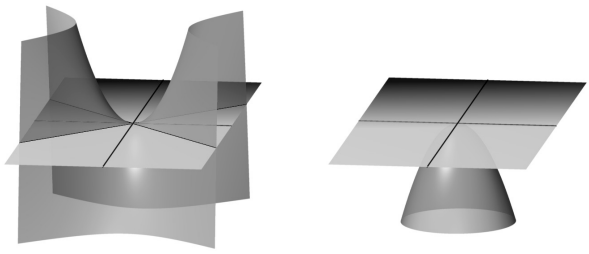
That is, $d_p f$ is the linear part of the Taylor expansion of f at p:

$$f = f(p) + d_p f + \text{terms of degree} \geq 2 \text{ in the } x_i - a_i.$$

2. Let $A \subset \mathbb{A}^n$ be a hypersurface, let $p \in A$ be a point, and let $f \in \mathbb{K}[x_1, \ldots, x_n]$ be a generator for $\mathrm{I}(A)$. Then the **tangent space to A at p**, denoted $T_p A$, is the linear subvariety

$$T_p A = \mathrm{V}(d_p f) \subset \mathbb{A}^n.$$

We say that p is a **smooth** (or a **nonsingular**) **point** of A if $T_p A$ is a hyperplane, that is, if $d_p f$ is nonzero.



Otherwise, $T_p A = \mathbb{A}^n$, and we call p a **singular point** of A. □

Example 4.1.2. The origin $o = (0, 0) \in \mathbb{A}^2(\mathbb{C})$ is a singular point of each cubic curve shown below:

$y^2 = x^3 + x^2$ $y^2 = x^3$ $y^2 = xy + x^2y - x^3$ □

The tangent space T_pA is the union of all lines meeting A with multiplicity at least 2 at p:

Proposition 4.1.3. *Let $A \subset \mathbb{A}^n$ be a hypersurface, and let $\mathrm{I}(A) = \langle f \rangle$.*

1. *Let $p = (a_1, \dots, a_n) \in A$ be a point, and let $L \subset \mathbb{A}^n$ be a line through p, given by the parametric equations $x_i = a_i + tv_i$, $i = 1, \dots, n$, where $v = (v_1, \dots, v_n) \in \mathbb{A}^n$ is a direction vector of L. Then $L \subset T_pA$ iff the polynomial $F(t) := f(p + tv) \in \mathbb{K}[t]$ vanishes with multiplicity ≥ 2 at 0.*
2. *The set A_{sing} of singular points of A is a proper algebraic subset of A:*

$$A_{\mathrm{sing}} = \mathrm{V}(f, \frac{\partial f}{\partial x_1}, \dots, \frac{\partial f}{\partial x_n}) \subsetneq A.$$

Proof. 1. The result follows from the chain rule: $\frac{\partial F}{\partial t}(0) = \sum_{i=1}^n v_i \frac{\partial f}{\partial x_i}(p)$.

2. That $A_{\mathrm{sing}} = \mathrm{V}(f, \frac{\partial f}{\partial x_1}, \dots, \frac{\partial f}{\partial x_n})$ is clear from our definitions. In particular, A_{sing} is an algebraic subset of A. To show that A_{sing} is properly contained in A, suppose the contrary. Then, for all i, the partial derivative $\frac{\partial f}{\partial x_i}$ is contained in $\langle f \rangle$, so that $\frac{\partial f}{\partial x_i} = 0$ by degree reasoning. If $\mathrm{char}\,\mathbb{K} = 0$, this implies that f is constant, contradicting our assumption that A is a hypersurface. If $\mathrm{char}\,\mathbb{K} = p > 0$, we must have $f \in \mathbb{K}[x_1^p, \dots, x_n^p]$ (see Exercise 1.1.3). As in the proof of Proposition 3.5.1, we conclude that f has a pth root in $\mathbb{K}[x_1, \dots, x_n]$. This contradicts the fact that $\mathrm{I}(A) = \langle f \rangle$ is a radical ideal. □

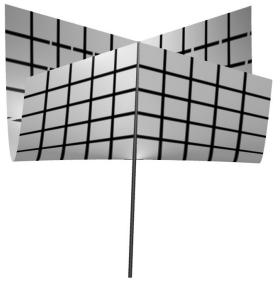
Example 4.1.4. The set of singular points of the Whitney umbrella

$$\mathrm{V}(x^2 - y^2 z) \subset \mathbb{A}^3(\mathbb{C})$$

is the z-axis

$$\mathrm{V}(x^2 - y^2 z, 2x, -2yz, -y^2) = \mathrm{V}(x, y).$$

We show a real picture:



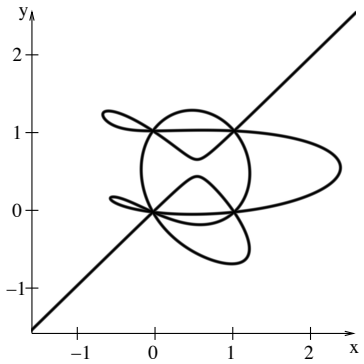
□

Exercise 4.1.5. 1. Find all singular points of the curve

$$\mathrm{V}(x^2 - 2x^3 + x^4 + y^2 - 2y^3 + y^4 - \frac{3}{2}x^2y^2) \subset \mathbb{A}^2(\mathbb{C}).$$

Draw a picture of the real points of this curve.

2. Find all singular points of the curve $\mathrm{V}(f) \subset \mathbb{A}^2(\mathbb{C})$, where f is the degree-7 polynomial considered in Example 1.2.4, part 3.



□

We, now, turn from hypersurfaces to arbitary algebraic sets:

Definition 4.1.6. Let $A \subset \mathbb{A}^n$ be an algebraic set, and let $p \in A$ be a point. The **tangent space** to A at p, denoted T_pA, is the linear subvariety

$$T_pA = \mathrm{V}(d_pf \mid f \in \mathrm{I}(A)) \subset \mathbb{A}^n.$$

□

As in Proposition 4.1.3, a line $L = \{p + tv \mid t \in \mathbb{K}\}$ is contained in T_pA iff all polynomials $f(p + tv) \in \mathbb{K}[t]$, $f \in \mathrm{I}(A)$, vanish with multiplicity ≥ 2 at 0.

Remark 4.1.7. 1. In defining the tangent space, it suffices to consider a set of generators for the vanishing ideal of A: if $\mathrm{I}(A) = \langle f_1, \ldots, f_r \rangle$, then

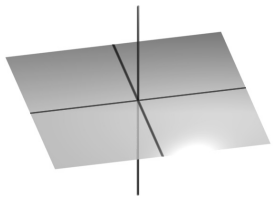
$$T_pA = \mathrm{V}(d_pf_i \mid i = 1, \ldots, r) \subset \mathbb{A}^n.$$

In particular,

$$\dim_{\mathbb{K}} T_pA = n - \operatorname{rank}\left(\frac{\partial f_i}{\partial x_j}(p)\right).$$

2. The function
$$A \to \mathbb{N},\ p \mapsto \dim T_p A,$$
is upper semicontinous in the Zariski topology on A. That is, for any integer k, the subset
$$\{p \in A \mid \dim_{\mathbb{K}} T_p A \geq k\} \subset A$$
is Zariski closed. Indeed, this subset is the intersection of A with the locus of zeros of the $(n-k+1) \times (n-k+1)$ minors of the **Jacobian matrix** $\left(\frac{\partial f_i}{\partial x_j}\right)$. □

Example 4.1.8. Let $A = \mathrm{V}(xz, yz) = \mathrm{V}(x, y) \cup \mathrm{V}(z) =: L \cup P \subset \mathbb{A}^3$ be the union of the z-axis and the xy-plane:



If $o = (0, 0, 0) \in \mathbb{A}^3$ is the origin, and $p \in A$ is any point, then $\dim T_p A = 1$ if $p \in L \setminus \{o\}$, $\dim T_p A = 2$ if $p \in P \setminus \{o\}$, and $\dim T_p A = 3$ if $p = o$. □

According to our definition, a hypersurface $A \subset \mathbb{A}^n$ is smooth at a point $p \in A$ if the dimension of A equals the dimension of the tangent space $T_p A$. In extending this definition to an arbitrary algebraic set A, we have to take into account that, in contrast to the hypersurface case, A may have irreducible components of different dimension. On the other hand, the behavior of A near $p \in A$ is only effected by those components passing through p.

Definition 4.1.9. Let $A \subset \mathbb{A}^n$ be an algebraic set, and let $p \in A$ be a point. The **local dimension of A at p**, written $\dim_p A$, is the maximum dimension of an irreducible component of A containing p. □

We always have
$$\dim_{\mathbb{K}} T_p A \geq \dim_p A. \tag{4.2}$$
In contrast to the hypersurface case, however, the result for arbitrary algebraic sets is not immediately clear from the definitions. We will prove it in a more general algebraic setting in Corollary 4.6.20 as a consequence of Krull's principal ideal theorem.

Definition 4.1.10. Let $A \subset \mathbb{A}^n$ be algebraic.

1. We say that $A \subset \mathbb{A}^n$ is **smooth** (or **nonsingular**) **at $p \in A$** if
$$\dim_{\mathbb{K}} T_p A = \dim_p A.$$

We, then, refer to p as a **smooth** (or a **nonsingular**) **point** of A. Otherwise, we say that A is **singular at p**, that p is a **singular point** of A, or that p is a **singularity** of A.

2. The set A_{sing} of singular points of A is called the **singular locus** of A. If A_{sing} is empty, that is, if A is smooth at each of its points, then A is called **smooth**. □

Remark 4.1.11. Let $A \subset \mathbb{A}^n$ be an algebraic set.

1. If A is smooth at p, then p is contained in a single component of A. In fact, if $A = V_1 \cup \cdots \cup V_s$ is the decomposition of A into its irreducible components, then

$$A_{\text{sing}} = \bigcup_{i \neq j} (V_i \cap V_j) \cup \bigcup_i (V_i)_{\text{sing}}$$

(we will establish this in Corollary 4.6.26). In particular, A_{sing} is an algebraic subset of A since this is true in the case where A is irreducible. Indeed, in this case, $\dim_p A = \dim A$ for all $p \in A$, and we may apply part 2 of Remark 4.1.7, with $k = \dim A + 1$.

2. The singular locus A_{sing} and A have no irreducible component in common. That is, for any irreducible component V_i of A, we have $A_{\text{sing}} \cap V_i \subsetneq V_i$. Using Theorem 3.5.2 and the formula in part 1 above, we will deduce this fact in Corollary 4.2.16 from the hypersurface case. □

If generators $f_1, \ldots, f_r$ for the vanishing ideal $\mathrm{I}(A)$ are given, and the local dimension $\dim_p A$ is known to us, we can decide whether A is smooth at p by computing $\dim_{\mathbb{K}} T_p A = n - \operatorname{rank}\left(\frac{\partial f_i}{\partial x_j}(p)\right)$, and comparing this number with $\dim_p A$. The Jacobian criterion, which we treat next, often allows one to test smoothness without having to check a priori that the given polynomials $f_1, \ldots, f_r$ defining A actually generate $\mathrm{I}(A)$. In fact, under the assumptions of the corollary to the Jacobian criterion stated below, this will follow a posteriori. In this way, the corollary gives a powerful method for establishing that $f_1, \ldots, f_r$ generate a radical ideal.

Theorem 4.1.12 (Jacobian Criterion). *Let $A \subset \mathbb{A}^n$ be an algebraic subset, let $p \in A$ a point, and let $f_1, \ldots, f_r \in \mathrm{I}(A)$. Then*

$$n - \operatorname{rank}\left(\frac{\partial f_i}{\partial x_j}(p)\right) \geq \dim_p A.$$

If equality holds, then A is smooth at p.

Proof. This follows from the chain of inequalities

$$n - \operatorname{rank}\left(\frac{\partial f_i}{\partial x_j}(p)\right) \geq \dim_{\mathbb{K}} T_p A \geq \dim_p A.$$

□

Corollary 4.1.13. *Let $I = \langle f_1, \ldots, f_r \rangle \subset \Bbbk[x_1, \ldots, x_n]$ be an ideal such that $A = \mathrm{V}(I) \subset \mathbb{A}^n$ is equidimensional of dimension d, and let $I_{n-d}\left(\frac{\partial f_i}{\partial x_j}\right)$ denote the ideal generated by the $(n-d) \times (n-d)$ minors of the Jacobian matrix of the f_i. If $I_{n-d}\left(\frac{\partial f_i}{\partial x_j}\right) + I = \langle 1 \rangle$, then A is smooth and $I\,\mathbb{K}[x_1, \ldots x_n] = \mathrm{I}(A)$. In particular, I is a radical ideal.*

Proof. The subset $\mathrm{V}(I_{n-d}\left(\frac{\partial f_i}{\partial x_j}\right)+I) = \{p \in A \mid n - \operatorname{rank}\left(\frac{\partial f_i}{\partial x_j}(p)\right) > d\} \subset A$ is empty by the assumption on $I_{n-d}\left(\frac{\partial f_i}{\partial x_j}\right) + I$ and Hilbert's Nullstellensatz. Since each irreducible component of A has dimension d, the Jacobian criterion implies that A is smooth. That $I\,\mathbb{K}[x_1, \dots x_n] = \mathrm{I}(A)$ will be established towards the end of Section 4.6. □

Under a stronger assumption, the Jacobian criterion can also be applied if $1 \notin I_{n-d}\left(\frac{\partial f_i}{\partial x_j}\right) + I$:

Corollary 4.1.14. *Let $I = \langle f_1, \dots, f_r\rangle \subset \Bbbk[x_1, \dots, x_n]$ be an ideal of dimension d, and let $A = \mathrm{V}(I) \subset \mathbb{A}^n$. Suppose that $\Bbbk[x_1, \dots, x_n]/I$ is Cohen-Macaulay (by the Unmixedness Theorem 3.3.12, this implies that A is equidimensional of dimension d). With notation as in Corollary 4.1.13, if*

$$\dim \mathrm{V}(I_{n-d}\left(\frac{\partial f_i}{\partial x_j}\right) + I) < \dim \mathrm{V}(I) = d,$$

then $I\,\mathbb{K}[x_1, \dots x_n] = \mathrm{I}(A)$ and $\mathrm{V}(I_{n-d}\left(\frac{\partial f_i}{\partial x_j}\right) + I) = A_{\mathrm{sing}}$. In particular, I is a radical ideal.

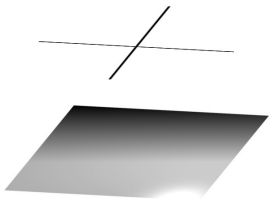
Proof. This will also be established towards the end of Section 4.6. □

The following example shows that the assumption of equidimensionality in Corollary 4.1.13 is really needed:

Example 4.1.15. Let $I = \langle f_1, f_2\rangle \subset \Bbbk[x_1, x_2, x_3]$ be the ideal generated by $f_1 = x_1^2 - x_1$ and $f_2 = x_1x_2x_3$. Buchberger's criterion shows that f_1, f_2 form a lexicographic Gröbner basis for I. By Proposition 3.3.3, the composition $\Bbbk[x_2, x_3] \subset \Bbbk[x_1, x_2, x_3] \to \Bbbk[x_1, x_2, x_3]/I$ is a Noether normalization, so that

$$d = \dim \Bbbk[x_1, x_2, x_3]/I = 2.$$

Though $1 = (2x_1 - 1)\frac{\partial f_1}{\partial x_1} - 4f_1 \in I_1(\frac{\partial f_i}{\partial x_j}) + I$, however, $A = \mathrm{V}(I) \subset \mathbb{A}^3$ is not smooth. In fact, $A = \mathrm{V}(x_1) \cup \mathrm{V}(x_1 - 1, x_2x_3)$ is the union of a plane and a pair of lines intersecting in a point which is necessarily a singular point of A.



□

Exercise 4.1.16. Consider the matrix

$$D = \begin{pmatrix} x_1 & x_2 & x_3^2 - 1 \\ x_2 & x_3 & x_1x_2 + x_3 + 1 \\ x_3^2 - 1 & x_1x_2 + x_3 + 1 & 0 \end{pmatrix}$$

and the ideal $I = \langle f_1, f_2 \rangle \subset \Bbbk[x_1, x_2, x_3]$ generated by $f_1 = \det D$ and the "first" 2×2 minor $f_2 = x_1x_3 - x_2^2$ of D. Verify by computation:

1. The algebraic set $A = \mathrm{V}(I) \subset \mathbb{A}^3$ is equidimensional of dimension $d = 1$.
2. The zero locus of the ideal $J = I_2(\frac{\partial f_i}{\partial x_j}) + I$ coincides with that of I. That is, $\mathrm{V}(J) = \mathrm{V}(I) = A$.
3. The vanishing ideal $\mathrm{I}(A) = (I : J)\,\mathbb{K}[x_1, x_2, x_3]$.
4. A is smooth.

The geometric interpretation of this is that the two hypersurfaces $\mathrm{V}(f_1)$ and $\mathrm{V}(f_2)$ touch each other along A.

Fig. 4.1. *The cone $V(f_2)$ (dark surface) together with $V(f_1)$ (bright surface) and their intersection (white curve).*

□

Definition 4.1.6 treats the tangent space T_pA *externally*, that is, as a subspace of the ambient space $\mathbb{A}^n$. Hence, it is not obvious that under an isomorphism $\varphi : A \to B$ the tangent spaces at p and $\varphi(p)$ are isomorphic. To prove this, we give an *intrinsic* description of T_pA which only depends on the coordinate ring $\mathbb{K}[A]$.

We consider $T_p\mathbb{A}^n = \mathbb{A}^n$ as an abstract vector space with origin p and coordinates $X_i = x_i - a_i$, $i = 1, \ldots, n$. Then $T_pA = \mathrm{V}(d_pf \mid f \in \mathrm{I}(A)) \subset T_p\mathbb{A}^n$ is a linear subspace. Indeed, for each $f \in \mathbb{K}[x_1, \ldots, x_n]$, the differential d_pf is linear in the $x_i - a_i$. Moreover, the restriction of d_pf to T_pA depends only on the residue class $\overline{f} = f + \mathrm{I}(A)$ of f in $\mathbb{K}[A]$. We, thus, obtain a well-defined linear map

$$d_p : \mathbb{K}[A] \to T_p^*A,\ \overline{f} \mapsto d_pf|T_pA,$$

where $T_p^*A = \mathrm{Hom}(T_pA, \mathbb{K})$ is the dual vector space of T_pA. The map d_p is surjective since the d_pX_i form a basis for the dual vector space of $T_p\mathbb{A}^n$ and every linear form on T_pA is induced by a linear form on $T_p\mathbb{A}^n$. To describe T_p^*A and, thus, $T_pA = (T_p^*A)^*$ in terms of $\mathbb{K}[A]$, we need to identify the kernel

of d_p. Since $d_p c = 0$ for each constant $c \in \mathbb{K}$, the map d_p is determined by its values on the maximal ideal

$$\mathrm{I}_A(p) := \mathrm{I}_A(\{p\}) = \{\overline{f} \in \mathbb{K}[A] \mid f(p) = 0\} \subset \mathbb{K}[A]$$

corresponding to p. We may, thus, as well study the restricted map

$$d_p : \mathrm{I}_A(p) \to T_p^* A,\ \overline{f} \mapsto d_p f | T_p A.$$

This map vanishes on the second power of $\mathrm{I}_A(p)$ (the terms of degree ≥ 2 in the Taylor expansion of f at p do not contribute to $d_p f$). In fact, we have the following result (the final version of this result, proved in Section 4.2, will lead us to the definition of the Zariski tangent space):

Theorem 4.1.17 (Zariski Tangent Space, Preliminary Version). *Let $A \subset \mathbb{A}^n$ be an algebraic set, and let $p \in A$ be a point. The $\mathbb{K}[A]$-module $\mathrm{I}_A(p)/\mathrm{I}_A^2(p)$ is naturally a $\mathbb{K}$-vector space. Moreover, the map d_p defines an isomorphism*

$$\mathrm{I}_A(p)/\mathrm{I}_A^2(p) \cong T_p^* A$$

of $\mathbb{K}$-vector spaces.

Proof. Since the $\mathbb{K}[A]$-module $\mathrm{I}_A(p)/\mathrm{I}_A^2(p)$ is annihilated by $\mathrm{I}_A(p)$, it is naturally a $\mathbb{K}[A]/\mathrm{I}_A(p)$-module. The first assertion follows since $\mathbb{K}[A]/\mathrm{I}_A(p) \cong \mathbb{K}$, where the isomorphism is defined by evaluating polynomial functions at p. To prove the theorem, it remains to show that $\ker d_p \subset \mathrm{I}_A^2(p)$. Let $\overline{f} \in \ker d_p$. That is, $\overline{f} \in \mathrm{I}_A(p)$ and $d_p f | T_p A = 0$. Then, if $f_1, \ldots, f_r$ are generators for $\mathrm{I}(A)$, the differential $d_p f$ is a $\mathbb{K}$-linear combination of the $d_p f_i$:

$$d_p f = \sum_{i=1}^{r} \lambda_i d_p f_i.$$

Set $g = f - \sum_{i=1}^{r} \lambda_i f_i$. Then $g(p) = 0$ and $d_p g = 0$. We conclude that $g \in \mathrm{I}^2(p) \subset \mathbb{K}[x_1, \ldots, x_n]$, so that $\overline{f} = \overline{g} \in \mathrm{I}_A^2(p) \subset \mathbb{K}[A]$. □

Let, now, $\varphi : A \to B$ be a morphism of affine algebraic sets, let $\varphi^* : \mathbb{K}[B] \to \mathbb{K}[A]$ be the induced map, let $p \in A$ be a point, and let $q = \varphi(p)$. Then

$$\varphi^*(\mathrm{I}_B(q)) \subset \mathrm{I}_A(p) \ \text{ and } \ \varphi^*(\mathrm{I}_B^2(q)) \subset \mathrm{I}_A^2(p).$$

Thus, φ defines a map $\varphi^* : \mathrm{I}_B(q)/\mathrm{I}_B^2(q) \to \mathrm{I}_A(p)/\mathrm{I}_A^2(p)$. The dual map

$$d_p\varphi : T_p A \cong (\mathrm{I}_A(p)/\mathrm{I}_A^2(p))^* \to (\mathrm{I}_B(q)/\mathrm{I}_B^2(q))^* \cong T_q B$$

is called the **differential** of φ at p. Note that if $\psi : B \to C$ is another morphism of affine algebraic sets, then

$$d_p(\psi \circ \varphi) = \mathrm{d}_{\varphi(p)}\, \psi \circ d_p \varphi.$$

Furthermore,

$$d_p(\mathrm{id}_A) = \mathrm{id}_{T_pA}.$$

These observations show that the tangent space is invariant under isomorphims:

Corollary 4.1.18. *If $\varphi : A \to B$ is an isomorphism of affine algebraic sets and $p \in A$ is a point, then*

$$d_p\varphi : T_pA \to T_{\varphi(p)}B$$

is an isomorphism of $\mathbb{K}$-vector spaces. □

4.2 Local Rings

In this section, given an algebraic set A and a point $p \in A$, we will describe the construction of the local ring $\mathcal{O}_{A,p}$. This ring is the basic invariant of A at p. We will use it to express smoothness in algebraic terms.

The elements of $\mathcal{O}_{A,p}$ are functions defined on A "near" p. More precisely, the functions are defined on Zariski open neighborhoods of p in A, and two such functions will be identified if they coincide on a sufficiently small neighborhood of p on which both functions are defined. In this sense, the elements of $\mathcal{O}_{A,p}$ are actually **germs of functions**.

What functions are allowed in the construction of $\mathcal{O}_{A,p}$? Since every Zariski neighborhood of p in A contains an open neighborhood of type $\mathrm{D}_A(f) = A \setminus \mathrm{V}_A(f)$, where $f \in \mathbb{K}[A]$ is not vanishing at p, we can restrict ourselves to describe the admissible functions on a neighborhood of this type. Now, note that on $\mathrm{D}_A(f)$, the function f and, thus, its powers f^m are invertible. It is therefore natural to associate to $\mathrm{D}_A(f)$ the $\mathbb{K}$-algebra $\mathbb{K}[A]_f$ of functions on $\mathrm{D}_A(f)$ obtained by adjoining $1/f$ to $\mathbb{K}[A]$. The elements of $\mathrm{D}_A(f)$ are, then, fractions of type g/f^m, where $g \in \mathbb{K}[A]$ and $m \geq 0$. Two such fractions g/f^m and $g'/f^{m'}$ define the same function on $\mathrm{D}_A(f)$ iff $gf^{m'} - g'f^m = 0$ as functions on $\mathrm{D}_A(f)$. Equivalently, $f(gf^{m'} - g'f^m) = 0$ on all of A. That is, $f(gf^{m'} - g'f^m) = 0 \in \mathbb{K}[A]$.

The desired local ring $\mathcal{O}_{A,p}$ is obtained by inverting all the functions in $\mathbb{K}[A]$ not vanishing at p. Its elements are fractions of type g/h, where $g, h \in \mathbb{K}[A]$, with $h(p) \neq 0$. Here, two such fractions g/h and g'/h' will be identified if $gh' - g'h = 0$ on some neighborhood of p contained in $\mathrm{D}_A(h) \cap \mathrm{D}_A(h')$. As pointed out above, we may choose this neighborhood to be of type $\mathrm{D}_A(f)$, where $f \in \mathbb{K}[A]$ is not vanishing at p. Thus, g/h and g'/h' will be identified if $f(gh' - g'h) = 0 \in \mathbb{K}[A]$ for some $f \in \mathbb{K}[A]$ with $f(p) \neq 0$.

The construction of both rings $\mathbb{K}[A]_f$ and $\mathcal{O}_{A,p}$ follows the same algebraic principle: we invert elements of a multiplicative closed subset U of a ring R (it is natural to invert elements from multiplicatively closed subsets since the product of two inverted elements is an inverse for the product).

The principle is familiar to us from Section 2.6 where we studied the quotient field of an integral domain R. In that case, $U = R \setminus \{0\}$. In the more general setting considered here, however, U may contain zerodivisors (such as x or y in $\mathbb{K}[x,z]/\langle xy\rangle$). Thus, we cannot conclude from an equation of type $f(gh' - g'h) = 0$ that $gh' - g'h = 0$.

Taking our cue from these considerations, we arrive at the following purely algebraic definition:

Remark-Definition 4.2.1. Let R be a ring, and let $U \subset R$ be a multiplicatively closed subset. The relation $\sim$ on $R \times U$ defined by

$$(r,u) \sim (r',u') \iff v(ru' - ur') = 0 \text{ for some } v \in U$$

is an equivalence relation (check this; observe that if we just had $ru' - ur' = 0$ in the definition of $\sim$, the transitivity law would fail if U contains zerodivisors). We write r/u for the equivalence class of (r,u) and

$$R[U^{-1}] = U^{-1}R = \{\frac{r}{u} \mid r \in R, u \in U\}$$

for the set of all equivalence classes. We make $R[U^{-1}]$ into a ring by defining

$$\frac{r}{u} + \frac{r'}{u'} = \frac{ur' + u'r}{uu'} \text{ and } \frac{r}{u} \cdot \frac{r'}{u'} = \frac{rr'}{uu'}$$

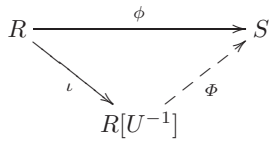
(check that these definitions are independent of the choice of representatives). This ring is called the **localization of R at U**.

We have the natural ring homomorphism

$$\iota : R \to R[U^{-1}],\ r \mapsto \frac{r}{1},$$

which sends every element of U to a unit in $R[U^{-1}]$, and maps an element $r \in R$ to zero iff r is annihilated by an element of U. In particular, ι is injective iff U does not contain a zerodivisor, and $R[U^{-1}]$ is zero iff $0 \in U$. □

Exercise* 4.2.2 (Universal Property of Localization). Let R be a ring, and let $U \subset R$ be a multiplicatively closed subset. Show that if $\phi : R \to S$ is a homomorphism of rings which maps the elements of U to units, there exists a uniquely determined homomorphism $\Phi : R[U^{-1}] \to S$ such that the diagram



commutes. □

Exercise* 4.2.3 (Localization Commutes with Passing to Quotients by Ideals). Let R and U be as above, let $I \subset R$ be an ideal, and let $\overline{U}$ be the image of U in R/I. Then show that the natural map

$$R \to R[U^{-1}] \to R[U^{-1}]/I\,R[U^{-1}]$$

induces an isomorphism

$$(R/I)[\overline{U}^{-1}] \cong R[U^{-1}]/I\,R[U^{-1}].$$

□

Basic examples of localized rings are obtained by considering the multiplicative closed sets introduced earlier in this book:

Remark-Definition 4.2.4. Let R be a ring.

1. If R is an integral domain, and $U = R \setminus \{0\}$, then $R[U^{-1}]$ is the quotient field $\mathrm{Q}(R)$ of R, and any localization of R can be regarded as a subring of $\mathrm{Q}(R)$, with quotient field $\mathrm{Q}(R)$ (apply the universal property). If R is arbitrary, we may consider the multiplicatively closed set U of all nonzerodivisors of R. We, again, write $\mathrm{Q}(R) = R[U^{-1}]$, and call $\mathrm{Q}(R)$ the **total quotient ring** of R. Since U does not contain a zerodivisor, the natural ring homomorphism $\iota : R \to \mathrm{Q}(R)$ is injective, and we may consider R as a subring of $\mathrm{Q}(R)$ by means of ι.
2. If f is an element of R, then $U = \{f^m \mid m \geq 0\}$ is multiplicatively closed. We write $R_f = R[1/f] = R[U^{-1}]$ in this case.
3. If $\mathfrak{p}$ is a prime ideal of R, then $U = R \setminus \mathfrak{p}$ is multiplicatively closed. We write $R_\mathfrak{p} = R[U^{-1}]$ in this case, and call $R_\mathfrak{p}$ the **localization of R at $\mathfrak{p}$**. □

Example 4.2.5. By inverting all elements in $U = \mathbb{Z} \setminus \{0\}$, we obtain the field $\mathbb{Q}$ of rational numbers. Inverting fewer elements, we get subrings of $\mathbb{Q}$. For instance, if $n \in \mathbb{Z}$ is any number, we get the subring

$$\mathbb{Z}[1/n] = \{a/b \in \mathbb{Q} \mid b = n^k \text{ for some } k \in \mathbb{N}\}.$$

Or, if $p \in \mathbb{Z}$ is any prime number, we get the subring

$$\mathbb{Z}_{\langle p \rangle} = \{a/b \in \mathbb{Q} \mid p \text{ does not divide } b\}.$$

If p does not divide n, we have ring inclusions

$$\mathbb{Z} \subset \mathbb{Z}[1/n] \subset \mathbb{Z}_{\langle p \rangle} \subset \mathbb{Q}.$$

□

Remark 4.2.6. If $\mathfrak{p}$ is a prime ideal of a ring R, the nonunits of the ring $R_\mathfrak{p}$ form the ideal

$$\mathfrak{p}R_\mathfrak{p} = \{r/u \mid r \in \mathfrak{p}, u \in R \setminus \mathfrak{p}\}.$$

Taking Remark 1.3.8 into account, we find that $(R_\mathfrak{p}, \mathfrak{p}R_\mathfrak{p})$ is a local ring in the sense of Definition 1.3.7. By Exercise 4.2.3, the residue field is

$$R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} \cong \mathrm{Q}(R/\mathfrak{p}).$$

□

Generalizing what we observed in the remark, our next result shows that the ideal theory of a localized ring is always a simplified version of the ideal theory of the original ring. This result is the main reason for the importance of rings of fractions in commutative algebra.

Theorem 4.2.7. *Let R be a ring, let $U \subset R$ be a multiplicative closed subset, and let $\iota : R \to R[U^{-1}]$, $r \mapsto r/1$, be the natural homomorphism.*

1. *If $I \subset R$ is an ideal, then*
$$\iota^{-1}(IR[U^{-1}]) = \{a \in R \mid ua \in I \text{ for some } u \in U\}.$$
2. *If $J \subset R[U^{-1}]$ is an ideal, then*
$$\iota^{-1}(J)R[U^{-1}] = J.$$
We, thus, get an injectice map of the set of ideals of $R[U^{-1}]$ into the set of ideals of R by sending J to $\iota^{-1}(J)$.
3. *If R is Noetherian, then so is $R[U^{-1}]$.*
4. *The injection $J \mapsto \iota^{-1}(J)$ restricts to a bijection between the set of prime ideals of $R[U^{-1}]$ and the set of prime ideals of R not meeting U.*

Proof. For part 1, observe that if $a \in R$, then $a \in \iota^{-1}(IR[U^{-1}]) \iff a/1 \in IR[U^{-1}] \iff ua \in I$ for some $u \in U$. For part 2, let $b/u \in R[U^{-1}]$, where $b \in R$ and $u \in U$. Then $b/u \in J \iff b/1 \in J \iff b \in \iota^{-1}(J) \iff b/u \in \iota^{-1}(J)R[U^{-1}]$. Part 3 follows from part 2 (for instance, use the ascending chain condition). For part 4, notice that if $\mathfrak{q}$ is a prime ideal of $R[U^{-1}]$, then $\mathfrak{p} = \iota^{-1}(\mathfrak{q})$ is a prime ideal of R. Moreover, $\mathfrak{p} \cap U = \emptyset$ since $\mathfrak{q}$ does not contain units. Conversely, let $\mathfrak{p}$ be a prime ideal of R such that $\mathfrak{p} \cap U = \emptyset$. If $a/u \cdot b/v \in \mathfrak{p}R[U^{-1}]$, with $u, v \in U$, then $wab \in \mathfrak{p}$ for some $w \in U$. Since $w \notin \mathfrak{p}$, we must have $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$ and, thus, $a/u \in \mathfrak{p}R[U^{-1}]$ or $b/v \in \mathfrak{p}R[U^{-1}]$. Moreover, $1 \notin \mathfrak{p}R[U^{-1}]$, so $\mathfrak{p}R[U^{-1}]$ is a prime ideal of $R[U^{-1}]$. The result follows from part 1 since $\iota^{-1}(\mathfrak{p}R[U^{-1}]) = \{a \in R \mid ua \in \mathfrak{p} \text{ for some } u \in U\} = \mathfrak{p}$. □

Exercise* 4.2.8 (Localization Commutes with Forming Radicals). If $I \subset R$ is an ideal, then show that $\operatorname{rad}(IR[U^{-1}]) = (\operatorname{rad} I)R[U^{-1}]$. Conclude that the injection $J \mapsto \iota^{-1}(J)$ restricts to a bijection between the set of primary ideals of $R[U^{-1}]$ and the set of primary ideals of R not meeting U. □

In the geometric setting, given an algebraic set A, we apply the constructions discussed in Example 4.2.4 to the coordinate ring $\mathbb{K}[A]$.

To begin with, the total quotient ring $\mathbb{K}(A) := \mathrm{Q}(\mathbb{K}[A])$ is the **ring of rational functions** on A. Here, the terminology introduced in Section 2.6 for rational functions on varieties carries over to rational functions on arbitrary algebraic sets. In particular, we define the **domain of definition** $\operatorname{dom}(f)$ of a rational function $f \in \mathbb{K}(A)$ as in Section 2.6, and view f as a function on $\operatorname{dom}(f)$. Note that $\operatorname{dom}(f)$ is open and, by Exercise 1.11.9, dense in the Zariski topology on A.

If $f \in \mathbb{K}[A]$, the localization $\mathbb{K}[A]_f$ is the $\mathbb{K}$-algebra of functions on $\mathrm{D}_A(f)$ considered in the introduction to this section.

Similarly, if $p \in A$ is a point, the local ring $\mathcal{O}_{A,p}$ is formally defined as the localization of $\mathbb{K}[A]$ at the maximal ideal of $\mathbb{K}[A]$ corresponding to p:

Remark-Definition 4.2.9. Let $A \subset \mathbb{A}^n$ be an algebraic set, and let $p \in A$ be a point. The **local ring of A at p,** written $\mathcal{O}_{A,p}$, is defined to be the localization

$$\mathcal{O}_{A,p} = \mathbb{K}[A]_{\mathfrak{m}},$$

where $\mathfrak{m} = \mathrm{I}_A(p) \subset \mathbb{K}[A]$ is the maximal ideal corresponding to p. Taking Remark 4.2.6 and part 3 of Proposition 4.2.7 into account, we find that $\mathcal{O}_{A,p}$ is a local Noetherian ring with maximal ideal

$$\mathfrak{m}_{A,p} := \{f/g \in \mathcal{O}_{A,p} \mid f(p) = 0\}.$$

Furthermore, by Exercise 4.2.3,

$$\mathcal{O}_{A,p} = \mathcal{O}_{\mathbb{A}^n,p}/\mathrm{I}(A)\,\mathcal{O}_{\mathbb{A}^n,p}.$$

□

Exercise 4.2.10. Let $B_1, B_2 \subset \mathbb{A}^n$ be algebraic sets, let $A = B_1 \cup B_2$, and let $p \in A$ be a point not lying on B_2. Then show that $\mathcal{O}_{A,p} \cong \mathcal{O}_{B_1,p}$. □

Remark 4.2.11. If V is an affine variety, the local rings $\mathcal{O}_{V,p}$, $p \in V$, are subrings of $\mathbb{K}(V)$ containing $\mathbb{K}[V]$. In fact, by Proposition 2.6.15,

$$\mathbb{K}[V] = \bigcap_{p \in V} \mathcal{O}_{V,p} \subset \mathbb{K}(V).$$

□

Remark 4.2.12. Instead of just considering local rings at points, it makes also sense to consider the **local ring of A along** a subvariety W of A. This ring, written $\mathcal{O}_{A,W}$, is the localization of $\mathbb{K}[A]$ at the prime ideal $\mathfrak{p} = \mathrm{I}_A(W)$. If $A = V$ is a variety, then $\mathcal{O}_{V,W}$ is a subring of $\mathbb{K}(V)$, namely the subring consisting of all rational functions on V that are defined at some point of W (and, hence, defined on a dense open subset of W). □

We postpone the further development of the general theory of localization to Section 4.5. Our next goal in this section is to characterize the smoothness of an algebraic set A at a point $p \in A$ in terms of the local ring $\mathcal{O}_{A,p}$. To begin with, we characterize the local dimension $\dim_p A$ in terms of $\mathcal{O}_{A,p}$:

Proposition 4.2.13. *If R is a ring, and $\mathfrak{p}$ is a prime ideal of R, then*

$$\dim R_{\mathfrak{p}} = \operatorname{codim} \mathfrak{p}.$$

In particular, if $A \subset \mathbb{A}^n$ is an algebraic set, and $p \in A$ is a point, then

$$\dim \mathcal{O}_{A,p} = \dim_p A.$$

Proof. By Proposition 4.2.7, there is a one-to-one correspondence between maximal chains of prime ideals of $R_{\mathfrak{p}}$ and maximal chains of prime ideals of R with largest ideal $\mathfrak{p}$:

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_d = \mathfrak{p}.$$

This shows the first assertion. For the second assertion, note that if $R = \mathbb{K}[A]$, and $\mathfrak{p} = \mathrm{I}_A(p) \subset R$ is the maximal ideal corresponding to p, then a chain as above corresponds to a chain of subvarieties $W_i := \mathrm{V}_A(\mathfrak{p}_i) \subset A$ containing p. The variety W_0 is actually an irreducible component of A since otherwise we could insert a prime ideal strictly contained in $\mathfrak{p}_0$. Moreover,

$$\langle 0 \rangle \subsetneq \mathfrak{p}_1/\mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_d/\mathfrak{p}_0$$

is a maximal chain of prime ideals of $\mathbb{K}[W_0] \cong \mathbb{K}[A]/\mathfrak{p}_0$. Every such chain has length $\dim W_0$ by Corollary 3.4.9. Conversely, if $\mathfrak{p}_0 \subset \mathbb{K}[A]$ is a prime ideal such that $\mathrm{V}_A(\mathfrak{p}_0)$ is an irreducible component of A passing through p, then $\mathfrak{p}_0$ fits as smallest ideal into a maximal chain of prime ideals of $\mathbb{K}[A]$ with largest ideal $\mathfrak{p} = \mathrm{I}_A(p)$. □

Next, in the final version of Theorem 4.1.17, we describe the tangent space T_pA in terms of $\mathcal{O}_{A,p}$. For this, note that if $(R, \mathfrak{m})$ is a local ring with residue field $R/\mathfrak{m}$, then $\mathfrak{m}/\mathfrak{m}^2$ is naturally an $R/\mathfrak{m}$-module. That is, $\mathfrak{m}/\mathfrak{m}^2$ is an $R/\mathfrak{m}$-vector space.

Theorem-Definition 4.2.14 (Zariski Tangent Space, Final Version). *If $A \subset \mathbb{A}^n$ is an algebraic set, and $p \in A$ is a point, there is a natural isomorphism of $\mathbb{K}$-vector spaces*

$$(\mathfrak{m}_{A,p}/\mathfrak{m}_{A,p}^2)^* \cong T_pA.$$

*We call $(\mathfrak{m}_{A,p}/\mathfrak{m}_{A,p}^2)^*$ the **Zariski tangent space** to A at p.*

Proof. Let $f = g/h \in \mathbb{K}(x_1, \ldots, x_n)$ be a rational function such that $h(p) \neq 0$. In extending what we did for polynomials, we define the **differential d_pf of f at p** by formally writing down the quotient rule:

$$d_pf := \frac{h(p)d_pg - g(p)d_ph}{h^2(p)}$$

(this is independent of the choice of representation for f as a fraction). Arguing, now, as in the proof of Theorem 4.1.17, we get a map

$$d_p : \mathfrak{m}_{A,p} \to T_p^*A,\ \overline{f} = \overline{g}/\overline{h} \mapsto d_pf|T_pA$$

whose kernel is $\mathfrak{m}_{A,p}^2$. □

Combining Proposition 4.2.13 and Theorem 4.2.14, we get:

Corollary 4.2.15. *Let $A \subset \mathbb{A}^n$ be an algebraic set, and let $p \in A$ be a point. Then A is smooth at p iff*

$$\dim_{\mathbb{K}} \mathfrak{m}_{A,p}/\mathfrak{m}_{A,p}^2 = \dim \mathcal{O}_{A,p}.$$

□

Corollary 4.2.16. *If $A \subset \mathbb{A}^n$ is an algebraic set, then A_{sing} and A have no irreducible component in common.*

Proof. As already pointed out in Remark 4.1.11, we will show in Corollary 4.6.26 that a point of A is singular iff it lies on the intersection of two irreducible components of A or is a singular point of one of the components. For our purposes here, it is, hence, enough to show that if V is such a component, then V contains V_{sing} properly. By Proposition 4.1.3, this is true in the hypersurface case. To reduce to this case, we apply Theorem 3.5.2: let $\phi : V \to W$ be a finite morphism onto a hypersurface $W \subset \mathbb{A}^{d+1}$ admitting a rational inverse $\psi : W \dashrightarrow V$. Then, since W_{sing} is a proper algebraic subset of W, the set $U := \text{dom}(\psi) \cap (W \setminus W_{\text{sing}})$ is Zariski dense in W. In particular, U is nonempty. But if $q = \phi(p)$ is a point of U, the isomorphism $\phi^* : \mathbb{K}(W) \to \mathbb{K}(V)$ restricts to an isomorphism $\mathcal{O}_{W,q} \cong \mathcal{O}_{V,p}$. Hence, we are done by Corollary 4.2.15. □

The inequality

$$\dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 \geq \dim R \tag{4.3}$$

holds for any local Noetherian ring $(R, \mathfrak{m})$ (this is the. general algebraic form of inequality (4.1) on Page 143 which we will be prove in Corollary 4.6.20). The importance of Corollary 4.2.15 is emphasized by the following definition:

Definition 4.2.17 (Krull). A local Noetherian ring $(R, \mathfrak{m})$ is called **regular** if $\dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = \dim R$. □

Using this notion, we can restate Corollary 4.2.15 as follows:

Corollary 4.2.18. *Let $A \subset \mathbb{A}^n$ be an algebraic set, and let $p \in A$ be a point. Then A is smooth at p iff $\mathcal{O}_{A,p}$ is a regular local ring .* □

In most textbooks on commutative algebra, the definition of a regular local ring involves a characterization of $\dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$ in terms of generators for $\mathfrak{m}$. This is obtained as an application of the following fundamental result:

Theorem 4.2.19 (Lemma of Nakayama). *Let $(R, \mathfrak{m})$ be a local ring, let M be a finitely generated R-module, and let $N \subset M$ be a submodule. Then*

$$N + \mathfrak{m}M = M \;\; \textit{iff} \;\; N = M.$$

Proof. Replacing M by M/N, we reduce to the case $N = 0$. That is, it suffices to show that $\mathfrak{m}M = M$ implies $M = 0$ (the converse implication is clear). Let $m_1, \ldots, m_r$ be a finite set of generators for M. If $\mathfrak{m}M = M$, we may write each m_i as an $\mathfrak{m}$-linear combination of the m_j:

$$m_i = \sum r_{ij} m_j, \text{ with all } r_{ij} \in \mathfrak{m}.$$

In matrix notation,

$$(E_r - B) \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix} = 0,$$

where $B = (r_{ij})$ and E_r is the $r \times r$ identity matrix. Arguing once more as in the proof of the Projection Theorem 3.1.2, we multiply with the matrix of cofactors of $(E_r - B)$, and obtain that $h = \det(E_r - B)$ annihilates each m_i. This implies that the m_i and, thus, M are zero. Indeed, h is a unit in R since $h \equiv 1 \mod \mathfrak{m}$. □

Starting from well-known facts on vector spaces, Nakayama's lemma allows us to deduce information on modules over local rings. In making this explicit, we use the following notation: If R is any ring, and M is any R-module, a **set of generators** for M is **minimal** if no proper subset generates M.

Corollary 4.2.20. *Let $(R, \mathfrak{m})$ and M be as in Nakayama's Lemma 4.2.19. Then $m_1, \ldots, m_r \in M$ generate M as an R-module iff the residue classes $\overline{m}_i = m_i + \mathfrak{m}M$ generate $M/\mathfrak{m}M$ as an $R/\mathfrak{m}$-vector space. In particular, any minimal set of generators for M corresponds to an $R/\mathfrak{m}$-basis for $M/\mathfrak{m}M$, and any two such sets have the same number of elements.*

Proof. Let $N = \langle m_1, \ldots, m_r \rangle \subset M$. Then $m_1, \ldots, m_r$ generate M iff $N + \mathfrak{m}M = M$ iff $\operatorname{span}(\overline{m}_1, \ldots, \overline{m}_r) = M/\mathfrak{m}M$. □

Corollary 4.2.21. *A local Noetherian ring $(R, \mathfrak{m})$ is* **regular** *iff $\mathfrak{m}$ can be generated by $\dim R$ elements.* □

The first part of the exercise below shows that the conclusion of Corollary 4.2.20 may be wrong over arbitrary rings:

Exercise 4.2.22. 1. Find an ideal of $\mathbb{k}[x_1, \ldots, x_n]$ which admits minimal sets of generators differing in their number of elements.
2. Let $\mathcal{O}_{\mathbb{A}^2,o}$ be the local ring of $\mathbb{A}^2$ at the origin $o = (0, 0)$. For each $n \in \mathbb{N}$, find an ideal of $\mathcal{O}_{\mathbb{A}^2,o}$ which is minimally generated by n elements. □

Another application of Nakayama's lemma, which we present for later use, is a special case of Krull's intersection theorem (see Eisenbud (1995), Corollary 5.4 for the general case):

Theorem 4.2.23 (Krull's Intersection Theorem). *Let $(R, \mathfrak{m})$ be a local Noetherian ring. Then*

$$\bigcap_{k=0}^{\infty} \mathfrak{m}^k = \langle 0 \rangle.$$

Proof. In the polynomial ring $R[t]$, consider the subalgebra

$$S = R[\mathfrak{m}t] = R \oplus \mathfrak{m}t \oplus \mathfrak{m}^2t^2 \oplus \ldots \subset R[t].$$

Since R is Noetherian, $\mathfrak{m}$ is a finitely generated ideal of R. It follows that S is a finitely generated R-algebra and, thus, that S is Noetherian, too. In particular, if $J = \bigcap_{k=0}^{\infty} \mathfrak{m}^k$, the ideal

$$J \oplus Jt \oplus Jt^2 \oplus \ldots \subset S$$

is generated by finitely many *homogeneous* polynomials in $R[t]$ (take the homogeneous components of any finite set of generators). If r is the maximum degree in of the generators, then $\mathfrak{m}tJt^r = Jt^{r+1}$. That is,

$$\mathfrak{m} \bigcap_{k=0}^{\infty} \mathfrak{m}^k = \bigcap_{k=0}^{\infty} \mathfrak{m}^k \subset R.$$

The result follows from Nakayama's lemma. □

Example 4.2.24. The conclusion of the intersection theorem may not hold if R is not Noetherian. For instance, let R be the ring of germs of $\mathcal{C}^\infty$ functions defined on arbitrarily small ϵ-neighborhoods of the origin $0 \in \mathbb{R}$ (that is, the elements of R are obtained by identifying two functions if they coincide on a sufficiently small neighborhood of 0). Then R is local with maximal ideal $\mathfrak{m} = \langle x \rangle$, where x is (the germ of) the coordinate function. On the other hand, the function

$$g(x) = \begin{cases} e^{-1/x^2} & \text{if } x \neq 0, \\ 0 & \text{if } x = 0 \end{cases}$$

defines a (nontrivial) element of $\bigcap_{k=0}^{\infty} \mathfrak{m}^k$: indeed, $g(x)/x^k$ is $\mathcal{C}^\infty$ for every k. In particular, R cannot be Noetherian by Krull's intersection theorem. □

We end this section as we have started it, namely by considering admissible functions. So far, given an algebraic set $A \subset \mathbb{A}^n$, we have described the functions allowed on distinguished open subsets of A. Now, taking our cue from Proposition 2.6.15, we deal with arbitrary open subsets:

Remark-Definition 4.2.25. Let $A \subset \mathbb{A}^n$ be an algebraic set, and let $U \subset A$ be an open subset. A function $f : U \to \mathbb{K}$ is called **regular at a point** $p \in U$ if there are $g, h \in \mathbb{K}[A]$ such that $h(q) \neq 0$ and $f(q) = g(q)/h(q)$ for all $q \in U$. We say that f is **regular on** $\boldsymbol{U}$ if it is regular at every point of U. The set $\mathcal{O}(U)$ of all regular functions on U becomes a ring, with pointwise defined algebraic operations. That is, we add and multiply values in $\mathbb{K}$.

On distinguished open subsets, we get the functions already familiar to us:

Proposition 4.2.26. *Let $A \subset \mathbb{A}^n$ be an algebraic set. If $0 \neq h \in \mathbb{K}[A]$, then for each regular function f on $\mathrm{D}_A(h)$, there exist $g \in \mathbb{K}[A]$ and $m \geq 1$ such that $f(p) = g(p)/h(p)^m$ for all $p \in \mathrm{D}_A(h)$. That is, we may identify $\mathcal{O}(\mathrm{D}_A(h)) = \mathbb{K}[A]_h$. In particular, taking $h = 1$, we get $\mathcal{O}(A) = \mathbb{K}[A]$. That is, the regular functions on A are precisely the polynomial functions.*

Proof. Let f be a regular function on $\mathrm{D}_A(h)$. Since the Zariski topology is quasicompact, we can find a finite family of pairs of functions $g_i, h_i \in \mathbb{K}[A]$, say $i = 1, \ldots, N$, such that $\mathrm{D}_A(h) = \bigcup_{i=1}^N \mathrm{D}_A(h_i)$, and such that $f = g_i/h_i$ as functions on $\mathrm{D}_A(h_i)$, for all i. Then, for all i, j, we have $g_i h_j - g_j h_i = 0$ on $\mathrm{D}_A(h_i) \cap \mathrm{D}_A(h_j) = \mathrm{D}_A(h_i h_j)$ and, thus, $h_i h_j (g_i h_j - g_g h_i) = 0$ on all of A. Replacing g_i by $g_i h_i$ and h_i by h_i^2 for all i, we may suppose that $g_i h_j = g_j h_i$ on A for all i, j.

Since $\mathrm{D}_A(h) = \bigcup_{i=1}^N \mathrm{D}_A(h_i)$, we have $\mathrm{V}_A(h) = \mathrm{V}_A(h_1, \ldots, h_N)$. The Nullstellensatz implies that $h^m \in \langle h_1, \ldots, h_N \rangle$ for some $m \geq 1$, say $h^m = \sum_{i=1}^N a_i h_i$, with $a_1, \ldots, a_N \in \mathbb{K}[A]$. Let $g = \sum_{i=1}^N a_i g_i$. Then for all j,

$$h^m g_j = \sum_{i=1}^N a_i h_i g_j = \sum_{i=1}^N a_i g_i h_j = g h_j$$

and, thus, $f = g_j/h_j = g/h^m$ as functions on $\mathrm{D}_A(h_j)$. The result follows since $\mathrm{D}_A(h) = \bigcup_{i=1}^N \mathrm{D}_A(h_i)$. □

Exercise 4.2.27. Show that regular functions are continous when $\mathbb{K}$ is identified with $\mathbb{A}^1$ in its Zariski topology.
Hint: The property that a subset Y of a topological space X is closed is a **local property** in the sense that Y is closed if it can be covered by open subsets U of X such that $Y \cap U$ is closed in Y for all U. □

Exercise 4.2.28 (Characterization of Rational Functions). Let A be an algebraic set. Let Σ be the set of pairs (U, f), where U is a Zariski dense open subset of A, and where $f \in \mathcal{O}(U)$. Show that the relation $\sim$ on Σ defined by

$$(U, f) \sim (U', f') \iff f|U \cap U' = f'|U \cap U'$$

is an equivalence relation. Show that the set of all equivalence classes is a ring which is naturally isomorphic to $\mathbb{K}(A)$ (the sum and product of two classes represented by pairs (U, f) and (U', f') are obtained by adding and multiplying f and f' on $U \cap U'$, respectively). Conclude that if $A = V_1 \cup \cdots \cup V_s$ is the decomposition of A into its irreducible components, then

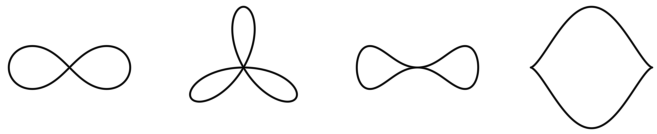
$$\mathbb{K}(A) \cong \mathbb{K}(V_1) \times \cdots \times \mathbb{K}(V_s).$$

□

4.3 Intersection Multiplicities of Plane Curves

In Section 5, we will prove Bezout's Theorem which says that if C, D are two plane curves of degrees d, e without a common component, then C and D intersect in precisely $d \cdot e$ points – provided we work in the right setting, and provided we count the intersection points with appropriate multiplicities. The right setting will be created in Section 5.1 by adding points at infinity. How to define the multiplicities will be explained now. We begin by fixing some terminology for dealing with singularities of plane curves.

Example 4.3.1. The following picture shows plane curves with different types of singularities:



node triple point tacnode cusps

□

Plane curves correspond to nonconstant square-free polynomials $f \in \Bbbk[x, y]$, where f is determined up to multiplication by a nonzero scalar. For reasons which will become clear later in this section, however, it is convenient to allow f to have multiple factors in the following definitions.

Definition 4.3.2. Let $f \in \Bbbk[x, y]$ be a nonconstant polynomial, and let $p = (a, b) \in \mathbb{A}^2$ be a point. Let

$$f = f_0 + f_1 + f_2 + \ldots + f_d \in \mathbb{K}[x, y]$$

be the Taylor expansion of f at p, where, for each i, the polynomial f_i collects the degree-i terms of f in $x-a$ and $x-b$. The **multiplicity of f at p**, written $\mathrm{mult}(f, p)$, is defined to be the least m such that $f_m \neq 0$. By convention, $\mathrm{mult}(0, p) = \infty$.

If f is square-free, and $C = \mathrm{V}(f) \subset \mathbb{A}^2$ is the corresponding curve, we write $\mathrm{mult}(C, p) = \mathrm{mult}(f, p)$, and call this number the **multiplicity of C at p**. □

Note that $p \in \mathrm{V}(f)$ iff $\mathrm{mult}(f, p) \geq 1$. If f is square-free, and $C = \mathrm{V}(f)$, then $\mathrm{mult}(C, p) = 1$ iff p is a smooth point of C. We speak of a **double point** if the multiplicity m is 2, of a **triple point**, if $m = 3$, and a **quadruple point**, if $m = 4$.

Example 4.3.3. The origin is a double point of each curve shown below:

$y^2 = x^3 + x^2$ $y^2 = x^3$ $y^2 = xy + x^2y - x^3$

□

Different types of singularities of plane curves can often be distinguished by considering the tangent lines at these points. To introduce tangent lines at singular points, we remark that over the algebraically closed field $\mathbb{K}$, every

homogeneous polynomial in two variables can be written as a product of linear factors. Indeed, if $g = y^s h \in \mathbb{K}[x,y]$, where y does not divide h, the dehomogenized polynomial $g(x,1) = h(x,1)$ is univariate and decomposes, hence, into linear factors: $g(x,1) = h(x,1) = \prod_{i=1}^{r-1}(\lambda_i x - \mu_i)^{e_i} \in \mathbb{K}[x,y]$. Homogenizing the factors, we get $g = y^s \prod_{i=1}^{r-1}(\lambda_i x - \mu_i y)^{e_i}$.

Definition 4.3.4. Let $f \in \Bbbk[x,y]$ be a nonconstant polynomial, and let $p = (a,b) \in \mathbb{A}^2$ be a point. Let

$$f = f_m + \ldots + f_d \in \mathbb{K}[x,y]$$

be the Taylor expansion of f at p as in Definition 4.3.2, where $m = \mathrm{mult}(f,p)$. Decompose f_m over $\mathbb{K}$ into pairwise different linear factors in $x-a$ and $y-b$:

$$f_m = \prod_{i=1}^{r}(\lambda_i(x-a) - \mu_i(y-b))^{e_i} \in \mathbb{K}[x,y].$$

The **tangent lines to f at p** are defined to be the lines

$$L_i = \mathrm{V}(\lambda_i(x-a) - \mu_i(y-b)) \subset \mathbb{A}^2,$$

and e_i is the **multiplicity** of L_i.

If f is square-free, and $C = \mathrm{V}(f) \subset \mathbb{A}^2$ is the corresponding curve, the tangent lines to f at p are also called the **tangent lines to C at p**. □

At a smooth point of C, the multiplicity $m = 1$, and the definition above yields precisely the tangent line introduced in Section 4.1. If C has $m \geq 2$ *distinct* tangent lines (of multiplicity 1) at p, we say that p is an **ordinary multiple point** of C. An ordinary double point is called a **node**.

Example 4.3.5. In Example 4.3.3, the origin o is a node of $\mathrm{V}(y^2 - x^2 - x^3)$, with tangent lines $\mathrm{V}(x+y)$ and $\mathrm{V}(x-y)$. Similarly, o is a node of the reducible curve $C = \mathrm{V}(y^2 - xy - x^2y + x^3)$: the two different tangent lines are the line $\mathrm{V}(x-y)$, which is one of the components of C, and the x-axis, which is the tangent line at o to the other component $\mathrm{V}(y - x^2)$ of C. In contrast, the curve $\mathrm{V}(y^2 - x^3)$ has a tangent line of multiplicity 2 at o. □

Exercise 4.3.6. The curves in Example 4.3.1 are defined by the polynomials below:

$$y^2 = (1-x^2)^3, \quad y^2 = x^2 - x^4, \quad y^3 - 3x^2y = (x^2+y^2)^2, \quad y^2 = x^4 - x^6.$$

Which curve corresponds to which polynomial? □

Before turning to intersection multiplicities, we present a result which shows that the ideals of local rings of plane curves at smooth points are easy to handle. We need the following notation:

Definition 4.3.7. A **discrete valuation** on a field K is a surjective map $v\colon K \setminus \{0\} \to \mathbb{Z}$ such that, for all $a, b \in K \setminus \{0\}$,

1. $v(ab) = v(a) + v(b)$, and
2. $v(a + b) \geq \min(v(a), v(b))$. □

Note that the first condition of the definition means that $v : K \setminus \{0\} \to \mathbb{Z}$ is a group homomorphism. In particular, $v(1) = 0$. By convention, $v(0) = \infty$. The set

$$R := \{a \in K \mid v(a) \geq 0\}$$

is, then, a subring of K to which we refer as the **valuation ring** of v.

Definition 4.3.8. An integral domain R is called a **discrete valuation ring** (**DVR** for short) if R is the valuation ring of a discrete valuation on its quotient field. □

Example 4.3.9. The ring $\Bbbk[[x]]$ of formal power series $f = \sum_{i=0}^{\infty} a_i x^i$ with coefficients $a_i \in \Bbbk$ is a DVR. Indeed, it is an integral domain with quotient field $\Bbbk((x))$, where

$$\Bbbk((x)) = \{\sum_{i=n}^{\infty} a_i x^i \mid a_i \in \Bbbk \text{ for all } i\}$$

is the field of formal Laurent series with coefficients in $\Bbbk$. The desired valuation on $\Bbbk((x))$ is obtained by setting $v(f) = n$ if $f = \sum_{i=n}^{\infty} a_i x^i$ with $a_n \neq 0$. Using the same terminology as for convergent power and Laurent series in complex analysis, we say that $v(f)$ is the **vanishing order** of a formal power series $f \in \Bbbk[[x]]$ and that a formal Laurent series $f \in \Bbbk((x)) \setminus \Bbbk[[x]]$ has a **pole** of order $-v(f)$. □

If R is a DVR with quotient field K and corresponding discrete valuation v on K, its set of nonunits, which is the set

$$\mathfrak{m} := \{a \in K \mid v(a) \geq 1\},$$

is an ideal of R. Hence, $(R, \mathfrak{m})$ is a local ring. Furthermore, R is a PID: Since v is surjective, there is an element $t \in \mathfrak{m}$ such that $v(p) = 1$, and we claim that every nonzero ideal I of R is of type $I = \langle t^k \rangle = \mathfrak{m}^k = \{a \in R \mid v(a) \geq k\}$, where k is minimal among all $v(g)$, $g \in I$. Indeed, to see this, just note that if a, b are two elements of R, then $v(a) = v(b)$ iff $v(ab^{-1}) = 0$ iff ab^{-1} is a unit of R iff $\langle a \rangle = \langle b \rangle$.

Exercise* **4.3.10.** Let R be a local Noetherian integral domain with maximal ideal $\mathfrak{m}$. Suppose that R contains a field L such that the composite map $L \to R \to R/\mathfrak{m}$ is an isomorphism. Then all quotients $\mathfrak{m}^k/\mathfrak{m}^{k+1}$ are L-vector spaces. In this situation, show that R is a DVR iff the following two conditions hold:

1. $\dim_L \mathfrak{m}^k/\mathfrak{m}^{k+1} = 1$ for all $k \geq 0$;
2. $\dim_L R/\mathfrak{m}^k = k$ for all $k \geq 1$. □

Proposition 4.3.11. *Let R be a local ring. Then the following are equivalent:*

1. R is a DVR.
2. R is regular of dimension 1.

Proof. 1 $\implies$ 2: If R is a DVR with maximal ideal $\mathfrak{m}$, the only chain of prime ideals of R is $\langle 0\rangle \subsetneq \mathfrak{m}$. So R has Krull dimension one. Moreover, as already pointed out in the discussion preceeding Exercise 4.3.10 , $\mathfrak{m}$ is generated by just one element. So R is regular.

2 $\implies$ 1: Conversely, suppose that R is regular of dimension one, and let t be a generator for the maximal ideal $\mathfrak{m}$. To show that R is a DVR, we first observe that $t^r \neq 0$ for all r. Indeed, otherwise, $\mathfrak{m} = \langle t\rangle$ would be the only prime ideal of R, so that R would be zerodimensional. Let, now, $0 \neq g \in R$. By Krull's intersection theorem, g cannot be contained in all powers of $\mathfrak{m}$. Let $k = \max\{r \mid g \in \mathfrak{m}^r\}$. Then $g = ut^k$ for some element $u \in R \setminus \mathfrak{m}$, which necessarily is a unit of R. Similarly, if $0 \neq h$ is another element of R, write h as a product vt^ℓ, for some unit v and some ℓ. Then $gh = uvt^{k+\ell}$ is nonzero, and we conclude that R is an integral domain. Furthermore, any element f of the quotient field $\mathrm{Q}(R)$ has a unique representation of type $f = wt^m$, for some unit w and some $m \in \mathbb{Z}$. Setting $v(f) = m$, we get the desired discrete valuation on $\mathrm{Q}(R)$. □

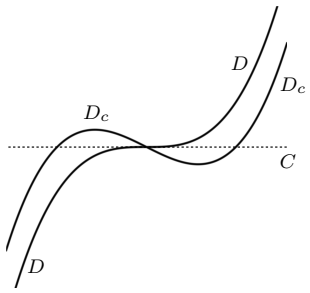
Taking Corollary 4.2.18 into account, we get:

Corollary 4.3.12. *An irreducible curve $C \subset \mathbb{A}^2$ is smooth at a point $p \in C$ iff $\mathcal{O}_{C,p}$ is a discrete valuation ring.* □

If C is smooth at p, we occasionally write $v_{C,p}$ for the corresponding discrete valuation on $\mathbb{K}(C)$. Motivated by Example 4.3.9, we say that $v_{C,p}(f)$ is the **vanishing order** of an element $f \in \mathcal{O}_{C,p}$, and that a rational function $f \in \mathbb{K}(C) \setminus \mathcal{O}_{C,p}$ has a **pole** of order $-v_{C,p}(f)$ at p.

We will, now, define intersection multiplicities. There are several ways of doing this, some of which go back to Newton and his contemporaries (see Fulton (1998), Chapter 7, Notes and References for some historical remarks).

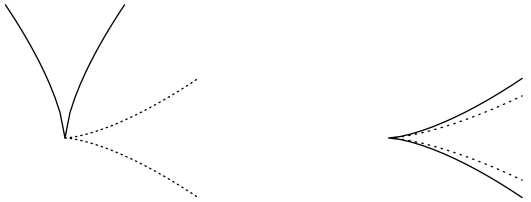
Example 4.3.13. Consider the curves $C = \mathrm{V}(y)$ and $D = \mathrm{V}(y - x^r)$ in $\mathbb{A}^2(\mathbb{C})$. Intuitively, we should count the origin $o = (0, 0)$ as an intersection point of multiplicity r. Indeed, if we perturb the equations defining C and D slightly, we get r distinct intersection points near o:



The case $r = 3$.

For a more precise statement, consider, for instance, a perturbation of the defining equation $f_0 = y - x^r$ for D, say $f_c = y - x^r + c_1 x^{r-1} + \ldots + c_r$, where $c = (c_1, \ldots, c_r)$ is a tuple of complex numbers, and let $D_c = \mathrm{V}(f_c) \subset \mathbb{A}^2(\mathbb{C})$. Given a sufficiently small $\epsilon > 0$, there is, then, a number $\delta > 0$ such that for any sufficiently general c with $|c_i| < \delta$, the curve D_c intersects C in r distinct points in the ϵ-neighborhood of the origin (we will prove this in the context of Bertini's theorem in Chapter 6). □

Example 4.3.14. Now, consider the pairs of curves $y^2 - x^3$ and $x^2 - y^3$, respectively $y^2 - x^3$ and $2y^2 - x^3$:



transversal cusps tangential cusps

In both cases, can you find the intersection multiplicity at the origin? □

It is not immediately clear that the **dynamic** point of view taken in the examples above gives well-defined intersection multiplicities. Furthermore, computing intersection multiplicities in this way can be quite elaborate.

Following Macaulay (1916), we will work with a purely algebraic definition of intersection multiplicities which is **static** in that we do not vary the given equations. The definition is less intuitive, but turns out to be just right.

Definition 4.3.15. Let $f, g \in \Bbbk[x, y]$ be nonconstant polynomials, and let $p \in \mathbb{A}^2$ be a point. The **intersection multiplicity of f and g at p**, written $i(f, g; p)$, is defined to be

$$i(f, g; p) = \dim_{\mathbb{K}} \mathcal{O}_{\mathbb{A}^2,p} / \langle f, g \rangle \mathcal{O}_{\mathbb{A}^2,p}.$$

If f, g are square-free, and $C = \mathrm{V}(f), D = \mathrm{V}(f) \subset \mathbb{A}^2$ are the corresponding curves, we write $i(C, D; p) = i(f, g; p)$, and call this number the **intersection multiplicity of C and D at p**. □

The calculations in Example 4.3.17 below rely on the following observation:

Remark 4.3.16. Let $I \subset \Bbbk[x_1, \ldots, x_n]$ be an ideal such that $\mathrm{V}(I) \subset \mathbb{A}^n$ consists of a single $\Bbbk$-rational point $p = (a_1, \ldots, a_n)$. Then there is a natural isomorphism of $\mathbb{K}$-algebras

$$R := \mathbb{K}[x_1, \ldots, x_n]/I\,\mathbb{K}[x_1, \ldots, x_n] \cong \mathcal{O}_{\mathbb{A}^n,p}/I\mathcal{O}_{\mathbb{A}^n,p} =: R'.$$

Indeed, R is a local ring with maximal ideal $\overline{\mathfrak{m}} = \langle x_1 - a_1, \ldots, x_n - a_n\rangle/I$. Hence, by the universal property of localization, $R = R_{\overline{\mathfrak{m}}}$. But $R_{\overline{\mathfrak{m}}} \cong R'$ by Exercise 4.2.3. □

Example 4.3.17. 1. In accordance with Example 4.3.13, we have

$$i(y, y - x^r; o) = r.$$

Indeed, by Remark 4.3.16,

$$\mathcal{O}_{\mathbb{A}^2,o}/\langle y, y - x^r\rangle\,\mathcal{O}_{\mathbb{A}^2,o} \cong \mathbb{C}[x, y]/\langle y, y - x^r\rangle \cong \mathbb{C}[x]/\langle x^r\rangle.$$

2. For the transversal cusps in Example 4.3.14, we get

$$i(y^2 - x^3, x^2 - y^3; o) = 4.$$

Indeed, since $1 - xy$ is a unit in $\mathcal{O}_{\mathbb{A}^2,o}$, we have

$$\langle y^2 - x^3, x^2 - y^3\rangle = \langle y^2 - x^3, x^2 - x^3y\rangle = \langle y^2 - x^3, x^2\rangle = \langle y^2, x^2\rangle \subset \mathcal{O}_{\mathbb{A}^2,o},$$

and the result follows as above from Remark 4.3.16. Similarly, for the tangential cusps,

$$i(y^2 - x^3, 2y^2 - x^3; o) = 6$$

since

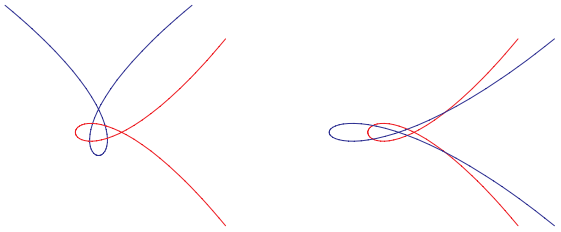
$$\langle y^2 - x^3, 2y^2 - x^3\rangle = \langle y^2, x^3\rangle \subset \mathcal{O}_{\mathbb{A}^2,o}.$$

To see this from the dynamical point of view, consider perturbed equations of type

$$y^2 - (x - c)^2(x + c) = x^2 - (y - d)^2(y + d) = 0$$

respectively

$$y^2 - (x - c)^2(x + c) = 2y^2 - x^2(x + d) = 0:$$



4 intersection points 6 intersection points

□

Since we allow polynomials with multiple factors, it makes sense to extend some of the terminology used when working with curves to the more general case considered here. If $f \in \Bbbk[x,y]$ is a nonconstant polynomial, and $p \in \mathbb{A}^2$ is a point, we say that f **passes through** $\boldsymbol{p}$ if $p \in \mathrm{V}(f)$. If $g \in \Bbbk[x,y]$ is another nonconstant polynomial, we say that f and g **intersect at** $\boldsymbol{p}$ if $p \in \mathrm{V}(f) \cap \mathrm{V}(g)$ (equivalently, both multiplicities $\mathrm{mult}(f,p)$ and $\mathrm{mult}(g,p)$ are ≥ 1). We say that f and g **intersect transversally at** $\boldsymbol{p}$ if $\mathrm{mult}(f,p) = \mathrm{mult}(g,p) = 1$ and the tangent line to f at p is different from the tangent line to g at p. Finally, if

$$f = \prod_{i=1}^{r} f_i^{e_i} \in \mathbb{K}[x,y]$$

is the decomposition of f into pairwise different irreducible factors f_i over $\mathbb{K}$, then each f_i is a **component of** $\boldsymbol{f}$, and e_i is the **multiplicity** of the component f_i.

Theorem 4.3.18 (Properties of Intersection Multiplicities). *Let $f, g \in \Bbbk[x,y]$ be nonconstant polynomials, and let $p = (a,b) \in \mathbb{A}^2$ be a point. Then:*

1. *$i(f,g;p) = 0$ iff f and g do not intersect at p.*
2. *$i(f,g;p) = \infty$ iff f and g have a common component passing through p.*
3. *$i(f,g;p) \geq \mathrm{mult}(f,p) \cdot \mathrm{mult}(g,p)$, with equality occuring iff f and g have no tangent line in common at p.*
4. *$i(f,g;p) = 1$ iff f and g intersect transversally at p.*
5. *$i(f,g;p) = i(g,f;p)$.*
6. *$i(f,g+hf;p) = i(f,g;p)$ for all $h \in \Bbbk[x,y]$.*
7. *If f is irreducible, and p is a smooth point of $C = \mathrm{V}(f) \subset \mathbb{A}^2$, then $i(f,g;p) = v_{C,p}(\overline{g})$, where $\overline{g} \in \mathbb{K}[C] \subset \mathcal{O}_{C,p}$ is the residue class of g.*
8. *$i(f,gh;p) = i(f,g;p) + i(f,h;p)$ for all $f,g,h \in \Bbbk[x,y]$.*

Proof. Parts 5 and 6 immediately follow from the definition. To show the remaining parts, we may suppose that all the components of f and g pass through p. Indeed, the other components are units in $\mathcal{O}_{\mathbb{A}^2,p}$ and do, hence, not contribute to $i(f,g;p)$. For simplicity, we write $\mathcal{O}_p = \mathcal{O}_{\mathbb{A}^2,p}$ and $\mathfrak{m}_p = \mathfrak{m}_{\mathbb{A}^2,p}$.

1. According to our definition, $i(f,g;p) = 0$ iff $\langle f,g\rangle \mathcal{O}_p = \mathcal{O}_p$. This, in turn, means that either f or g is a unit in $\mathcal{O}_p$ and, thus, that $p \notin \mathrm{V}(f) \cap \mathrm{V}(g)$.

2. If f and g have a common component h, then $\langle f,g\rangle \mathcal{O}_p \subset \langle h\rangle \mathcal{O}_p \subsetneq \mathcal{O}_p$. Hence, $i(f,g;p) \geq \dim_{\mathbb{K}} \mathcal{O}_p/\langle h\rangle \mathcal{O}_p$, and it suffices to show that the quotient of $\mathcal{O}_p$ modulo a proper principal ideal has infinite $\mathbb{K}$-dimension. We postpone the proof of this until we have formulated a version of Macaulay's Theorem 2.3.5 which holds in the ring $\mathcal{O}_p$. See Remark 4.4.24 in the next section.

For the converse, suppose that f and g have no common component. Then $\dim_{\mathbb{K}} \mathbb{K}[x,y]/\langle f,g\rangle$ is finite by Exercises 1.7.13 and 1.6.5. In particular, there is a unique $\langle x-a, y-b\rangle$-primary component of $\langle f,g\rangle \subset \mathbb{K}[x,y]$, which we denote by I. Then $\mathcal{O}_p/\langle f,g\rangle \mathcal{O}_p = \mathcal{O}_p/I\mathcal{O}_p$ (we will see this in Exercise 4.5.5, where

we will study the behavior of primary decompositions under localization). Since, in turn, $\mathcal{O}_p/I\,\mathcal{O}_p \cong \mathbb{K}[x,y]/I$ by Remark 4.3.16, we conclude that $i(f,g;p) = \dim_{\mathbb{K}} \mathbb{K}[x,y]/I \leq \dim_{\mathbb{K}} \mathbb{K}[x,y]/\langle f,g\rangle < \infty$, as desired.

3. We will prove this part towards the end of the next section using Gröbner bases in the local case.

4. This special case of part 3 is easy to do directly. Indeed, applying Nakayama's lemma as in the proof of Corollary 4.2.20, we get: $i(f,g;p) = 1 \iff \langle f,g\rangle = \mathfrak{m}_p \iff \langle f,g\rangle + \mathfrak{m}_p^2 = \mathfrak{m}_p \iff \operatorname{span}(d_pf + \mathfrak{m}_p^2, d_pg + \mathfrak{m}_p^2) = \mathfrak{m}_p/\mathfrak{m}_p^2$. Since $\mathfrak{m}_p/\mathfrak{m}_p^2$ is a two dimensional $\mathbb{K}$-vector space, $i(f,g;p) = 1$ iff d_pf and d_pg are $\mathbb{K}$-linearly independent, that is, iff C and D are smooth in p with different tangent lines.

7. According to our assumptions in this part, $\mathcal{O}_{C,p}$ is a DVR, with corresponding discrete valuation $v_{C,p}$ on $\mathbb{K}(C)$. Hence,

$$\mathcal{O}_p/\langle f,g\rangle\,\mathcal{O}_p \cong \mathcal{O}_{C,p}/\langle \overline{g}\rangle \cong \mathcal{O}_{C,p}/\langle t^k\rangle,$$

where $k = v_{C,p}(\overline{g})$. This shows the result since $\dim_{\mathbb{K}} \mathcal{O}_{C,p}/\langle t^k\rangle = k$ by Exercise 4.3.10.

8. Since the assertion follows from part 2 otherwise, we may suppose that f and gh have no common component. Consider, then, the sequence

$$0 \to \mathcal{O}_p/\langle f,h\rangle\,\mathcal{O}_p \xrightarrow{\phi} \mathcal{O}_p/\langle f,gh\rangle\,\mathcal{O}_p \xrightarrow{\psi} \mathcal{O}_p/\langle f,g\rangle\,\mathcal{O}_p \to 0, \tag{4.4}$$

where ϕ is multiplication by g and ψ is induced by the identity on $\mathcal{O}_p$. By Exercise 2.8.4 on the additive behavior of $\mathbb{K}$-dimension, we are done if we show that (4.4) is exact.

For this, note that the syzygies on f,g over $\mathcal{O}_p$ are generated by the trivial syzygy $(g,-f)^t \in \mathcal{O}_p^2$. Indeed, given an $\mathcal{O}_p$-linear relation $Af+Bg=0$, choose a polynomial $u \in \mathbb{K}[x,y]$ with $u(p)=0$, and such that $a := uA \in \mathbb{K}[x,y]$ and $b := uB \in \mathbb{K}[x,y]$. Then $af+bg = 0 \in \mathbb{K}[x,y]$. Since $\mathbb{K}[x,y]$ is a UFD and f and g have no common component, b must be a multiple of f, so that $-b = cf$ for some $c \in \mathbb{K}[x,y]$. Then $(a,b)^t = c\cdot(g,-f)^t \in \mathbb{K}[x,y]^2$ and, thus, $(A,B)^t = C\cdot(g,-f)^t \in \mathcal{O}_p^2$, where $C = c/u$.

It follows that ϕ is injective: if $bg \in \langle f,gh\rangle\,\mathcal{O}_p$, say $bg = af + cgh$ with $a,c \in \mathcal{O}_p$, then $(a,-b+ch)^t$ is a syzygy on f,g, so that $b - ch \in f\mathcal{O}_p$ and, thus, $b \in \langle f,h\rangle\,\mathcal{O}_p$. Since, furthermore, ψ is surjective by its very definition, it remains to show that $\operatorname{im}\phi = \ker\psi$. This is completely straightforward and we leave it to the reader. □

Note that it are properties 6 and 8 which force us to allow polynomials with multiple factors in our definitions and statements. These properties are useful in that they often enable us to simplify the computation of intersection numbers. Let us, for instance, rewrite the last computation in Example 4.3.17. Property 6 (with the help of property 5) gives $i(y^2-x^3, 2y^2-x^3; o) = i(y^2, x^3; o)$. But $i(y^2,x^3;o) = 6$ by property 8. □

Exercise* **4.3.19.** Let $f \in \Bbbk[x,y]$ be a square-free polynomial, let $C = \mathrm{V}(f) \subset \mathbb{A}^2$ be the corresponding plane curve, and let $p \in C$ be a point.

1. Suppose that p is a double point at which C has precisely one tangent line L. Show that, then, $i(C,L;p) \geq 3$. We say that p is a **cusp** of C if $i(C,L;p) = 3$.
2. If p is the origin, and L is the x-axis, show that p is a cusp of C with tangent line L iff f is of type $f = ay^2 + bx^3 +$ other terms of degree ≥ 3, where $ab \neq 0$. □

4.4 Gröbner Bases in the Local Case

In this section, we will adjust the concept of Gröbner bases and Buchberger's algorithm to computations in the local ring of $\mathbb{A}^n$ at a given point of $\mathbb{A}^n$. This will, in particular, allow us to compute intersection multiplicities via Gröbner bases.

For our purposes, it is enough to consider the case where the given point is the origin $o \in \mathbb{A}^n$. Indeed, if $p = (a_1, \ldots, a_n) \in \mathbb{A}^n$ is any point, we may translate p to o (on the level of rings, we have the isomorphism $\mathcal{O}_{\mathbb{A}^n,p} \cong \mathcal{O}_{\mathbb{A}^n,o}$ which extends the substitution homomorphism $\mathbb{K}[x_1,\ldots,x_n] \to \mathbb{K}[x_1,\ldots,x_n],\ x_i \mapsto x_i - a_i$). As usual, $\Bbbk \subset \mathbb{K}$ will be the ground field over which the generators of the ideals under consideration (and the originally given point p) are defined. Taking into account that Remark 2.7.1 on field extensions applies to the adjusted version of Buchberger's algorithm, too, we will be concerned with computations in the local ring

$$\mathcal{O}_o = \Bbbk[x_1,\ldots,x_n]_{\langle x_1,\ldots,x_n\rangle}.$$

Note that every ideal I of $\mathcal{O}_o$ can be generated by polynomials (choose any finite set of generators and clear denominators). Starting from a set of polynomial generators for I, the adjusted version of Buchberger's algorithm will compute a Gröbner basis for I consisting of polynomials, too. In fact, all computations in Buchberger's test will take place in the polynomial ring.

Reflecting the significance of the lowest degree terms of a polynomial f for local studies (as indicated by our treatment of singular points in the preceeding section), we will pick the leading term of f from among those terms. One way of making this precise would be to choose a degree-compatible monomial order such as the degree reverse lexicographic order, and pick the *least* term of f as the leading term. Pursuing an alternative approach, we will make use of monomial orders which are **degree-anticompatible**:

$$\deg x^\alpha < \deg x^\beta \Longrightarrow x^\alpha > x^\beta.$$

Example 4.4.1. The **local degree reverse lexicographic order** $>_{\mathrm{ldrlex}}$ on $\Bbbk[x_1,\ldots,x_n]$ is defined by setting

$$x^\alpha >_{\mathrm{ldrlex}} x^\beta \iff \deg x^\alpha < \deg x^\beta, \text{ or } (\deg x^\alpha = \deg x^\beta \text{ and the last nonzero entry of } \alpha - \beta \in \mathbb{Z}^n \text{ is negative}).$$ □

A degree-anticompatible monomial order such as $>_{\mathrm{ldrlex}}$ is never global. It is, in fact, local in the following sense:

Definition 4.4.2. A monomial order on $\Bbbk[x_1, \ldots, x_n]$ is **local** if

$$x_i < 1 \quad \text{for} \quad i = 1, \ldots, n.$$ □

Example 4.4.3. A weight order $>_w$ on $\Bbbk[x_1, \ldots, x_n]$ is local iff the coefficients of w are strictly negative. □

Remark 4.4.4. Given a local monomial order $>$ on $\Bbbk[x_1, \ldots, x_n]$, a polynomial $u \in \Bbbk[x_1, \ldots, x_n]$ is a unit in $\mathcal{O}_o$ iff its leading monomial is 1. □

A drawback of local monomial orders is that they are not Artinian. As a consequence, the usual division process may not terminate. This is illustrated by Example 2.2.9 which we revisit now:

Example 4.4.5. In the case of one variable x, there is precisely one local monomial order:

$$1 > x > x^2 > \cdots$$

Dividing $g = x$ by $f_1 = x - x^2$ with respect to this order, we successively get the expressions $g = 1 \cdot f_1 + x^2$, $x^2 = x \cdot f_1 + x^3, \ldots$. This may be interpreted by saying that the result of the division process, computed in *infinitely* many steps, is a standard expression whose quotient g_1 is the formal power series $\sum_{k=0}^{\infty} x^k$:

$$g = g_1 \cdot f_1 + 0 \in \Bbbk[[x]], \quad \text{where} \quad g_1 = \sum_{k=0}^{\infty} x^k. \tag{4.5}$$

On the other hand, expressing the fact that $1 - x$ is a multiplicative inverse to $\sum_{k=0}^{\infty} x^k$ in $\Bbbk[[x]]$, we have the **formal geometric series expansion**

$$\frac{1}{1-x} = \sum_{k=0}^{\infty} x^k.$$

We may, hence, rewrite (4.5) in a form which makes sense as an equation in the ring we are actually interested in:

$$g = \frac{1}{1-x} \cdot f_1 + 0 \in \Bbbk[x]_{\langle x \rangle}.$$

Multiplying both sides above by the unit $u = 1 - x \in \Bbbk[x]_{\langle x \rangle}$, we get the expression

$$u \cdot g = 1 \cdot f_1 + 0 \in \Bbbk[x] \tag{4.6}$$

which involves polynomials only. □

In what follows, we will discuss a division algorithm, designed by Mora (1982), which computes standard expressions such as (4.6). Based on this, we will formulate a version of Buchberger's criterion for $\mathcal{O}_o$. To prove the criterion, we will reduce to Buchberger's criterion for the formal power series ring $\Bbbk[[x_1, \ldots, x_n]]$ (which, in turn, will be proved as in the polynomial case). Setting the stage for the reduction, we treat, now, power series expansion in general: given $f \in \mathcal{O}_o$, write f as a fraction of type $g/(1-h)$, with polynomials $g \in \Bbbk[x_1, \ldots, x_n]$ and $h \in \langle x_1, \ldots, x_n \rangle$, and set

$$f = \frac{g}{1-h} = g \sum_{k=0}^{\infty} h^k. \tag{4.7}$$

The crucial point is that the right hand side of (4.7) makes sense as an element of $\Bbbk[[x_1, \ldots, x_n]]$. To verify this, we use a bit of topology.

Remark-Definition 4.4.6. Given any ring R and any ideal $\mathfrak{m}$ of R, it makes sense to define the **$\mathfrak{m}$-adic topology** on R by taking the cosets $f + \mathfrak{m}^k$ as a basis, where $f \in R$ and $k \geq 0$. The $\mathfrak{m}$-adic topology is Hausdorff iff $\bigcap_{k=0}^{\infty} \mathfrak{m}^k = \langle 0 \rangle$. Due to Krull's intersection theorem, this condition is, in particular, fulfilled if R is a local Noetherian ring with maximal ideal $\mathfrak{m}$. □

If we endow a ring R with the $\mathfrak{m}$-adic topology for some ideal $\mathfrak{m} \subset R$, we say that a sequence $(f_\nu) \subset R$ is a **Cauchy sequence** if for every $k \geq 0$, there exists a number ν_0 such that $f_\nu - f_\mu \in \mathfrak{m}^k$ for all $\nu, \mu \geq \nu_0$. In the same spirit, a **sequence** $(f_\nu) \subset R$ is called **convergent**, with **limes** f, if for every $k \geq 0$, there exists a number ν_0 such that $f_\nu - f \in \mathfrak{m}^k$ for all $\nu \geq \nu_0$. A **series** $\sum_{\nu=0}^{\infty} f_\nu$ in R is **convergent** if the sequence formed by its partial sums is convergent. If the $\mathfrak{m}$-adic topology is Hausdorff, every convergent sequence (f_ν) has a unique limes, denoted $\lim_{\nu \to \infty} f_\nu$. In particular, every convergent series constitutes, then, an element of R.

Definition 4.4.7. Given a ring R and an ideal $\mathfrak{m}$ of R, we say that R is **complete with respect to $\mathfrak{m}$** if the $\mathfrak{m}$-adic topology is Hausdorff, and if every Cauchy sequence converges. □

Proposition 4.4.8. *Let $\mathfrak{m} = \langle x_1, \ldots, x_n \rangle \subset \Bbbk[[x_1, \ldots, x_n]]$. Then:*

1. *The $\mathfrak{m}$-adic topology on $\Bbbk[[x_1, \ldots, x_n]]$ is Hausdorff:*

$$\bigcap_{k=0}^{\infty} \mathfrak{m}^k = \langle 0 \rangle.$$

2. *$\Bbbk[[x_1, \ldots, x_n]]$ is complete with respect to $\mathfrak{m}$.*
3. *A series $\sum_{\nu=0}^{\infty} f_\nu$ in $\Bbbk[[x_1, \ldots, x_n]]$ converges with respect to the $\mathfrak{m}$-adic topology iff $\lim_{\nu \to \infty} f_\nu = 0$.*
4. *$\Bbbk[[x_1, \ldots, x_n]]$ is a local ring with maximal ideal $\mathfrak{m}$.*

5. *There is a natural embedding of local rings $\mathcal{O}_o \subset \Bbbk[[x_1, \ldots, x_n]]$ defined by power series expansion. The image of the maximal ideal of $\mathcal{O}_o$ under this embedding is contained in the maimal ideal $\mathfrak{m}$.*

Proof. 1. This is clear: if the power series $f = \sum a_\alpha x^\alpha$ is contained in $\mathfrak{m}^k$, then $a_\alpha = 0$ for all α with $|\alpha| < k$.

2. Given a Cauchy sequence $(f_\nu) = \left(\sum a_\alpha^{(\nu)} x^\alpha\right) \subset \Bbbk[[x_1, \ldots, x_n]]$, define $f = \sum a_\alpha x^\alpha \in \Bbbk[[x_1, \ldots, x_n]]$ as follows: for each $k \geq 1$, pick a number ν_0 such that $f_\nu - f_\mu \in \mathfrak{m}^k$ for all $\nu, \mu \geq \nu_0$, and set $a_\alpha = a_\alpha^{(\nu_0)}$ for all α with $|\alpha| = k - 1$. Then $f = \lim_{\nu \to \infty} f_\nu$.

3. This follows from part 2: the sequence formed by the partial sums of $\sum_{\nu=0}^{\infty} f_\nu$ is a Cauchy sequence iff $\lim_{\nu \to \infty} f_\nu = 0$.

4. We have to show that each element $f \in \Bbbk[[x_1, \ldots, x_n]] \setminus \mathfrak{m}$ is a unit in $\Bbbk[[x_1, \ldots, x_n]]$. For this, write $f = a_0 - h$, with $0 \neq a_0 \in \Bbbk$ and $h \in \mathfrak{m}$, and expand:

$$\frac{1}{a_0 - h} = \frac{1}{a_0} \sum_{k=0}^{\infty} (\frac{h}{a_0})^k.$$

Then, by part 3, the series on the right hand side converges and defines, thus, a multiplicative inverse to f.

5. This follows similarly: it is, now, clear that the series on the right hand side of (4.7) constitutes an element of $\Bbbk[[x_1, \ldots, x_n]]$. □

Exercise* **4.4.9.** Let S be a ring which is complete with respect to some ideal $\mathfrak{m}$. Given $s_1, \ldots, s_n \in \mathfrak{m}$, show that there exists a unique homomorphism $\Phi : \Bbbk[[x_1, \ldots, x_n]] \to S$ such that $\Phi(x_i) = s_i$ for all i. In fact, Φ is the map which sends a a power series f to the series $f(s_1, \ldots, s_n) \in S$. As in the polynomial case, we refer to Φ as a **substitution homomorphism**. □

We, now, come to division with remainder and Gröbner bases in $\Bbbk[[x_1, \ldots, x_n]]$. This topic is of theoretical interest and was first considered by Hironaka (1964) and, independently, Grauert (1972) who used the name **standard basis** instead of Gröbner basis. Our terminology will be the same as in Chapter 2. For instance, if $0 \neq f = \sum_{\alpha \in \mathbb{N}^n} a_\alpha x^\alpha \in \Bbbk[[x_1, \ldots, x_n]]$, we call any $a_\alpha x^\alpha$ with $a_\alpha \neq 0$ a **term** of f. And, given a local monomial order $>$ on $\Bbbk[x_1, \ldots, x_n] \subset \Bbbk[[x_1, \ldots, x_n]]$, we define the **leading term** of f, written $\mathbf{L}(f) = \mathbf{L}_>(f)$, to be the largest term of f. This makes sense since every nonempty set X of monomials in $\Bbbk[x_1, \ldots, x_n]$ has a *largest* element with respect to the *local* order $>$. Indeed, arguing as in the proof of Proposition 2.2.10, we may take the largest element of a finite set of monomial generators for the ideal $\langle X \rangle \subset \Bbbk[x_1, \ldots, x_n]$. As usual, $\mathbf{L}_>(0) = \mathbf{L}(0) = 0$.

Since a global monomial order $>$ is Artinian, there is no sequence $(m_\nu)_{\nu \in \mathbb{N}}$ of monomials m_ν such that $m_1 > m_2 > \cdots$. In the local case, we have instead:

Lemma 4.4.10. *Let $\mathfrak{m} = \langle x_1, \ldots, x_n \rangle$ be the maximal ideal of $\Bbbk[[x_1, \ldots, x_n]]$, and let $>$ be a local monomial order on $\Bbbk[x_1, \ldots, x_n] \subset \Bbbk[[x_1, \ldots, x_n]]$.*

1. *If $(m_\nu)_{\nu\in\mathbb{N}}$ is a sequence of monomials in $\Bbbk[x_1,\ldots,x_n]$ such that $m_1 > m_2 > \cdots$, then $\lim_{\nu\to\infty} m_\nu = 0$ with respect to the $\mathfrak{m}$-adic topology.*
2. *If $>$ is a local weight order $>_w$, and $(f_\nu)_{\nu\in\mathbb{N}}$ is a sequence of formal power series in $\Bbbk[[x_1,\ldots,x_n]]$, then, with respect to the $\mathfrak{m}$-adic topology, we have:*

$$\lim_{\nu\to\infty} \mathbf{L}_{>_w}(f_\nu) = 0 \implies \lim_{\nu\to\infty} f_\nu = 0$$

□

Proof. Given k, only finitely many of the monomials in $\Bbbk[x_1,\ldots,x_n]$ are not contained in $\mathfrak{m}^k$. In particular, there is an integer ν_0 such that $m_\nu \in \mathfrak{m}^k$ for all $\nu \geq \nu_0$. This shows part 1. For part 2, set

$$r = \min\{w(m) \mid m \text{ a monomial such that } m \notin \mathfrak{m}^k\}.$$

Then, if $\lim_{\nu\to\infty} \mathbf{L}_{>_w}(f_\nu) = 0$, there is a number ν_1 such that $w(\mathbf{L}_{>_w}(f_\nu)) < r$ for all $\nu \geq \nu_1$ (indeed, the coefficients of w are strictly negative by assumption). We conclude that $f_\nu \in \mathfrak{m}^k$ for all $\nu \geq \nu_1$, as desired. □

Theorem 4.4.11 (Grauert's Division Theorem). *Let $>$ be a local monomial order on $\Bbbk[x_1,\ldots,x_n]$, write $R = \Bbbk[[x_1,\ldots,x_n]]$, and let $f_1,\ldots,f_r \in R\setminus\{0\}$. For every $g \in R$, there exists a uniquely determined expression*

$$g = g_1 f_1 + \ldots + g_r f_r + h, \text{ with } g_1,\ldots,g_r,h \in R,$$

and such that:

(DD1) For $i > j$, no term of $g_i\,\mathbf{L}(f_i)$ is divisible by $\mathbf{L}(f_j)$.
(DD2) For all i, no term of h is divisible by $\mathbf{L}(f_i)$.

This expression is called a **Grauert standard expression** *for g with* **remainder** *h (in terms of the f_i, with respect to $>$).*

Proof. The *uniqueness* follows as in the polynomial case (see Theorem 2.2.12). For the *existence*, we first note that as in the polynomial case, the result clearly holds if $f_1,\ldots,f_r$ are terms. In the general case, we get, thus, a unique expression

$$g^{(0)} := g = \sum_{j=1}^{r} g_j^{(0)}\,\mathbf{L}(f_j) + h^{(0)}$$

satisfying conditions (DD1) and (DD2). Then either $g^{(1)} := g - \sum_{j=1}^{r} g_j^{(0)} f_j - h^{(0)}$ is zero, and we are done, or $\mathbf{L}(g^{(0)}) > \mathbf{L}(g^{(1)})$. Recursively, we are either done in finitely many steps, or we get sequences $(g^{(\nu)})$, $(g_j^{(\nu)})$, $j = 0,\ldots,r$, and $(h^{(\nu)})$ of formal power series such that, for all ν,

$$g^{(\nu+1)} = g - \sum_{j=1}^{r}\sum_{\mu=1}^{\nu} g_j^{(\mu)} f_j - \sum_{\mu=1}^{\nu} h^{(\mu)}.$$

In the latter case, the result will follow once we show that all our sequences converge to zero with respect to the $\langle x_1, \ldots, x_n \rangle$-adic topology on $\Bbbk[[x_1, \ldots, x_n]]$. For this, consider the monomial ideals $I_j \subset \Bbbk[x_1, \ldots, x_n]$ generated by all terms of f_j except the $\mathbf{L}(f_j)$, $j = 1, \ldots, r$. For each j, let X_j consist of the minimal (monomial) generators for I_j together with $\mathbf{L}(f_j)$. Then $X := \bigcup X_j$ is a finite set of monomials. By Exercise 2.2.11, there exists a local weight order $>_w$ on $\Bbbk[x_1, \ldots, x_n]$ which coincides on X with the given local order $>$. Due to our construction of X, we have $\mathbf{L}_{>_w}(f_j) = \mathbf{L}_>(f_j)$ for all j. Hence, repeating the division process above with $>$ replaced by $>_w$, we get the same sequences $(g^{(\nu)})$, $(g_j^{(\nu)})$, and $(h^{(\nu)})$.

Since $\mathbf{L}(g^{(0)}) > \mathbf{L}(g^{(1)}) > \ldots$, we have $\lim_{\nu\to\infty} \mathbf{L}(g^{(\nu)}) = 0$ by part 1 of Lemma 4.4.10. Then also $\lim_{\nu\to\infty} \mathbf{L}(g_j^{(\nu)}) = 0$ and $\lim_{\nu\to\infty} \mathbf{L}(h^{(\nu)}) = 0$ since $\mathbf{L}(g^{(\nu)}) \geq_w \mathbf{L}(g_j^{(\nu)} f_j) = \mathbf{L}(g_j^{(\nu)})\mathbf{L}(f_j)$ and $\mathbf{L}(g^{(\nu)}) \geq_w \mathbf{L}(h^{(\nu)})$ for all ν. We are, thus, done by part 2 of Lemma 4.4.10. □

Leading ideals, **standard monomials**, and **Gröbner bases** for ideals in $\Bbbk[[x_1, \ldots, x_n]]$ are defined as for ideals in $\Bbbk[x_1, \ldots, x_n]$. Making use of Gordan's lemma as in the polynomial case is one way of showing that $\Bbbk[[x_1, \ldots, x_n]]$ **is Noetherian**. Furthermore, we have the following variant of Macaulay's Theorem 2.3.5:

Proposition 4.4.12. *Let $I \subset \Bbbk[[x_1, \ldots, x_n]] =: R$ be an ideal, and let $>$ be a local monomial order on $\Bbbk[x_1, \ldots, x_n]$. Then:*

1. *The standard monomials represent $\Bbbk$-linearly independent elements of R/I, and their residue classes generate a subspace of R/I which is dense with respect to the $\mathfrak{m}_{R/I}$-adic topology, where $\mathfrak{m}_{R/I}$ is the maximal ideal of R/I.*
2. *If $\dim_\Bbbk R/I < \infty$, the standard monomials represent a $\Bbbk$-vector space basis for R/I.*

Proof. 1. Let

$$\mathcal{B} := \{m + I \mid m \in R \text{ a standard monomial}\} \subset R/I,$$

and let W be the subspace of R/I generated by the elements of $\mathcal{B}$. Arguing as in the proof of Macaulay's Theorem 2.3.5, we find:

(a) The elements of $\mathcal{B}$ are $\Bbbk$-linearly independent.
(b) Given a power series $g \in R$, there is a power series $h = \sum_\alpha b_\alpha x^\alpha \in R$ whose terms involve only standard monomials, and such that $g + I = h + I$. In fact, h is uniquely determined by g, I, and $>$ as the remainder in a Grauert standard expression $g = \sum_{i=1}^r g_i f_i + h$, where $f_1, \ldots, f_r$ is any Gröbner basis for I.

Statement (a) is precisely the first assertion of part 1 of the proposition. To show that W is dense in R/I, we note that in the situation of (b), given an

integer $k \geq 0$, we have $h - \sum_{|\alpha|<k} b_\alpha x^\alpha \in \mathfrak{m}^k$, where $\mathfrak{m}$ is the maximal ideal of R. Hence, $g \equiv \sum_{|\alpha|<k} b_\alpha x^\alpha \mod I + \mathfrak{m}_{R/I}^k$, as desired.

If $\dim_{\Bbbk} R/I < \infty$, there are only finitely many standard monomials by (a). Hence, given $g \in R$, any power series h as in (b) is, in fact, a polynomial. Together with (a), this shows part 2. □

Definition 4.4.13. As in the polynomial case, we call the remainder h in the proof above the **normal form** of g mod I. □

Finally, we have a version of Buchberger's criterion for $\Bbbk[[x_1, \ldots, x_n]]$ whose statement and proof read word for word identically to what we did in the polynomial case (in particular, in the statement of the criterion, it is enough to consider standard expressions in the weak sense of Remark 2.2.16). We leave the details to the reader:

Exercise* **4.4.14.** Let $R = \Bbbk[[x_1, \ldots, x_n]]$.

1. Formulate and prove versions of Grauert's division theorem and Buchberger's criterion for free R-modules.
2. Show that Hilbert's syzygy theorem holds for R: Every finitely generated R-module M has a finite free resolution of length at most n, by finitely generated free R-modules. □

As is already clear from Example 4.4.5, this does not give us an algorithm for computing Gröbner bases in power series rings: even if we start with polynomials, the remainder on Grauert division may be a power series, and it may take infinitely many steps to compute this series.

Next, we turn from $\Bbbk[[x_1, \ldots, x_n]]$ to $\mathcal{O}_o$. To begin with, we show by example that the strong condition (DD2) of Grauert's division theorem cannot always be achieved in $\mathcal{O}_o$:

Example 4.4.15. Consider the polynomials $f = x$ and $f_1 = x - x^2 - y$ in $\Bbbk[x, y] \subset \Bbbk[[x, y]]$, and fix a local monomial order $>$ on $\Bbbk[x, y]$ such that $\mathbf{L}(f_1) = x$ (for instance, take $>_{\mathrm{ldrlex}}$). Suppose there is a standard expression $x = g_1 f_1 + h$ as in Grauert's division theorem, with $g_1, h \in \Bbbk[x, y]_{\langle x,y\rangle}$. Then no term of the remainder h is divisible by $\mathbf{L}(f_1) = x$. That is, $h \in \Bbbk[y]_{\langle y\rangle}$. This implies that $x = \mathbf{L}(x) = \mathbf{L}(g_1 f_1) = \mathbf{L}(g_1) \cdot x$ and, thus, that g_1 is a unit in $\Bbbk[x, y]_{\langle x,y\rangle}$ (that is, $g(0, 0) \neq 0$). Furthermore, substituting h for x in $x = g_1 f_1 + h$, we get the equality

$$g_1(h, y) \cdot (h - h^2 - y) = 0 \in \Bbbk[y]_{\langle y\rangle}.$$

On the other hand, since f and f_1 vanish at the origin, h cannot have a constant term. It follows that $g_1(h, y) \neq 0$ since $g(0, 0) \neq 0$. We conclude that

$$h - h^2 - y = 0. \tag{4.8}$$

This is impossible since regarding (4.8) as a quadratic equation in h and solving it, we do not get a rational function: $h = \frac{1 \pm \sqrt{1-4y}}{2}$. Arguing more

formally (supposing that h does exist as a rational function), write h as a fraction $h = \frac{h_1}{1+h_2}$, with polynomials $h_1 \in \Bbbk[y]$ and $h_2 \in \langle y \rangle \subset \Bbbk[y]$. Then, from (4.8), we obtain

$$(1 + h_2) \cdot h_1 - h_1^2 - y \cdot (1 + h_2)^2 = 0 \in \Bbbk[y]. \tag{4.9}$$

A check on degrees gives a contradiction as follows: If $\deg h_1 \geq 1 + \deg h_2$, then $\deg h_1^2 > 1 + \deg(h_2^2) = \deg(y \cdot (1 + h_2^2))$ and $\deg h_1^2 > \deg((1 + h_2) \cdot h_1)$. If $\deg h_2 \geq \deg h_1$, then $\deg((1 + h_2^2) \cdot y) > \deg((1 + h_2) \cdot h_1) \geq \deg h_1^2$. Hence, in both cases, the degree of one of the three summands on the left hand side of (4.9) is strictly larger than the degree of any other summand, absurd. □

Our discussion of division with remainder and Gröbner bases in $\mathcal{O}_o$ is motivated by what we did in Example 4.4.5. Taking additionally into account that every ideal in $\mathcal{O}_o$ is generated by polynomials, our statements will be formulated such that they involve polynomial data only.

Theorem 4.4.16 (Mora's Division Theorem). *Let $>$ be a monomial order on $\Bbbk[x_1, \ldots, x_n]$, and let $f_1, \ldots, f_r \in \Bbbk[x_1, \ldots, x_n] \setminus \{0\}$. For every $g \in \Bbbk[x_1, \ldots, x_n]$, there exists an expression*

$$u \cdot g = g_1 f_1 + \ldots + g_r f_r + h,$$

where $u, g_1, \ldots, g_r, h \in \Bbbk[x_1, \ldots, x_n]$, with $\mathbf{L}(u) = 1$, and such that:

(ID1) $\mathbf{L}(g) \geq \mathbf{L}(g_i f_i)$ *whenever both sides are nonzero.*
(ID2) *If h is nonzero, then $\mathbf{L}(h)$ is not divisible by any $\mathbf{L}(f_i)$.*

Every such expression is called a **Mora standard expression** *for g with* **remainder** *h (in terms of the f_i, with respect to $>$).* □

The proof of the theorem consists of an algorithm for computing Mora standard expressions. In comparison with the division algorithms discussed in Chapter 2, the crucial new idea of Mora is to not only divide by $f_1, \ldots, f_r$, but also by some of the intermediate dividends. To decide whether an intermediate dividend should be stored as a possible divisor for division steps still to come, its ecart will be computed.

Definition 4.4.17. Let $>$ be a monomial order on $\Bbbk[x_1, \ldots, x_n]$. Given a nonzero polynomial $f \in \Bbbk[x_1, \ldots, x_n]$, the **ecart** of f (with respect to $>$), written $\operatorname{ecart}(f)$, is defined to be

$$\operatorname{ecart}(f) = \deg f - \deg \mathbf{L}(f).$$

□

In stating Mora's division algorithm, we focus on the computation of the remainder h. How to compute the unit u and the quotients g_i (this requires some extra bookkeeping) will be described in the correctness argument given in the proof below.

Algorithm 4.4.18 (Mora's Division Algorithm). *Let $>$ be a monomial order on $\Bbbk[x_1,\dots,x_n]$. Given nonzero polynomials $g, f_1,\dots,f_r \in \Bbbk[x_1,\dots,x_n]$, compute a remainder h of g on Mora division by $f_1,\dots,f_r$.*

1. *Set $h := g$ and $D := \{f_1,\dots,f_r\}$.*
2. *`while`* $\big(h \neq 0$ *and* $D(h) := \{f \in D \mid \mathbf{L}(h)$ *is divisible by* $\mathbf{L}(f)\} \neq \emptyset\big)$
   - *choose $f \in D(h)$ with* $\operatorname{ecart}(f)$ *minimal;*
   - *`if`* $(\operatorname{ecart}(f) > \operatorname{ecart}(h))$ *`then`* $D := D \cup \{h\}$*;*
   - *set* $h := h - \frac{\mathbf{L}(h)}{\mathbf{L}(f)} f$.
3. *`return`*(h). □

Remark 4.4.19. 1. If we apply Mora's algorithm to homogeneous polynomials $g, f_1,\dots,f_r$, all polynomials computed in the resulting division process are homogeneous, too. Hence, all ecart's are zero, and Mora's algorithm follows the steps of an indeterminate version of the usual division algorithm. In fact, as shown by the correctness argument in the proof below, the algorithm computes a standard expression of type $g = g_1 f_1 + \ldots + g_r f_r + h$.

2. If $>$ is a global monomial order, and $\mathbf{L}(h)$ is a multiple of $\mathbf{L}(f)$, then $\mathbf{L}(h) \geq \mathbf{L}(f)$. Hence, even if added to D in the division process, h will not be used in further division steps. Thus, we obtain again an indeterminate version of the usual division algorithm, but in the nonhomogeneous case, the freedom of choice is reduced. □

Proof (of termination and correctness). We write D_k and h_k respectively for the set of intermediate divisors and the intermediate dividend after the kth iteration of the `while` loop, starting with $D_0 = D$ and $h_0 = g$.

Termination. We proceed in two steps. In the first step, we show that the set D of divisors will be enlarged in at most finitely many iterations of the `while` loop. Then, taking our cue from the remark above, we homogenize with respect to an extra variable x_0 to reduce to the termination result for the usual division algorithm.

After k iterations, the algorithm continues with the `while` loop iff $0 \neq \mathbf{L}(h_k) \in \langle \mathbf{L}(f) \mid f \in D_k\rangle \subset \Bbbk[x_1,\dots,x_n]$. In this case, h_k is added to D_k iff $x_o^{\operatorname{ecart}(h_k)}\mathbf{L}(h_k)$ is not contained in the monomial ideal

$$I_k = \langle x_o^{\operatorname{ecart}(f)}\mathbf{L}(f) \mid f \in D_k\rangle \subset \Bbbk[x_0,\dots,x_n].$$

By Gordan's lemma, the ascending chain $I_1 \subset I_2 \dots$ is eventually stationary, say $I_N = I_{N+1} = \cdots$ for some N. Then also $D_N = D_{N+1} = \cdots$. Say, $D_N = \{f_1,\dots,f_{r'}\}$.

Termination will follow once we show that after finitely many further iterations, either $h = 0$ or $D(h) = \emptyset$. For this, homogenize h_{N+1} and the f_i with respect to x_0: set

$$H_{N+1} = x_0^{\deg(h_{N+1})} h_{N+1}(x_1/x_0, \dots x_n/x_0) \text{ and}$$

$$F_i = x_0^{\deg(f_i)} f_i(x_1/x_0, \ldots x_n/x_0),\ i = 1, \ldots, r'.$$

On $\Bbbk[x_0, \ldots, x_n]$, consider the monomial order $>_g$ defined by setting

$$x_o^c x^\alpha >_g x_o^d x^\beta \iff \begin{array}{l} \deg x_o^c x^\alpha > \deg x_o^d x^\beta, \text{ or} \\ (\deg x_o^c x^\alpha = \deg x_o^d x^\beta \text{ and } x^\alpha > x^\beta). \end{array}$$

This order is global, and we have $\mathbf{L}_{>_g}(F_i) = x_o^{\mathrm{ecart}(f_i)} \mathbf{L}_>(f_i)$. Thus, if we divide h_{N+1} by the f_i, Mora's algorithm follows the steps of an indeterminate version of the division algorithm, as desired.

Correctness. Recursively, starting with $u_0 = 1$ and $g_i^{(0)} = 0$, $i = 1, \ldots, r$, suppose that, due to the first $k-1$ iterations of the while loop, we already have expressions of type

$$u_\ell \cdot g = g_1^{(\ell)} f_1 + \ldots + g_r^{(\ell)} f_r + h_\ell, \text{ with } \mathbf{L}(u_\ell) = 1,$$

$\ell = 0, \ldots, k-1$. Then, if the test condition for the k-th iteration of the while loop is fulfilled, choose a polynomial $f = f^{(k)}$ as in the statement of the algorithm, and set $h_k = h_{k-1} - m_k f^{(k)}$, where $m_k = \frac{\mathbf{L}(h_{k-1})}{\mathbf{L}(f^{(k)})}$. There are two possibilities: either,

(a) $f^{(k)}$ is one of $f_1, \ldots, f_r$, or
(b) $f^{(k)}$ is one of $h_0, \ldots, h_{k-1}$.

Accordingly, substituting $h_k + m_k f^{(k)}$ for h_{k-1} in the expression for $u_{k-1} \cdot g$, we get an expression of type

$$u_k \cdot g = g_1^{(k)} f_1 + \ldots + g_r^{(k)} f_r + h_k,$$

where either,

(a) $u_k = u_{k-1}$, or
(b) $u_k = u_{k-1} - m_k u_\ell$, for some ℓ.

In any case, $\mathbf{L}(u_k) = \mathbf{L}(u_{k-1}) = 1$ (in case (b), note that $\mathbf{L}(h_l) > \mathbf{L}(h_{k-1}) = \mathbf{L}(m_k \cdot h_\ell) = m_k \cdot \mathbf{L}(h_\ell)$, so that $\mathbf{L}(u_{k-1}) = 1 > m_k = \mathbf{L}(m_k \cdot u_\ell)$). We conclude that, upon termination, the algorithm outputs a Mora standard expression as desired (that the conditions (ID1) and (ID2) are fulfilled is clear). □

Example 4.4.20. Dividing $g = x$ by $f_1 = x - x^2$ with respect to the unique local monomial order on $\Bbbk[x]$, we successively get:

$$h_0 = x,\ D_0 = \{x - x^2\},\ 1 \cdot g = 0 \cdot f_1 + x,$$

$$f^{(1)} = x - x^2,\ D_1 = \{x - x^2, x\},\ h_1 = x^2,\ 1 \cdot g = 1 \cdot f_1 + x^2,$$

and

$$f^{(2)} = x,\ h_1 = 0,\ (1 - x) \cdot g = 1 \cdot f_1 + 0.$$

□

Exercise 4.4.21. Consider $>_{\mathrm{ldrlex}}$ on $\Bbbk[x,y,z]$ and compute a Mora standard expression for $g = x^3y + x^5 + x^2y^2z^2 + z^6$ in terms of $f_1 = x^2 + x^2y$, $f_2 = y^3 + xyz$, $f_3 = x^3y^2 + z^4$. □

We, now, come to Gröbner bases in $\mathcal{O}_o$. Let $>$ be a local monomial order on $\Bbbk[x_1,\ldots,x_n]$. Considering the embedding $\mathcal{O}_o \subset \Bbbk[[x_1,\ldots,x_n]]$, we define the **leading term** of an element $f \in \mathcal{O}_o$, written $\mathbf{L}(f) = \mathbf{L}_>(f)$, to be the leading term of its power series expansion. Given an ideal $I \subset \mathcal{O}_o$, the **leading ideal** of I is the monomial ideal $\mathbf{L}(I) = \mathbf{L}_>(I) \subset \Bbbk[x_1,\ldots,x_n]$ generated by the leading terms of the elements of I. **Standard monomials** and **Gröbner bases** for ideals in $\mathcal{O}_o$ are defined as in the polynomial case. In fact, we ask that the Gröbner basis elements are polynomials (otherwise, clear denominators). Based on Mora Division with remainder, we get the $\mathcal{O}_o$ analog of Buchberger's Criterion 2.3.9:

Theorem 4.4.22 (Buchberger's Criterion for $\mathcal{O}_o$). *Let $>$ be a local monomial order on $\Bbbk[x_1,\ldots,x_n]$, and let $f_1,\ldots,f_r \in \Bbbk[x_1,\ldots,x_n] \setminus \{0\}$. For every $i = 2,\ldots,r$ and every minimal monomial generator x^α for*

$$M_i = \langle \mathbf{L}(f_1),\ldots,\mathbf{L}(f_{i-1})\rangle : \mathbf{L}(f_i) \subset \Bbbk[x_1,\ldots,x_n],$$

choose an S-polynomial $\mathrm{S}(f_i,f_j)$ as in Buchberger's Criterion 2.3.9. Then $f_1,\ldots,f_r$ form a Gröbner basis iff any such $\mathrm{S}(f_i,f_j)$ has a Mora standard expression with remainder zero.

Proof. The condition on the remainders is clearly necessary. It is also sufficient. Indeed, considering the syzygies arising from the Mora standard expressions with remainder zero and arguing as in the proof of Buchberger's criterion 2.3.9, we find for every nonzero $g \in I = \langle f_1,\ldots,f_r\rangle \subset \mathcal{O}_o \subset \Bbbk[[x_1,\ldots,x_n]]$ a Grauert standard expression in terms of the f_k with remainder zero. Hence, $\mathbf{L}(g)$ is divisible by one of the $\mathbf{L}(f_k)$. □

The $\mathcal{O}_o$ analog of Macaulay's Theorem 2.3.5 is part 2 below:

Proposition 4.4.23. *Let $>$ be a local monomial order on $\Bbbk[x_1,\ldots,x_n]$. Then:*

1. *Let I be an ideal of $\mathcal{O}_o$, and let $f_1,\ldots,f_r \in I$ be polynomials. Then the f_k form a Gröbner basis for I iff they form a Gröbner basis for the extended ideal $I\,\Bbbk[[x_1,\ldots,x_n]]$.*
2. *Proposition 4.4.12 on standard monomials remains true if $\Bbbk[[x_1,\ldots,x_n]]$ is replaced by $\mathcal{O}_o$.*

Proof. Let $I^e = I\,\Bbbk[[x_1,\ldots,x_n]]$.

1. The implication from right to left is clear: Since $I \subset I^e$, we also have $\mathbf{L}(I) \subset \mathbf{L}(I^e)$.

Conversely, suppose that the f_k form a Gröbner basis for I. Then $f_1,\ldots,f_r$ generate I and, hence, also I^e. It is, thus, enough to show that the f_k form a

Gröbner basis in $\Bbbk[[x_1,\dots,x_n]]$. By assumption, the f_k satisfy Buchberger's criterion for $\mathcal{O}_o$. That is, we have Mora standard expressions of type

$$u \cdot \mathrm{S}(f_i, f_j) = \sum g_k f_k,$$

where u is a unit in $\mathcal{O}_o$. Multiplying both sides by the power series expansion of the inverse of u, we get a standard expression (in the weak sense of Remark 2.2.16) for $\mathrm{S}(f_i, f_j)$ in $\Bbbk[[x_1,\dots,x_n]]$ with remainder zero. Hence, Buchberger's criterion is satisfied in the power series ring as well.

2. Let I be an ideal of $\mathcal{O}_o$. Given an element $g \in \mathcal{O}_o \subset \Bbbk[[x_1,\dots,x_n]]$, we consider the remainder $h = \sum_\alpha b_\alpha x^\alpha$ in a Grauert standard expression $g = \sum_{i=1}^r g_i f_i + h$, where $f_1,\dots,f_r$ is any Gröbner basis for I (and, thus, also for I^e by part 1). Then, if $\mathfrak{m}_o$ denotes the maximal ideal of $\mathcal{O}_o$, and k is an integer ≥ 0, we can replace h modulo $I + \mathfrak{m}_o^k$ by the polynomial $\sum_{|\alpha|<k} b_\alpha x^\alpha$. Arguing as in the proof of Proposition 4.4.12, we are done. □

The result on standard monomials gives us in particular:

Remark 4.4.24. If $n > 1$, and $\langle f\rangle \subsetneq \mathcal{O}_o$ is a proper principal ideal, then $\dim_\Bbbk \mathcal{O}_o/\langle f\rangle = \infty$ since there are infinitely many standard monomials for $\langle f\rangle$. This concludes the proof of part 2 of Theorem 4.3.18. □

As in Chapter 2, Buchberger's criterion gives us **Buchberger's test** and **Buchberger's algorithm** for computing Gröbner bases (being able to compute remainders, the termination of the algorithm only relies on the ascending chain condition for monomial ideals, but not on the fact that the given order is Artinian; see Corollary 2.3.11).

Exercise 4.4.25. Consider $\Bbbk[x,y]$ with $>_{\mathrm{ldrlex}}$. Compute Gröbner bases for the following ideals:

$$I = \langle x^3 - y^3, x^2y^2\rangle,\ J = \langle x^3 - y^3, x^2y^2 + xy^3\rangle,\ \text{ and }\ K = \langle x^3 - y^4, x^2y^2\rangle.$$

Hint: You should get

$$\{x^3{-}y^3, x^2y^2, y^5\},\ \{x^3{-}y^3, x^2y^2{+}xy^3, xy^4{-}y^5, y^6\},\ \text{ and }\ \{x^3{-}y^4, x^2y^2, y^6\}.$$

In the proof below, we will make use of the ideals I, J, and K to illustrate the main arguments by examples. □

Proof of Theorem 4.3.18, Part 3. Let $f, g \in R = \Bbbk[x,y]$ be nonconstant polynomials, let $m = \mathrm{mult}(f,o)$ and $n = \mathrm{mult}(f,o)$ be their multiplicities at the origin o, and let f_m and g_n be the homogeneous components of f and g of degrees m and n, respectively. We have to show that $i(f,g;o) \geq m \cdot n$, with equality occuring iff f and g have no tangent line in common at o. This is clear if $i(f,g;o) = \infty$. Writing $I_o = \langle f, g\rangle \mathcal{O}_o$, we may, therefore, assume that

$$i(f,g;o) = \dim_\Bbbk \mathcal{O}_o/I_o < \infty. \tag{4.10}$$

By part 2 of Theorem 4.3.18, the geometric meaning of this is that f and g do not have a common component passing through o.

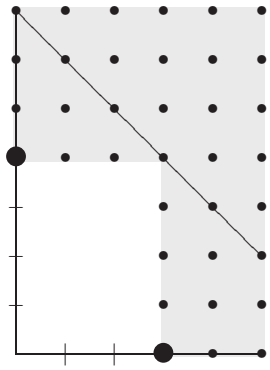
Given any local monomial order on $\Bbbk[x, y]$, it follows from (4.10) and part 2 of Proposition 4.4.23 that $i(f, g; p)$ is precisely the number of standard monomials for I_o. To compute this number, we fix the local degree reverse lexicographic order $>_{\mathrm{ldrlex}}$. Then, since $>_{\mathrm{ldrlex}}$ is degree-anticompatible, the leading terms $\mathbf{L}(f)$ and $\mathbf{L}(g)$ are among the terms of f_m and g_n, respectively. We may, hence, choose the coordinates such that $\mathbf{L}(f) = x^m$ and, then, suppose that $\mathbf{L}(g)$ is of type $\mathbf{L}(g) = x^{\beta_1} y^{\beta_2}$, where $m > \beta_1$ and $\beta_1 + \beta_2 = n$ (subtract a multiple of f from g and adjust constants, if necessary). To proceed, we distinguish two cases.

Case 1: Suppose f and g are homogeneous. That is, $f = f_m$ and $g = g_n$. Then f and g have no common tangent line at o (every such line would be a common component of f and g at o). Hence, in this case, we have to show that the number of standard monomials for I_o is $m \cdot n$.

If $\beta_1 = 0$, we are done right away: Since

$$\mathrm{S}(g, f) \in \langle x, y \rangle^d \subset \langle \mathbf{L}(f), \mathbf{L}(g) \rangle, \tag{4.11}$$

where d is the degree of the "corner" $\mathrm{LCM}(\mathbf{L}(g), \mathbf{L}(f)) = x^m y^n$, the remainder of $\mathrm{S}(g, f)$ on Mora division by f, g is zero. Hence, f, g form a Gröbner basis for I_o, and the monomials $x^{\alpha_1} y^{\alpha_2}$ with $0 \leq \alpha_1 \leq m - 1$ and $0 \leq \alpha_2 \leq n - 1$ are precisely the standard monomials:



2 Gröbner basis elements

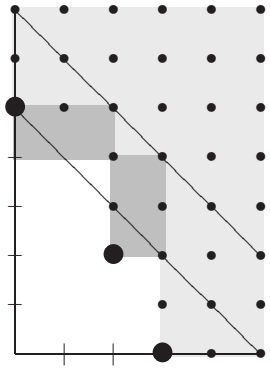
If $\beta_1 > 0$, however, then f, g do not form a Gröbner basis since this would imply that there are infinitely many standard monomials. Hence, the remainder of $S(g, f) = x^{(m-\beta_1)} g - y^{\beta_2} f$ on Mora division by f, g is nonzero and gives a new (homogeneous) Gröbner basis element h_3 for I whose leading term is a scalar times a monomial of type $x^{\gamma_1} y^{\gamma_2}$, with $\beta_1 > \gamma_1$ and $\gamma_1 + \gamma_2 = m + \beta_2$.

Applying Buchberger's criterion to f, g, h_3, the only new S-polynomial to be tested is $S(h_3, g)$ since $x^{m-\gamma_1}$ is divisible by $x^{\beta_1 - \gamma_1}$. If nonzero, we add

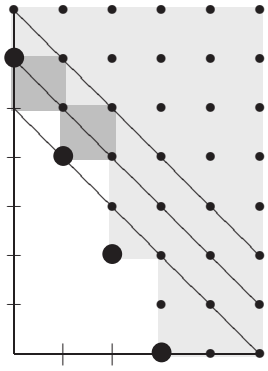
the remainder arising from this test to the set of generators and continue in this way. The resulting process yields (homogeneous) Gröbner basis elements $h_1 = f, h_2 = g, h_3, \ldots$, where, at each stage of the process, only $S(h_k, h_{k-1})$ needs to be tested, and where the degree of the new generator h_{k+1} coincides with that of the "corner" $\mathrm{LCM}(\mathbf{L}(h_k), \mathbf{L}(h_{k-1}))$.

Eventually, we will get an element h_r such that $\mathbf{L}(h_r)$ is a scalar times a power of y. Then the remainder of $S(h_r, h_{r-1})$ on Mora division by the h_k is zero by reasons of degree (as in (4.11)). Hence, $h_1, \ldots, h_r$ form a Gröbner basis for I_0.

In visualizing the process just described, we may say that the leading monomials of the h_k determine a staircase which connects the x-axis with the y-axis. An elementary inductive argument shows that the area under the stairs has size $m \cdot n$, as in the case where $\beta_1 = 0$:



3 Gröbner basis elements

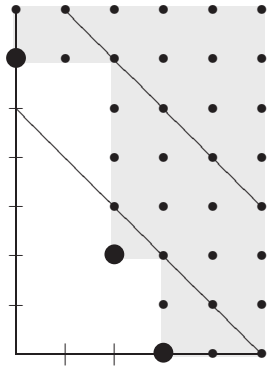


4 Gröbner basis elements

Case 2: Let, now, f and g be nonhomogeneous. As above, by computing a Gröbner basis $h_1 = f, h_2 = g, \ldots, h_r$ for I_o, we get a staircase of leading terms which connects the x-axis with the y-axis. Now, however, the Gröbner basis elements are not necessarily homogeneous. Let $\widetilde{h}_{k+1}$ be the part of h_{k+1} of degree $\deg \mathrm{LCM}(\mathbf{L}(h_k), \mathbf{L}(h_{k-1}))$, and let s be the least number k such that $\widetilde{h}_{k+1}$ is zero. Then $\widetilde{h}_1, \ldots, \widetilde{h}_s$ form a Gröbner basis for $\langle f_m, g_n \rangle \mathcal{O}_o$ such that $\mathbf{L}(h_k) = \mathbf{L}(\widetilde{h}_k)$ for all $k \leq s$ (recall that $>_{\mathrm{ldrlex}}$ is degree-anticompatible). We, hence, have two possibilities:

Case 2a: If f and g do not have a common tangent line at o, the $\mathbf{L}(\widetilde{h}_k)$ must reach the y-axis as well, which means that the staircase arising from f_m, g_n coincides with that arising from f, g. Then, again, there are precisely $m \cdot n$ standard monomials for I_o.

Case 2b: If, however, f and g do have a common tangent line at o, we must have $s < r$. Then $\deg \mathbf{L}(h_{s+1}) > \deg \mathrm{LCM}(\mathbf{L}(h_s), \mathbf{L}(h_{s-1}))$, so that for the staircase arising from f, g, the area under the stairs has size $> m \cdot n$:



This concludes the proof of Theorem 4.3.18. □

Exercise* 4.4.26 (Multiplicities in Terms of the Local Ring). Let $f \in \Bbbk[x_1, \ldots, x_n]$ be a nonconstant polynomial, let $p \in \mathbb{A}^n$ be a point, and let R be the local ring $R = \mathcal{O}_{\mathbb{A}^n,p}/\langle f \rangle\, \mathcal{O}_{\mathbb{A}^n,p}$ with its maximal ideal $\mathfrak{m}_R$. The **multiplicity of f at p**, written $\operatorname{mult}(f,p)$, is defined to be

$$\operatorname{mult}(f,p) = \min\{k \mid \dim_{\mathbb{K}} R/\mathfrak{m}_R^{k+1} < \binom{n+k}{k}\}.$$

Show that $\operatorname{mult}(f,p) \geq 1$ iff $p \in \mathrm{V}(f)$. If f is square-free, show that $\operatorname{mult}(f,p) = 1$ iff p is a smooth point of $\mathrm{V}(f)$. In case $n = 1$, show that $\operatorname{mult}(f,p)$ is the usual multiplicity of p as a root of f. In the case of plane curves, show that the definition of multiplicity given here coincides with the one given in Definition 4.3.2. □

We conclude this section with some remarks on convergent power series. Recall that in case $\Bbbk = \mathbb{C}$ (or $\Bbbk = \mathbb{R}$), a power series $f = \sum_\alpha f_\alpha x^\alpha \in \mathbb{C}[[x_1, \ldots, x_n]]$ is convergent if there exist a polyradius $\rho = (\rho_1, \ldots, \rho_n) \in \mathbb{R}^n_{>0}$ such that the series

$$||f||_\rho = \sum_\alpha |f_\alpha| \rho_1^{\alpha_1} \cdots \rho_n^{\alpha_n} < \infty$$

In this case, f converges absolutely on the polydisc $D_\rho = \{|x_1| \leq \rho_1, \ldots, |x_n| \leq \rho_n\}$ and $R_\rho = \{f \mid ||f||_\rho < \infty\}$ is a Banach space.

The set of convergent power series is a ring which we denote by $\mathbb{C}\{x_1, \ldots, x_n\}$. We, then, have a chain of ring inclusions

$$\mathbb{C}[x_1, \ldots, x_n] \subset \mathcal{O}_{\mathbb{A}^n(\mathbb{C}),o} \subset \mathbb{C}\{x_1, \ldots, x_n\} \subset \mathbb{C}[[x_1, \ldots, x_n]].$$

Proposition 4.4.27. *Let $>$ be a local monomial order on $\mathbb{C}[x_1, \ldots, x_n]$. If $g, f_1, \ldots, f_r$ are convergent power series, and $g = \sum g_i f_i + h$ is the unique exprssion satisfying the conditions (DD1) and (DD2) of Grauert's division*

theorem, then the g_i and h are convergent, too. In particular, the reduced Gröbner basis of an ideal in $\mathbb{C}\{x_1,\ldots,x_n\}$ generated by convergent power series consists of convergent power series, too. □

Proof. Let $>_w$ be local weight order on $\mathbb{C}[x_1,\ldots,x_n]$ given by $\mathbb{Q}$-linear independent negative weights such that $\mathbf{L}_w(f_i) = \mathbf{L}(f_i)$. Without of generality we assume that the f_i are monique, say $\mathbf{L}(f_j) = x^{\alpha^j}$. Consider tupels

$$K = \{(g_1,\ldots,g_r,h) \in \mathbb{C}[[x_1,\ldots,x_n]]^{r+1} \mid \text{ satisfying condition DD2}\}$$

and the subspace K_ρ of tuples, which have finite norm

$$||(g_1,\ldots,g_r,h)||_\rho := \sum ||g_i||_\rho \rho^{\alpha^j} + ||h||_\rho < \infty$$

Then the map

$$\psi : K_\rho \to R_\rho, (g_1,\ldots,g_r,h) \mapsto \sum g_i x^{\alpha^i} + h$$

is an isometrie of Banach spaces. We claim that for suitable ρ the pertubation

$$\phi : K_\rho \to R_\rho, (g_1,\ldots,g_r,h) \mapsto \sum g_i f_i + h$$

is still an isomorphism. For this we consider the weight order given by w and a polyradius $\rho(\tau) = (\tau^{-w_1},\ldots,\tau^{-w_n})$ for $0 < \tau << 1$ such that $g, f_1,\ldots,f_r$ converge in $D_{\rho(\tau)}$ and $q = \sum_i ||f_i - ini_w(f_i)||_{\rho(\tau)} \rho(\tau)^{-alpha^i} < 1$. Then $\phi \circ \psi^{-1} = id_{R_{\rho(\tau)}} + \epsilon$ with operator norm $||\epsilon||_{\rho(\tau)} \leq q < 1$. Hence $\sum_k (-1)^k \epsilon^k$ is a convergent series of operators, which gives $(id_{R_r ho(\tau)} + \epsilon)^{-1}$.

Thus given $g \in \mathbb{C}\{x_1,\ldots,x_n\}$ we can choose $0 < \tau << 1$ such that additionally $g \in R_{\rho(\tau)}$. Then $g_1, dots, g_r$ and h converge in this polydisc as well.

The rings $\Bbbk[[x_1,\ldots,x_n]]$ and $\mathbb{C}\{x_1,\ldots,x_n\}$. As for the polynomial ring, the proof uses induction and Gauss' Lemma., utilizing the Weierstrass Preparation Theorem which frequently is also used to prove the Noetherian property of these rings. We need the following notation: A power series $f \in \Bbbk[[x_1,\ldots,x_n]]$ is called x_n**-general** if $f(0,x_n) \neq 0 \in \Bbbk[x_n]$.

Exercise 4.4.28 (Weierstrass Preparation Theorem). If $f \in \Bbbk[[x_1,\ldots,x_n]]$ is a power series, show:

1. By a triangular change of coordinates, we can achieve that f is x_n-general.
2. If f is x_n-general, there exisits a local monomial order on $\Bbbk[x_1,\ldots,x_n]$ such that $\mathbf{L}(f) = \mathbf{L}(f(0,x_n))$.
3. If f is x_n-general, then $\langle f \rangle$ is generated by a Weierstrass polynomial

   $$p = x_n^d + a_1(x_1,\ldots,x_{n-1})x_n^{n-1} + \ldots + a_d(x_1,\ldots,x_{n-1}) \in \Bbbk[[x_1,\ldots,x_{n-1}]][x_n] \text{ with } p(0,x_n) = x_n^d,$$

   that is there exists a unit $u \in \Bbbk[[x_1,\ldots,x_n]]$ with $f = up$. *Hint:* Grauert division gives an expression $x_n^d = uf + h$ satisfying conditions /DD1) and (DD2). Set $p_n = x_n^d - h$ and show that u is a unit. □

Exercise 4.4.29. Complete the proof of the fact that $\Bbbk[[x_1, \ldots, x_n]]$ is factorial. □

Exercise 4.4.30. 1. Formal implicit mappimg theorem
2. Formal inverse function theorem

□

4.5 The Local-Global Principle

The technique of localization often allows one to reduce the proof of a result in commutative algebra to the local case, where the result is easier to establish (for instance, since we can apply Nakayama's lemma). We will see several examples of how this works in the next section. Now, in preparing the ground for some of the arguments, we extend localization from rings to modules, and study **properties** of a module M over a ring R which are **local** in the sense that M has the property iff $M_{\mathfrak{p}}$ has the property for all prime ideals $\mathfrak{p}$ of R. Here, $M_{\mathfrak{p}} = M[U^{-1}]$ is the localization of M at $U = R \setminus \mathfrak{p}$ in the following sense:

Remark-Definition 4.5.1. Let R be a ring, let $U \subset R$ be a multiplicatively closed subset, and let M be an R-module. As in case $M = R$, the relation

$$(m, u) \sim (m', u') \iff v(mu' - um') = 0 \text{ for some } v \in U$$

is an equivalence relation, and we write

$$M[U^{-1}] = U^{-1}M = \{\frac{m}{u} \mid m \in M, u \in U\}$$

for the set of all equivalence classes. We consider $M[U^{-1}]$ as an $R[U^{-1}]$-module, with addition defined as for $R[U^{-1}]$, and with the action

$$\frac{r}{u} \cdot \frac{m}{u'} = \frac{rm}{uu'}.$$

This module is called the **localization of M at U**.

If $\varphi : M \to N$ is an R-module homomorphism, there is an induced homomorphism $\varphi[U^{-1}] : M[U^{-1}] \to N[U^{-1}]$ of $R[U^{-1}]$-modules taking m/u to $\varphi(m)/u$. We have:

1. $\mathrm{id}_M[U^{-1}]) = \mathrm{id}_{M[U^{-1}]}$.
2. If
$$M' \xrightarrow{\varphi} M \xrightarrow{\psi} M''$$
are maps of R-modules, then
$$(\psi \circ \varphi)[U^{-1}] = \psi[U^{-1}] \circ \varphi[U^{-1}].$$

These properties are usually referred to by saying that U^{-1} is a **functor** from the category of R-modules to the category of $R[U^{-1}]$-modules.

Finally, note that if $I \subset R$ is an ideal, then

$$IR[U^{-1}] = I[U^{-1}].$$

Indeed, this is clear since every element $\sum f_i/u_i$ with $f_i \in I$ and $u_i \in U$ for all i can be brought to a common denominator. □

In what follows, let R and U be as above.

Exercise 4.5.2. If M is an R-module, show that

$$M[U^{-1}] \cong M \otimes_R R[U^{-1}].$$ □

Proposition 4.5.3. *The* **functor** U^{-1} *is* **exact**. *That is, if a sequence of R-modules*

$$M' \xrightarrow{\varphi} M \xrightarrow{\psi} M''$$

is exact at M, then the induced sequence of $R[U^{-1}]$-modules

$$M'[U^{-1}] \xrightarrow{\varphi[U^{-1}]} M[U^{-1}] \xrightarrow{\psi[U^{-1}]} M''[U^{-1}]$$

is exact at $M[U^{-1}]$.

Proof. By assumption and since U^{-1} is a functor, $0 = (\psi \circ \varphi)[U^{-1}] = \psi[U^{-1}] \circ \varphi[U^{-1}]$. Hence, $\operatorname{im} \varphi[U^{-1}] \subset \ker \psi[U^{-1}]$. To show the opposite inclusion, let $m/u \in \ker \psi[U^{-1}]$. That is, $0 = \psi[U^{-1}](m/u) = \psi(m)/u$. Then there is an element $v \in U$ such that $0 = v\psi(m) = \psi(vm)$. Hence, $vm \in \ker \psi = \operatorname{im} \varphi$ and, thus, $vm = \varphi(m')$ for some $m' \in M'$. We conclude that

$$m/u = vm/vu = \varphi(m')/vu = \varphi[U^{-1}](m'/vu) \in \operatorname{im} \varphi[U^{-1}].$$ □

The proposition implies, in particular, that if N is a submodule of M, then the induced map $N[U^{-1}] \to M[U^{-1}]$ is injective. We may, thus, regard $N[U^{-1}]$ as a submodule of $M[U^{-1}]$.

Exercise* 4.5.4. Show that localization commutes with forming sums and intersections of submodules.That is, if N and N' are submodules of an R-module M, then:

1. $(N + N')[U^{-1}] = N[U^{-1}] + N'[U^{-1}]$.
2. $(N \cap N')[U^{-1}] = N[U^{-1}] \cap N'[U^{-1}]$. □

Proposition 4.5.5 (Primary Decomposition and Localization). *Let R be a Noetherian ring, let $I \subset R$ be an ideal, let $U \subset R$ be a multiplicatively closed subset, and let $\iota : R \to R[U^{-1}]$ be the natural homomorphism. If $I = \bigcap_{i=1}^{t} \mathfrak{q}_i$ is a minimal primary decomposition, then*

$$I[U^{-1}] = \bigcap_{\mathfrak{q}_i \cap U = \emptyset} \mathfrak{q}_i[U^{-1}] \quad \text{and} \quad \iota^{-1}(I[U^{-1}]) = \bigcap_{\mathfrak{q}_i \cap U = \emptyset} \mathfrak{q}_i$$

are minimal primary decompositions as well.

Proof. We write $\mathfrak{p}_i = \operatorname{rad} \mathfrak{q}_i$.

If $\mathfrak{q}_i \cap U \neq \emptyset$, then $\mathfrak{q}_i[U^{-1}] = R[U^{-1}]$ since the elements of U are sent to units in $R[U^{-1}]$. In contrast, if $\mathfrak{q}_i \cap U = \emptyset$, then $\mathfrak{q}_i[U^{-1}]$ is $\mathfrak{p}_i[U^{-1}]$-primary and $\iota^{-1}(\mathfrak{q}_i[U^{-1}]) = \mathfrak{q}_i$ (see Exercise 4.2.8). Taking Exercise 4.5.4 into account, we find that

$$I[U^{-1}] = \bigcap_{\mathfrak{q}_i \cap U = \emptyset} \mathfrak{q}_i[U^{-1}]$$

and

$$\iota^{-1}(I[U^{-1}]) = \bigcap_{\mathfrak{q}_i \cap U = \emptyset} \iota^{-1}(\mathfrak{q}_i[U^{-1}]) = \bigcap_{\mathfrak{q}_i \cap U = \emptyset} \mathfrak{q}_i$$

are primary decompositions. These decompositions are minimal since the original decomposition of I is minimal (apply Theorem 4.2.7 to see that the involved prime ideals are distinct). □

Exercise* **4.5.6.** Prove the 2nd Uniqueness Theorem 1.8.9 for primary decomposition. □

Now, we give some examples of local properties:

Proposition 4.5.7. *If M is an R-module, the following are equivalent:*

1. $M = 0$.
2. $M_{\mathfrak{p}} = 0$ *for all prime ideals* $\mathfrak{p}$ *of* R.
3. $M_{\mathfrak{m}} = 0$ *for all maximal ideals* $\mathfrak{m}$ *of* R.

Proof. The only nontrivial part of the proof is to show that condition 3 implies condition 1. For this, suppose that $M \neq 0$, and let $m \in M$ be a nonzero element. Then the annihilator $\operatorname{Ann}(m)$ is a proper ideal of R which is necessarily contained in a maximal ideal $\mathfrak{m} \subset R$. It follows that $m/1 \in M_{\mathfrak{m}}$ cannot be zero since otherwise $vm = 0$ for some $v \in R \setminus \mathfrak{m}$, a contradiction to $\operatorname{Ann}(m) \subset \mathfrak{m}$. In particular, $M_{\mathfrak{m}} \neq 0$, as desired. □

In the proposition below, if $\mathfrak{p}$ is a prime ideal of R and $U = R \setminus \mathfrak{p}$, we write $\phi_{\mathfrak{p}} = \phi[U^{-1}]$.

Proposition 4.5.8. *If $\phi : M \to N$ is a homomorphism of R-modules, the following are equivalent:*

1. ϕ *is injective.*
2. $\phi_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ *is injective for all prime ideals* $\mathfrak{p}$ *of* R.
3. $\phi_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ *is injective for all maximal ideals* $\mathfrak{m}$ *of* R.

The same holds if we replace "injective" by "surjective" in all statements.

Proof. 1 $\implies$ 2: This follows by applying Proposition 4.5.3 to the exact sequence

$$0 \to M \to N.$$

2 $\implies$ 3: This is clear.

3 $\Longrightarrow$ 1: Applying Proposition 4.5.3 to the exact sequence

$$0 \to \ker \phi \to M \to N,$$

we find that the localized sequences

$$0 \to (\ker \phi)_{\mathfrak{m}} \to M_{\mathfrak{m}} \to N_{\mathfrak{m}}$$

are exact for all maximal ideals $\mathfrak{m}$ of R. Since all the $(\ker \phi)_{\mathfrak{m}}$ are zero by assumption, also $\ker \phi$ is zero by Proposition 4.5.7.

The surjectivity part follows in the same way. □

Exercise 4.5.9. Show that being normal is a local property of integral domains. □

4.6 Artinian Rings and Krull's Principal Ideal Theorem

In practical applications, we might wish to compute intersection numbers in cases where the intersection points are not rational over the given field of definition of our curves.

Example 4.6.1. In $\mathbb{A}^2(\mathbb{C})$, consider the parabola $C = \mathrm{V}(y^2 - x)$ and the graph $D = \mathrm{V}(x^3 - 6x^2 + 2xy + 9x - 6y + 1)$ of the rational function which sends x to $\frac{x^3-6x^2+9x+1}{6-2x}$.

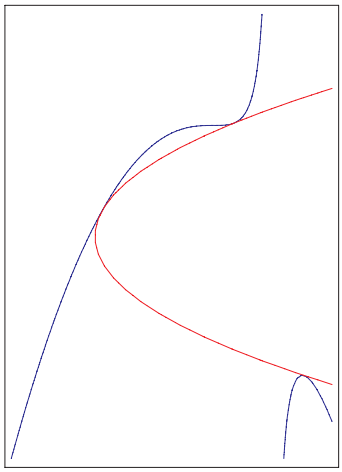


Fig. 4.2. *Three intersection points of multiplicity 2.*

Both curves are defined over $\mathbb{Q}$. Plugging in y^2 for x in the equation defining D, we find that the y-coordinates of the intersection points satisfy the equation $(y^3 - 3y + 1)^2 = 0$. Hence, we have three intersection points, say $p_i = (a_i, b_i)$, $i = 1, 2, 3$. Since the polynomial $y^3 - 3y + 1$ is irreducible over $\mathbb{Q}$, the p_i are not defined over $\mathbb{Q}$. They are, in fact, defined over the number field

$$\mathbb{Q}(b_i) \cong \mathbb{Q}[y]/\langle y^3 - 3y + 1\rangle$$

which is an extension field of $\mathbb{Q}$ of degree 3. Intuitively, considering Figure 4.2, each intersection point should be counted with multiplicity 2. Checking this for p_i using Definition 4.3.15, we would have to extend our ground field from $\mathbb{Q}$ to $\mathbb{Q}(b_i)$ and work in $\mathbb{Q}(b_i)[x, y]_{\langle x-a_i, y-b_i\rangle}$.

In what follows, we will describe an alternative way of defining intersection multiplicities which, in the example here, compares the ring

$$R = \mathbb{Q}[x, y]/\langle y^2 - x, x^3 - 6x^2 + 2xy + 9x - 6y + 1\rangle \cong \mathbb{Q}[y]/\langle y^3 - 3y + 1\rangle^2$$

with its quotient

$$R/\langle \overline{y}^3 - 3\overline{y} + 1\rangle \cong \mathbb{Q}[y]/\langle y^3 - 3y + 1\rangle. \qquad \square$$

In making the alternative definition of intersection multiplicities, we will rely on the concept of length. This provides a measure for the size of a module and constitutes, thus, one way of extending the concept of dimension from vector spaces to modules. Here is the relevant terminology.

Let R be any ring, and let M be any R-module. A **normal series** of M is a sequence

$$M = M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \ldots \supsetneq M_k = \langle 0\rangle$$

of submodules of M with strict inclusions. The number k of inclusions is called the **length** of the normal series. A **composition series** of M is a maximal normal series, that is, a normal series which cannot be extended to a normal series of greater length by inserting an extra submodule. Equivalently, each **factor** M_i/M_{i+1} is simple. Here, an R-module $0 \neq M$ is called **simple** if it has no submodules other than $\langle 0\rangle$ and M itself. Note that simple modules (over *commutative* rings) are fields:

Lemma 4.6.2. *A module $0 \neq M$ over a ring R is simple iff M can be written as a quotient $R/\mathfrak{m}$, where $\mathfrak{m} \subset R$ is a maximal ideal.*

Proof. If $M \cong R/\mathfrak{m}$ is a field, then it is clearly simple. For the converse, choose any element $0 \neq m \in M$. Then $M = mR$ and, hence, $M \cong R/\mathfrak{m}$, where $\mathfrak{m} = \mathrm{Ann}(m)$. Necessarily, $\mathfrak{m}$ is a maximal ideal since otherwise M would contain a proper nonzero submodule. $\square$

Definition 4.6.3. A module M over a ring R is said to be a **module of finite length** if it has a composition series. In this case, the length of the series is called the **length of M**, written $\ell(M)$. If no composition series exists, set $\ell(M) = \infty$. A **ring** R is **of finite length** if it is of finite length as an R-module. $\square$

We show that $\ell(M)$ is well defined:

Theorem 4.6.4 (Jordan-Hölder). *Let M be a module over a ring R. Suppose that M has a composition series. Then any two such series have the same length. Furthermore, any normal series of M can be extended to a composition series.*

Proof. Let $M = M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \ldots \supsetneq M_\ell = \langle 0 \rangle$ be any composition series of M. Both statements of the theorem follow from the claim that every normal series of M has length $\leq \ell$. Indeed, the first statement is obtained by applying the claim to a composition series of minimum length. For the second statement, given a normal series of M which is not maximal, note that the process of inserting extra submodules must stop as soon as we reach length l.

To establish the claim, observe that the cases $\ell = 0$ (that is, $M = \langle 0 \rangle$) and $\ell = 1$ (that is, M is simple) are trivial. We consider, therefore, the case $\ell \geq 2$, and suppose inductively that the claim holds for all R-modules with a composition series of length $\leq \ell - 1$.

Let $M = N_0 \supsetneq N_1 \supsetneq N_2 \supsetneq \ldots \supsetneq N_k = \langle 0 \rangle$ be any normal series of M. If $N_1 \subset M_1$, the induction hypothesis applied to M_1 yields $k-1 \leq \ell-1$ since M_1 has a composition series of length $\ell-1$. If $N_1 \not\subset M_1$, we must have $N_1 + M_1 = M$ since M/M_1 is simple. Then $N_1/(M_1 \cap N_1) \cong (N_1 + M_1)/M_1 \cong M/M_1$ is simple as well. On the other hand, applying, once more, the induction hypothesis to M_1, we find that all normal series of the proper submodule $M_1 \cap N_1$ of M_1 must have length $\leq \ell - 2$. It follows that N_1 has a composition series of length $\leq \ell - 2 + 1 = \ell - 1$ since $N_1/(M_1 \cap N_1)$ is simple. As above, we conclude that $k - 1 \leq \ell - 1$. □

Exercise* 4.6.5. Let R be a ring, let M be an R-module of finite length, and let $M = M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \ldots \supsetneq M_\ell = \langle 0 \rangle$ be a composition series of M. If $\mathfrak{m}$ is a maximal ideal of R, show that the length of the $R_\mathfrak{m}$-module $M_\mathfrak{m}$ is the number of quotients M_i/M_{i+1} isomorphic to $R/\mathfrak{m}$. □

Our next goal is to characterize modules of finite length in terms of chain conditions. For this, we not only consider the ascending chain condition, but also the descending chain condition:

Definition 4.6.6. A **module** M over a ring R is called **Artinian** if it satifies the **descending chain condition**. That is, every chain

$$M = M_0 \supset M_1 \supset M_2 \supset \ldots M_k \supset \ldots$$

of submodules of M is eventually stationary. A **ring** R is called **Artinian** if it is Artinian as an R-module. That is, R satisfies the descending chain condition on ideals. □

As in Exercise 1.4.5 one shows that M is Artinian iff the **minimal condition** on submodules holds: Every nonempty set of ideals of R has a minimal element with respect to inclusion.

Proposition 4.6.7. *Let M be a module over a ring R. Then the following are equivalent:*

1. *M is of finite length.*
2. *M is Artinian and Noetherian.*

Proof. 1 $\implies$ 2: If $\ell(M) < \infty$, the length of any normal series of M is bounded by $\ell(M)$. Hence, both chain conditions hold.

2 $\implies$ 1: Since M is Noetherian, it satisfies the maximal condition. In particular, there is a maximal submodule $M_1 \subsetneq M = M_0$ which, necessarily, is Noetherian as well. Applying the same argument to M_1 and so forth, we get a descending chain $M = M_0 \supsetneq M_1 \supsetneq \dots$ which, since M is Artinian, is eventually stationary. It is, hence, a composition series of M. □

Exercise* 4.6.8. Let R be a ring, and let

$$0 \to M' \to M \to M'' \to 0$$

be a short exact sequence of R-modules. Show:

1. M is Artinian (respectively Noetherian) iff both M' and M'' are Artinian (respectively Noetherian).
2. M is of finite length iff both M' and M'' are of finite length. In this case,

$$\ell(M) = \ell(M') + \ell(M'').$$

□

The examples in the following exercise illustrate our definitions:

Exercise* 4.6.9. Show:

1. If M is a module over a field K, that is, M is a K-vector space, then M is Noetherian iff M is Artinian iff M is of finite length iff $\dim_K M < \infty$.
2. If I is an ideal of a ring R, then R/I is of finite length as a ring iff it is of finite length as an R-module.
3. An affine $\Bbbk$-algebra $\Bbbk[x_1, \dots, x_n]/I$ is of finite length iff it has finite dimension as a $\Bbbk$-vector space. Geometrically, this is the case where the vanishing locus $\mathrm{V}(I) \subset \mathbb{A}^n$ consists of finitely many points.
4. The $\Bbbk[x]$-module $M = \Bbbk[x, x^{-1}]/\Bbbk[x]$ is Artinian, but not Noetherian. □

Definition 4.6.10. Let $f, g \in \Bbbk[x, y]$ be nonconstant polynomials, and let $\mathfrak{m}$ be a maximal ideal of $\Bbbk[x, y]$. The **intersection multiplicity of f and g at $\mathfrak{m}$**, written $i(f, g; \mathfrak{m})$, is defined to be

$$i(f, g; \mathfrak{m}) = \ell(\Bbbk[x, y]_{\mathfrak{m}} / \langle f, g \rangle \Bbbk[x, y]_{\mathfrak{m}}).$$

□

As a consequence of the definition, the following facts are easy to prove:

Exercise 4.6.11 (Properties of Intersection Multiplicities). Let $f, g \in \Bbbk[x, y]$ be nonconstant polynomials, and let $\mathfrak{m} \subset \Bbbk[x, y]$ be a maximal ideal. Then show:

1. $i(f,g;\mathfrak{m}) = 0$ iff $\mathrm{V}(\mathfrak{m}) \not\subset \mathrm{V}(f) \cap \mathrm{V}(g) \subset \mathbb{A}^2$.
2. $i(f,g;\mathfrak{m}) = \infty$ iff f and g have a common factor contained in $\mathfrak{m}$.
3. If $\mathrm{V}(f) \cap \mathrm{V}(g) \subset \mathbb{A}^2$ is finite, then $i(f,g;\mathfrak{m})$ is the number of quotients in a composition series of $\Bbbk[x,y]/\langle f,g\rangle$ which are isomorphic to $\Bbbk[x,y]/\mathfrak{m}$.
4. If the field extension $\Bbbk[x,y]/\mathfrak{m} \supset \Bbbk$ is separable, then $\mathrm{V}(\mathfrak{m}) \subset \mathbb{A}^2$ consists of $[\Bbbk[x,y]/\mathfrak{m} : \Bbbk]$ points (which form an orbit under the natural action of the Galois group of $\overline{\Bbbk}$ over $\Bbbk$). For each such point p,
$$i(f,g;p) = i(f,g;\mathfrak{m}).$$
5. If $\Bbbk[x,y]/\mathfrak{m} \supset \Bbbk$ is inseparable, then $\mathrm{V}(\mathfrak{m})$ consists of $[\Bbbk[x,y]/\mathfrak{m} : \Bbbk]_{sep}$ points. For each such point p,
$$i(f,g;p) = i(f,g;\mathfrak{m}) \cdot [\Bbbk[x,y]/\mathfrak{m} : \Bbbk]_{insep}.$$
Here, the subscripts *sep* and *insep* refer to the separable and inseparable degrees, respectively. □

Example 4.6.12. The affine $\mathbb{Q}$-algebra
$$R = \mathbb{Q}[x,y]/\langle y^2 - x, x^3 - 6x^2 + 2xy + 9x - 6y + 1\rangle \cong \mathbb{Q}[y]/\langle y^3 - 3y + 1\rangle^2$$
from Example 4.6.1 has finite length since it has finite dimension as a $\mathbb{Q}$-vector space. In fact, $R \supsetneq \langle \overline{y}^3 - 3\overline{y} + 1\rangle \supsetneq \langle 0\rangle$ is a composition series. Note that both factors are isomorphic to $\mathbb{Q}[y]/\langle y^3 - 3y + 1\rangle$. Taking parts 4, 3 of Exercise 4.6.11 into account, we find, as expected, that the curves C, D from Example 4.6.1 have three intersection points, each of which has multiplicity 2. □

Exercise 4.6.13. Let $I \subset \Bbbk[x_1,\ldots,x_n]$ be an ideal such that $\mathrm{V}(I) \subset \mathbb{A}^n$ is finite, and let $\mathfrak{m} \subset \Bbbk[x_1,\ldots,x_n]$ be a maximal ideal. Express
$$\ell(\Bbbk[x_1,\ldots,x_n]_{\mathfrak{m}}/I\Bbbk[x_1,\ldots,x_n]_{\mathfrak{m}})$$
in terms of the sequence $\dim_{\Bbbk} \Bbbk[x_1,\ldots,x_n]/I_k$, $k \geq 0$, where I_k is defined inductively by $I_0 = I$ and $I_k = I_{k-1} : \mathfrak{m}$. □

Exercise 4.6.14. Some examples for intersection number computations. □

Despite the formal symmetry between the ascending and the decending chain condition, the notions of Noetherian and Artinian rings are quite different. In fact, our next result shows that every Artinian ring is Noetherian, but of a very special kind (so that most Notherian rings are not Artinian):

Theorem 4.6.15. *For a ring R, the following are equivalent:*

1. *R is Noetherian and* $\dim R = 0$.
2. *R has finite length.*
3. *R is Artinian.*

If these conditions are satisfied, then R has only finitely many maximal ideals.

Proof. 1 $\implies$ 2: Suppose that R is Noetherian. If R is not of finite length, the set

$$\Gamma := \{I \subset R \text{ ideal } \mid R/I \text{ is not of finite length}\}$$

is nonempty since $\langle 0\rangle \in \Gamma$. Hence, since R is Noetherian, Γ contains a maximal element $\mathfrak{p}$. We show that $\mathfrak{p}$ is a prime ideal. For this, let $f, g \in R$ be elements such that $fg \in \mathfrak{p}$, but $f \notin \mathfrak{p}$. Consider the exact sequence

$$0 \to R/(\mathfrak{p} : f) \xrightarrow{\cdot f} R/\mathfrak{p} \to R/(\mathfrak{p} + \langle f\rangle) \to 0.$$

Since $\mathfrak{p} + \langle f\rangle \supsetneq \mathfrak{p}$, the module $R/(\mathfrak{p} + \langle f\rangle)$ must have finite length by the maximality of $\mathfrak{p}$ as an element of Γ. If g would not be an element of $\mathfrak{p}$, then $\mathfrak{p} : f$ would contain $\mathfrak{p}$ properly, and $R/(\mathfrak{p} : f)$ would have finite length as well. But, then, $R/\mathfrak{p}$ would have finite length by Exercise 4.6.8, a contradiction to our choice of $\mathfrak{p}$.

Now, suppose not only that R is Notherian, but also that $\dim R = 0$. Then all prime ideals of R are maximal. In particular, if R were not of finite length, the prime ideal $\mathfrak{p}$ just constructed would be a maximal ideal, so that $R/\mathfrak{p}$ would be a field. This contradicts, again, the fact that $R/\mathfrak{p}$ is not of finite length.

2 $\implies$ 3: This is clear.

3 $\implies$ 1: Now, suppose that R is Artinian. To show that R satifies condition 1, we proceed in four steps.

Step 1. We show that $\dim R = 0$. For this, consider a nested pair of prime ideals $\mathfrak{p}_1 \subset \mathfrak{p}_2 \subset R$, and let f be any element of $\mathfrak{p}_2/\mathfrak{p}_1 \subset R/\mathfrak{p}_1$. Since $R/\mathfrak{p}_1$ is Artinian as well, the descending chain condition yields a number m such that $\langle f^m\rangle = \langle f^{m+1}\rangle$. Then $f^m = gf^{m+1}$ for some $g \in R/\mathfrak{p}_1$. That is, $(1 - gf)f^m = 0$. Since $R/\mathfrak{p}_1$ is an integral domain and $f \in \mathfrak{p}_2/\mathfrak{p}_1 \subsetneq R/\mathfrak{p}_1$ is not a unit, we conclude that $f = 0$. It follows that $\mathfrak{p}_1 = \mathfrak{p}_2$ and, thus, that $\dim R = 0$, as claimed.

Step 2. The ring R has only finitely many maximal ideals since any infinite sequence $\mathfrak{m}_1, \mathfrak{m}_2, \mathfrak{m}_3, \ldots$ of maximal ideals of R would yield an infinite descending chain of ideals

$$\mathfrak{m}_1 \supset \mathfrak{m}_1 \cap \mathfrak{m}_2 \supset \ldots \supset \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \ldots \cap \mathfrak{m}_k \supset \ldots$$

with strict inclusions (by part 2 of Exercise 1.3.4). Writing $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$ for the distinct maximal ideals of R and taking into account that every prime ideal of R is maximal by step 1, we conclude from Exercise 3.2.11 that

$$\operatorname{rad}\langle 0\rangle = \mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_s. \tag{4.12}$$

Step 3. For any i, the descending chain of ideals $\mathfrak{m}_i \supset \mathfrak{m}_i^2 \supset \mathfrak{m}_i^3 \supset \ldots$ is eventually stationary. We may, hence, choose a number N such thst $\mathfrak{m}_i^N = \mathfrak{m}_i^{N+1}$ for all i. Consider the ideal

$$I = \prod_{i=1}^{s} \mathfrak{m}_i^N.$$

Then $I^2 = I$. We use this to show that $I = \langle 0 \rangle$. Suppose the contrary. Then the set

$$\Gamma := \{J \subsetneq R \mid JI \neq \langle 0 \rangle\}$$

contains I since $I^2 = I \neq \langle 0 \rangle$. Hence, since R is Artinian, Γ contains a minimal element J_0. Let f be an element of J_0 such that $fI \neq \langle 0 \rangle$. Then $\langle f \rangle = J_0$ by the minimality of J_0. The same argument gives $fI = J_0 = \langle f \rangle$ since $(fI)I = fI^2 = fI \neq 0$. Choose an element $g \in I$ such that $fg = f$. Then $f = fg = fg^2 = \ldots = fg^m = 0$ for some $m \geq 1$ since every element of I is nilpotent by (4.12). This contradiction proves that $I = \langle 0 \rangle$, as claimed.

Step 4. Each of the successive quotients in the descending chain of ideals

$$R \supset \mathfrak{m}_1 \supset \ldots \supset \mathfrak{m}_1^N \supset \mathfrak{m}_1^N \mathfrak{m}_2 \supset \ldots \supset \prod_{i=1}^{s} \mathfrak{m}_i^N = \langle 0 \rangle \tag{4.13}$$

is a vector space over some field $R/\mathfrak{m}_i$. Hence, taking part 1 of Exercise 4.6.8 and part 1 of Exercise 4.6.9 into account, we get the following chain of equivalences: R is Artinian $\iff$ each quotient in (4.13) is Artinian $\iff$ each quotient in (4.13) is Noetherian $\iff$ R is Noetherian. This concludes the proof. □

Next, we establish a structure result for Artinian rings. Then, following Krull, we will apply Theorem 4.6.15 above to prove the principal ideal theorem which is fundamental to the dimension theory of Noetherian rings.

Theorem 4.6.16 (Structure Theorem for Artinian Rings). *Let R be an Artinian ring, and let $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$ be the distinct maximal ideals of R. Then*

$$R \cong \prod_{i=1}^{s} R_{\mathfrak{m}_i}$$

is a finite direct product of local Artinian rings.

Proof. To begin with, we conclude from Theorem 4.2.7 that any localization of an Artinian ring is again Artinian. Now, as in the preceeding proof, choose a number N such that $\prod_{i=1}^{s} \mathfrak{m}_i^N = \langle 0 \rangle$. Since the $\mathfrak{m}_i$ are pairwise coprime, the $\mathfrak{m}_i^N$ are pairwise coprime as well (see part 4 of Exercise 1.5.12). Hence, the natural map

$$R \to \prod_{i=1}^{s} R/\mathfrak{m}_i^N \tag{4.14}$$

is an isomorphism by the Chinese remainder theorem (see Exercise 1.3.9). To conclude the proof, we localize both sides of (4.14) and find that $R_{\mathfrak{m}_i} \cong (R/\mathfrak{m}_i^N)_{\mathfrak{m}_i} \cong R/\mathfrak{m}_i^N$ (indeed, $(R/\mathfrak{m}_j^N)_{\mathfrak{m}_i} = 0$ for $j \neq i$ and $R/\mathfrak{m}_i^N$ is a local ring). □

In the geometric context, the structure theorem extends Remark 4.3.16:

Corollary 4.6.17. *Let $I \subset \Bbbk[x_1, \ldots, x_n]$ be an ideal such that $\mathrm{V}(I) \subset \mathbb{A}^n$ is finite, say $\mathrm{V}(I) = \{p_1, \ldots, p_s\}$. Then there is a natural isomorphism of $\mathbb{K}$-algebras*

$$\mathbb{K}[x_1, \ldots, x_n]/I\,\mathbb{K}[x_1, \ldots, x_n] \cong \prod_{i=1}^{s} \mathcal{O}_{\mathbb{A}^n, p_i}/I\mathcal{O}_{\mathbb{A}^n, p_i}.$$

□

Theorem 4.6.18 (Krull's Principal Ideal Theorem, First Version). *Let R be a Noetherian ring, and let $f \in R$. Then every minimal prime $\mathfrak{p}$ of $\langle f \rangle$ satisfies*

$$\operatorname{codim} \mathfrak{p} \leq 1.$$

If f is not a zerodivisor of R, then equality holds.

Proof. To show the first statement of the theorem, we will localize and apply Nakayama's lemma. To begin with, recall from Proposition 4.2.13 that if $\mathfrak{p}$ is any prime ideal of any ring R, then $\operatorname{codim} \mathfrak{p} = \dim R_{\mathfrak{p}}$. With our assumptions here, we have, in addition, that $\mathfrak{p}R_{\mathfrak{p}}$ is a minimal prime of $\langle f \rangle R_{\mathfrak{p}}$. Replacing R by $R_{\mathfrak{p}}$, we may, hence, assume that R is local ring with maximal ideal $\mathfrak{p}$. The first statement of the theorem will follow once we show that $\operatorname{codim} \mathfrak{q} = \dim R_{\mathfrak{q}} = 0$ for every prime ideal $\mathfrak{q} \subsetneq \mathfrak{p}$.

For this, given $\mathfrak{q}$, consider the ideals

$$\mathfrak{q}^{(n)} = \{a \in R \mid ua \in \mathfrak{q}^n \text{ for some } u \notin \mathfrak{q}\},\ n \geq 1.$$

Then, by part 1 of Proposition 4.2.7, $\mathfrak{q}^{(n)}$ is the preimage of $\mathfrak{q}^n R_{\mathfrak{q}}$ under the localization map $R \to R_{\mathfrak{q}}$. Since the maximal ideal $\mathfrak{p} + \langle f \rangle$ of the quotient ring $R/\langle f \rangle$ is also minimal, this ring is zerodimensional. Being also Noetherian, it is Artinian by Theorem 4.6.15. Hence, the descending chain

$$\mathfrak{q}^{(1)} + \langle f \rangle \supset \mathfrak{q}^{(2)} + \langle f \rangle \supset \ldots$$

is eventually stationary, say $\mathfrak{q}^{(n)} + \langle f \rangle = \mathfrak{q}^{(n+1)} + \langle f \rangle$. As a consequence, any element $g \in \mathfrak{q}^{(n)}$ can be written as a sum $g = h + af$ with $h \in \mathfrak{q}^{(n+1)}$ and $a \in R$. Then $af \in \mathfrak{q}^{(n)}$. Since $\mathfrak{p}$ is a minimal prime of $\langle f \rangle$, we have $f \notin \mathfrak{q}$ and, thus, $a \in \mathfrak{q}^{(n)}$ by the very definition of $q^{(n)}$. This shows that

$$\mathfrak{q}^{(n)} = f\mathfrak{q}^{(n)} + \mathfrak{q}^{(n+1)}.$$

Since f is contained in the maximal ideal $\mathfrak{p}$ of R, Nakayama's lemma yields $\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)}$. Then $\mathfrak{q}^n R_{\mathfrak{q}} = \mathfrak{q}^{n+1} R_{\mathfrak{q}}$ by part 2 of Proposition 4.2.7. Applying Nakayama's lemma in $R_{\mathfrak{q}}$, we, hence, get $\mathfrak{q}^n R_{\mathfrak{q}} = \langle 0 \rangle$. We conclude that $\dim R_{\mathfrak{q}} = 0$, as desired.

The second statement of the theorem follows from the first one. Indeed, the Noetherian ring R contains only finitely many minimal prime ideals, say $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. Thus, if f is a not a zerodivisor of R, it is not contained in any of the $\mathfrak{p}_i$ by Exercise 3.2.12. This implies that $\operatorname{codim} \mathfrak{p} \geq 1$. □

Theorem 4.6.19 (Krull's Principal Ideal Theorem, General Version). *Let R be a Noetherian ring. If $I = \langle f_1, \ldots, f_c \rangle \subset R$ is an ideal which is generated by c elements, then every minimal prime $\mathfrak{p}$ of I satisfies*

$$\operatorname{codim} \mathfrak{p} \leq c.$$

Conversely, if $\mathfrak{p} \subset R$ is a prime ideal such that $\operatorname{codim} \mathfrak{p} = c$, there exist elements $y_1, \ldots, y_c \in R$ such that $\mathfrak{p}$ is a minimal prime of $\langle y_1, \ldots, y_c \rangle$.

Proof. To show the first statement of the theorem, let $\mathfrak{p}$ be a minimal prime of I. As in the preceeding proof, we may assume that R is a local ring with maximal ideal $\mathfrak{p}$. We do induction on c.

If $c = 0$, there is nothing to show. If $c > 0$, since R is Noetherian, we may find a prime ideal $\mathfrak{q} \subsetneq \mathfrak{p}$ such that no other prime ideal is between $\mathfrak{q}$ and $\mathfrak{p}$. Since $\mathfrak{p}$ is a minimal prime of $I = \langle f_1, \ldots, f_c \rangle$, at least one of the f_i is not contained in $\mathfrak{q}$, say $f_c \notin \mathfrak{q}$. Then the maximal ideal $\mathfrak{p} + (\mathfrak{q} + \langle f_c \rangle)$ of the quotient ring $R/(\mathfrak{q} + \langle f_c \rangle)$ is also minimal, so that this ring is an Artinian local ring. In particular, all the f_i are nilpotent mod $\mathfrak{q} + \langle f_c \rangle$. Say,

$$f_i^N = g_i + a_i f_c \text{ with } g_i \in \mathfrak{q} \text{ snd } a_i \in R,\ i = 1, \ldots, c-1.$$

Then $\mathfrak{p} \supset \langle g_1, \ldots, g_{c-1}, f_c \rangle$, and the image $\overline{\mathfrak{p}}$ of $\mathfrak{p}$ in $R/\langle g_1, \ldots, g_{c-1} \rangle$ is a minimal prime of the principal ideal $\langle \overline{f}_c \rangle$. Hence, $\overline{\mathfrak{p}}$ has codimension at most 1 by the first version of the principal ideal theorem. In R, this shows that $\mathfrak{q}$ is a minimal prime of $\langle g_1, \ldots, g_{c-1} \rangle$. The induction hypothesis gives $\operatorname{codim} \mathfrak{q} \leq c-1$ and, thus, $\operatorname{codim} \mathfrak{p} \leq c$.

For the converse statement, given $\mathfrak{p}$ as in the statement, we choose the y_i one at a time. Inductively, with $0 \leq k < c$, suppose that $y_1, \ldots, y_k \in \mathfrak{p}$ have already been chosen to generate an ideal of codimension k. Then, by prime avoidance, it is possible to pick an element $y_{k+1} \in \mathfrak{p}$ not contained in any of the finitely many minimal primes of $\langle y_1, \ldots, y_k \rangle$ (indeed, any such prime does not contain $\mathfrak{p}$ since its codimension is $\leq k < c$ by the first statement of the theorem). Clearly, $\operatorname{codim} \langle y_1, \ldots, y_k, y_{k+1} \rangle = k+1$, and the result follows. □

We are, now, ready to prove inequality (4.1) in its general form (4.3):

Corollary 4.6.20. *Let $(R, \mathfrak{m})$ be a local Noetherian ring. Then*

$$\dim R = \min\{d \mid \text{ there exists an } \mathfrak{m}\text{-primary ideal } \langle y_1, \ldots, y_d \rangle\}. \tag{4.15}$$

In particular,

$$\dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 \geq \dim R.$$

Proof. The last statement follows from the first one since $\mathfrak{m}$ is generated by $\dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$ elements (see Corollary 4.2.20 to Nakayama's lemma).

For the first statement, let $d = \dim R = \operatorname{codim} \mathfrak{m}$, and let d' be the minimum on the right hand side of (4.15). Then $d \leq d'$ respectively $d' \leq d$ follow from the first respectively second statement of the generalized principal ideal theorem. □

Its applications to geometry make Corollary 4.6.20 an important result of commutative algebra, where, in the situation of the corollary, a sequence of $d = \dim R$ elements $y_1, \ldots, y_d \in \mathfrak{m}$ is called a **system of parameters** for R if it generates an $\mathfrak{m}$-primary ideal. If $(R, \mathfrak{m})$ is regular, that is, if $\dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = d$, then, by Corollary 4.2.20, every minimal set of generators for $\mathfrak{m}$ is a system of parameters consisting of d elements. Such a system is called a **regular system of parameters** for R. A typical example is given below:

Corollary 4.6.21. *The formal power series ring $\Bbbk[[x_1, \ldots, x_n]]$ is regular of dimension n. In fact, $x_1, \ldots, x_n$ form a regular system of parameters.*

Proof. Since $\Bbbk[[x_1, \ldots, x_n]]$ is an integral domain, $\dim \Bbbk[[x_1, \ldots, x_n]]/\langle x_n \rangle = \dim \Bbbk[[x_1, \ldots, x_n]] - 1$ by Krull's principal ideal theorem. On the other hand, $\Bbbk[[x_1, \ldots, x_n]]/\langle x_n \rangle \cong \Bbbk[[x_1, \ldots, x_{n-1}]]$. Hence, we conclude by induction on n that $\dim \Bbbk[[x_1, \ldots, x_n]] = n$. The result follows. □

Remark 4.6.22. We mention in passing that every regular local ring $(R, \mathfrak{m})$ is an integral domain (to prove this, induct on $\dim R$ and use Nakayama's lemma). This, in turn, implies that if $y_1, \ldots, y_d$ is a regular system of parameters for R, then $y_1, \ldots, y_d$ is a **regular sequence** on R. That is, each y_i represents a nonzerodivisor of $R/\langle y_1, \ldots, y_{i-1} \rangle$, $i = 1, \ldots, d$. See Eisenbud (1995), Corollaries 10.14, 10.15 for details and further reading. □

At this point, the general definition of a Cohen-Macaulay ring deserves mentioning (though we will not need it in this book). According to this definition and the remark above, every regular local ring is Cohen-Macaulay.

Definition 4.6.23. A local Noetherian ring $(R, \mathfrak{m})$ is called **Cohen-Macaulay** if it has a system of parameters which is at the same time a regular sequence for R. An arbitrary Noetherian ring is called **Cohen-Macaulay** iff its lcoalization $R_{\mathfrak{p}}$ is Cohen-Macaulay for every prime ideal $\mathfrak{p}$ of R. □

The first statement made in Remark 4.6.22 says, in particular, that the local ring of an algebraic set at a smooth point is an integral domain. In the next two propositions, we give a direct proof for this fact:

Proposition 4.6.24. *Let $p = (a_1, \ldots, a_n) \in \mathbb{A}^n$ be a point, let $f_1, \ldots, f_r \in \Bbbk[x_1, \ldots, x_n]$ be polynomials vanishing at p, where $1 \leq r \leq n$, and let $R := \mathcal{O}_{\mathbb{A}^n,p}/\langle f_1, \ldots, f_r \rangle \mathcal{O}_{\mathbb{A}^n,p}$. Suppose the matrix $M = \left(\frac{\partial f_i}{\partial x_j}(p)\right)_{1 \leq i,j \leq r}$ has maximal rank r. Then R is isomorphic to a subring of $\mathbb{K}[[x_{r+1} - a_{r+1}, \ldots, x_n - a_n]]$. In particular, R is an integral domain.*

Proof. By translating p to the origin o, we may assume that $p = o$. We write $M^{-1} = (a_{ki})$ and set $g_k = \sum_{i=1}^{r} a_{ki} f_i$, $k = 1, \ldots r$. Then each g_k is of type $x_k +$ terms of degree ≥ 2. In particular, by Buchberger's criterion, the g_k form a Gröbner basis for the ideal generated by the f_i in $\mathbb{K}[[x_1, \ldots, x_n]]$ (fix a degree-anticompatible monomial order on $\mathbb{K}[x_1, \ldots, x_n]$). Given any

$g \in \mathcal{O}_{\mathbb{A}^n,o} \subset \mathbb{K}[[x_1,\dots,x_n]]$, the uniquely determined remainder h on Grauert division of g by the g_k is contained in $\mathbb{K}[[x_{r+1},\dots,x_n]]$. Sending g to h defines, thus, a map $\mathcal{O}_{\mathbb{A}^n,o} \to \mathbb{K}[[x_{r+1},\dots,x_n]]$ whose kernel is $\langle f_1,\dots,f_r\rangle \mathcal{O}_{\mathbb{A}^n,o}$. The result follows. □

Proposition 4.6.25. *Let $A \subset \mathbb{A}^n$ be an algebraic set, let $p \in A$ be a point, and let $d = \dim_p A$. Suppose we can find polynomials $f_1,\dots,f_{n-d} \in \mathrm{I}(A)$ such that the matrix $M = \left(\frac{\partial f_i}{\partial x_j}(p)\right)_{1\le i,j\le n-d}$ has maximal rank $n-d$. Then $\mathcal{O}_{A,p} \cong \mathcal{O}_{\mathbb{A}^n,p}/\langle f_1,\dots,f_{n-d}\rangle \mathcal{O}_{\mathbb{A}^n,p}$, and this ring is a regular local ring.*

Proof. Of course, up to renumbering the variables, the assumption just means that p is a smooth point of A. To establish the result, we consider the natural epimorphism of local rings

$$\phi : R := \mathcal{O}_{\mathbb{A}^n,p}/\langle f_1,\dots,f_{n-d}\rangle \mathcal{O}_{\mathbb{A}^n,p} \to \mathcal{O}_{A,p}.$$

Corollary 4.6.20 gives us $d = \dim \mathcal{O}_{A,p} \le \dim R \le \dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = d$, where $\mathfrak{m}$ is the maximal of R (for the latter equality, note that $d_p f_1,\dots,d_p f_{n-d}$ are $\mathbb{K}$-linearly independent by virtue of the assumption on the matrix M). Since R is an integral domain by the preceeding proposition, we conclude that $\ker\phi$ is zero (which completes the proof): if $f \in \ker\phi$ were a nonzero element, Krull's principal ideal theorem would give us $d = \dim \mathcal{O}_{A,p} \le \dim R/\langle f\rangle \le \dim R - \operatorname{codim}\langle f\rangle = d-1$. □

We can, now, prove part 2 of Remark 4.1.11:

Corollary 4.6.26. *Let A be an algebraic set. If $A = V_1 \cup \dots \cup V_s$ is the decomposition of A into its irreducible components, then*

$$A_{\mathrm{sing}} = \bigcup_{i\ne j}(V_i \cap V_j) \cup \bigcup_i (V_i)_{\mathrm{sing}}.$$

Proof. Let $p \in A$ be a smooth point of A. Then, since $\mathcal{O}_{A,p}$ is an integral domain by the preceeding propositions, p lies on a unique component V_i of A. It is, then, a smooth point of V_i. We conclude that $A \setminus A_{\mathrm{sing}} \subset (\bigcup_i V_i \setminus (V_i)_{\mathrm{sing}}) \setminus \bigcup_{i\ne j}(V_i \cap V_j)$. The converse inclusion is clear. □

Furthermore, we can show the corollaries to the Jacobian criterion. For this, let $I = \langle f_1,\dots,f_r\rangle \subset \Bbbk[x_1,\dots,x_n]$ be an ideal, let $A = \mathrm{V}(I) \subset \mathbb{A}^n$, and let $I_{n-d}\left(\frac{\partial f_i}{\partial x_j}\right)$ be the ideal generated by the $(n-d)\times(n-d)$ minors of the Jacobian matrix of the f_i. Moreover, let $I^e = I\,\mathbb{K}[x_1,\dots,x_n]$.

Proof of Corollary 4.1.13, conclusion. Supposing that A is equidimensional of dimension d, we have to show: If

$$I_{n-d}\left(\frac{\partial f_i}{\partial x_j}\right) + I = \langle 1\rangle,$$

then $I^e = \mathrm{I}(A)$.

Let $\mathfrak{m} \subset \mathbb{K}[x_1, \ldots, x_n]$ be any maximal ideal, and let $p \in \mathbb{A}^n$ be the corresponding point. Since $I^e \subset \mathrm{I}(A) \subset \mathbb{K}[x_1, \ldots, x_n]$, also $I^e_{\mathfrak{m}} \subset \mathrm{I}(A)_{\mathfrak{m}} \subset \mathcal{O}_{\mathbb{A}^n,p}$ by the injectivity part of Proposition 4.5.8, and our claim will follow from the surjectivity part of that proposition once we show that $I^e_{\mathfrak{m}} = \mathrm{I}(A)_{\mathfrak{m}}$. For this, we distinguish two cases.

If $p \in \mathbb{A}^n \setminus A$, there is a polynomial $f \in I^e \subset \mathrm{I}(A)$ which is not contained in $\mathfrak{m}$. Then f is a unit in $\mathcal{O}_{\mathbb{A}^n,p}$, which implies that $I^e_{\mathfrak{m}} = \mathrm{I}(A)_{\mathfrak{m}} = \mathcal{O}_{\mathbb{A}^n,p}$.

If $p \in A$, then $I^e \subset \mathrm{I}(A) \subset \mathfrak{m}$. By assumption, at least one $(n-d) \times (n-d)$ minor of $\left(\frac{\partial f_i}{\partial x_j}(p)\right)$ is nonzero, say $\det\left(\frac{\partial f_i}{\partial x_j}(p)\right)_{1 \le i,j \le n-d} \neq 0$. Then $(\langle f_1, \ldots, f_{n-d}\rangle\, \mathbb{K}[x_1, \ldots, x_n])_{\mathfrak{m}} = \mathrm{I}(A)_{\mathfrak{m}}$ by Proposition 4.6.25 and, thus, also $I^e_{\mathfrak{m}} = \mathrm{I}(A)_{\mathfrak{m}}$. □

Proof of Corollary 4.1.14. Supposing that $\Bbbk[x_1, \ldots, x_n]/I$ is Cohen-Macaulay of dimension d, we have to show: If

$$\dim \mathrm{V}(I_{n-d}\left(\frac{\partial f_i}{\partial x_j}\right) + I) < \dim \mathrm{V}(I) = d,$$

then $I^e = \mathrm{I}(A)$ and $\mathrm{V}(I_{n-d}\left(\frac{\partial f_i}{\partial x_j}\right) + I) = A_{\mathrm{sing}}$.

Arguing as in the previous proof, we see that the equality $I^e_{\mathfrak{m}} = \mathrm{I}(A)_{\mathfrak{m}}$ holds for the maximal ideal $\mathfrak{m}$ of any point $p \in A$ which is not contained in $B := \mathrm{V}(I_{n-d}(\frac{\partial f_i}{\partial x_j}) + I)$. On the other hand, by virtue of the Cohen-Macaulay assumption, we conclude from the Unmixedness Theorem 3.3.12 that I^e has only isolated primary components, all of dimension d. In particular, by the 2nd uniqueness theorem for primary decomposition, I^e admits a uniquely determined minimal primary decomposition, say, $I^e = \bigcap_{i=1}^t \mathfrak{q}_i$. The radicals $\mathfrak{p}_i = \operatorname{rad} \mathfrak{q}_i$ are the associated primes of $\mathrm{I}(A)$, and the vanishing loci $V_i = \mathrm{V}(\mathfrak{q}_i)$ are the irreducible components of A.

For each i, since $\dim V_i = d > \dim B$, there is a point $p_i \in V_i \setminus (B \cup \bigcup_{j \neq i} V_j)$. Localize $R = \mathbb{K}[x_1, \ldots, x_n]$ at the maximal ideal $\mathfrak{m}_i$ of p_i, and let $\iota : R \to R_{\mathfrak{m}_i}$ be the natural homomorphism. Then, by Proposition 4.5.5, we have $\mathfrak{q}_i = \iota^{-1}(I^e_{\mathfrak{m}_i}) = \iota^{-1}(\mathrm{I}(A)_{\mathfrak{m}_i}) = \mathfrak{p}_i$. This shows that $I^e = \mathrm{I}(A)$.

Replacing I by $\mathrm{I}(A)$ in the definition of B, we see that $\dim T_pA > d$ iff $p \in B$. Hence, $B = A_{\mathrm{sing}}$ since A is equidimensional of dimension d. □

4.7 Analytic Type and Tangent Cone

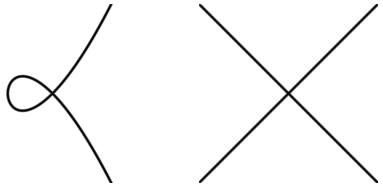
So far, we have defined two invariants of an algebraic set A at a point $p \in A$, namely the local ring $\mathcal{O}_{A,p}$ with its maximal ideal $\mathfrak{m}_{A,p}$, and the Zariski tangent space $T_pA \cong (\mathfrak{m}_{A,p}/\mathfrak{m}^2_{A,p})^*$. In this section, motivated by the fact that both invariants have their drawbacks at singular points, we will introduce two further invariants of A at p.

To begin, we note that the concept of the local ring is too fine at singular points in that two rings $\mathcal{O}_{A,p}$ and $\mathcal{O}_{B,q}$ may differ although our intuition is that locally, near p respectively q, the algebraic sets A and B look alike.

Example 4.7.1. For the plane curves

$$C = \mathrm{V}(y^2 - x^2 - x^3) \subset \mathbb{A}^2(\mathbb{C}) \text{ and } D = \mathrm{V}(v^2 - u^2) \subset \mathbb{A}^2(\mathbb{C}),$$

our intuitive understanding is that C and D look alike near the origin o:



$y^2 - x^2 - x^3 = 0$ $\qquad$ $v^2 - u^2 = 0$

Nevertheless, the local rings $\mathcal{O}_{C,o}$ and $\mathcal{O}_{D,o}$ are not isomorphic. In fact, since C is irreducible, $\mathcal{O}_{C,o}$ is a subring of the rational function field $\Bbbk(C)$ and, thus, an integral domain. In contrast, reflecting the fact that o is contained in two irreducible components of D, the ring $\mathcal{O}_{D,o}$ contains zerodivisors: $(v-u)(v+u) = 0 \mod \langle v^2 - u^2 \rangle$. □

From a geometric point of view, the problem in the example is that near the origin, both curves consist of two different "branches", but for the curve C, the decomposition into branches does not happen in a *Zariski* neighborhood of the origin. In terms of functions, the polynomial $y^2 - x^2 - x^3$ cannot be factored in $\mathcal{O}_{C.o}$. Naively, to overcome the problem, we should work with smaller neighborhoods and, correspondingly, a larger class of functions. This is easy to establish in case $\mathbb{K} = \mathbb{C}$ where we may consider arbitraryly small Euclidean neighborhoods and allow convergent power series as functions on these:

$$y^2 - x^2 - x^3 = (y + x\sqrt{1+x}) \cdot (y - x\sqrt{1+x}),$$

where the Taylor series

$$\sqrt{1+x} = \sum_{k=0}^{\infty} \binom{1/2}{k} x^k$$

is convergent for $|x| < 1$. Ring theoretically, this suggests to consider the local ring

$$\mathbb{C}\{x_1 - a_1, \ldots, x_n - a_n\}/\mathrm{I}(A)\,\mathbb{C}\{x_1 - a_1, \ldots, x_n - a_n\}$$

instead of the local ring

$$\mathcal{O}_{A,p} \cong \mathcal{O}_{\mathbb{A}^n(\mathbb{C}),p}/\mathrm{I}(A)\,\mathcal{O}_{\mathbb{A}^n(\mathbb{C}),p}.$$

Over an arbitrary field $\mathbb{K}$, there is no analogue to the Euclidean topology, and it is not meaningful to speak of convergent power series. We, may, however, consider the local ring

$$\mathbb{K}[[x_1 - a_1, \ldots, x_n - a_n]]/\mathrm{I}(A)\mathbb{K}[[x_1 - a_1, \ldots, x_n - a_n]].$$

It turns out that this ring is naturally obtained from the local ring $\mathcal{O}_{A,p}$ by completing $\mathcal{O}_{A,p}$ with respect to the $\mathfrak{m}_{A,p}$-adic topology.

In what follows, we describe the construction of the completion in a general algebraic context: Let R be any ring, and let $\mathfrak{m}$ be any ideal of R. Considering the $\mathfrak{m}$-adic topology on R, we call two Cauchy sequences $(f_\nu), (g_\nu) \subset R$ equivalent if the sequence of differences $(f_\nu - g_\nu)$ converges to zero. The set of all equivalence classes of Cauchy sequences carries a natural ring structure: If $(f_\nu), (g_\nu) \subset R$ are Cauchy sequences, then so are $(f_\nu + g_\nu)$ and $(f_\nu \cdot g_\nu)$, and the classes of these depend only on the classes of (f_ν) and (g_ν). Suppressing the ideal $\mathfrak{m}$ in our notation, we write $\widehat{R}$ for the resulting ring, and call it the **completion of R with respect to $\mathfrak{m}$**. For each $f \in R$, the class of the constant sequence (f) is an element $\iota(f) \in \widehat{R}$. This defines a ring homomorphism $\iota : R \to \widehat{R}$. The kernel of ι is the ideal $\bigcap_{k=0}^{\infty} \mathfrak{m}^k$. Hence, we may consider R as a subring of $\widehat{R}$ if this ideal is zero, that is, if R is Hausdorff with respect to the $\mathfrak{m}$-adic topology. By Krull's intersection theorem, this holds, in particular, if $(R, \mathfrak{m})$ is a local Noetherian ring.

In treating the completion of affine rings and, similarly, that of $\mathcal{O}_{A,p}$, we make use of the following lemma.

Lemma 4.7.2. *Let $I \subset \Bbbk[x_1, \ldots, x_n]$ be an ideal, let $>$ be a degree-anticompatible monomial order on $\Bbbk[x_1, \ldots, x_n]$, and let $f_1, \ldots, f_r$ form a Gröbner basis for I. Then, for any $k \geq 1$, the f_i together with the monomials of degree k form a Gröbner basis for the ideal $I + \langle x_1, \ldots, x_n \rangle^k$.*

Proof. We write $\mathcal{G}$ for the set of proposed Gröbner basis elements. By assumption, the remainder in any standard expression for an S-polynomial of type $\mathrm{S}(f_i, f_j)$ in terms of $\mathcal{G}$ is zero. On the other hand, each term of an S-polynomial of type $\mathrm{S}(f_i, x^\alpha)$, where $|\alpha| = k$, has degree $\geq k$ since with respect to $>$, $\mathbf{L}(f_i)$ is chosen among the lowest degree terms of f_i. Hence, also in this case, Buchberger's test yields a remainder which is zero. □

Proposition 4.7.3. *If $R = \Bbbk[x_1, \ldots, x_n]/I$ is an affine ring, the completion of R with respect to the maximal ideal $\mathfrak{m} = \langle \overline{x}_1, \ldots, \overline{x}_n \rangle \subset R$ is*

$$\widehat{R} \cong \Bbbk[[x_1, \ldots, x_n]]/I\,\Bbbk[[x_1, \ldots, x_n]].$$

Proof. Let $I^e = I\,\Bbbk[[x_1, \ldots, x_n]]$. Given a power series $g = \sum_\alpha a_\alpha x^\alpha \in \Bbbk[[x_1, \ldots, x_n]]$, we write $g^{(\nu)}$ for the truncation $\sum_{|\alpha| \leq \nu} a_\alpha x^\alpha$. Associating to each g the sequence of truncations $(g^{(\nu)})$ and taking residue classes, we get a homomorphism

$$\phi : \Bbbk[[x_1, \ldots, x_n]] \to \widehat{R}$$

with $I^e \subset \ker \phi$. The proposition will follow once we show that $I^e = \ker \phi$, and that ϕ is surjective. For this, fix a degree-anticompatible monomial order on $\Bbbk[x_1, \ldots, x_n]$.

We first show that $I^e = \ker \phi$. Given $g \in \ker \phi$, let $h \in \Bbbk[[x_1, \ldots, x_n]]$ be the normal form of g mod I^e. Then, in particular, no term of h is contained in $\mathbf{L}(I)$. Moreover, since $\phi(g) = 0$, also $\phi(h) = 0$. In terms of the truncations $h^{(\nu)}$ this means that for all $k \geq 0$, there is an index ν_0 such that $h^{(\nu)} + I \in \mathfrak{m}^k$ for all $\nu \geq \nu_0$. By Lemma 4.7.2, the latter condition is equivalent to $h^{(\nu)} \in I + \langle x_1, \ldots, x_n \rangle^k$ for all $\nu \geq \nu_0$. Since k can be chosen arbitarily high, we have $\mathbf{L}(h) \in \mathbf{L}(I)$. By the choice of h, this is only possible if $h = 0$ and, thus, $g \in I^e$.

Next, we show that ϕ is surjective. For this, consider a sequence of polynomials (g_ν) in $\Bbbk[x_1, \ldots, x_n] \subset \Bbbk[[x_1, \ldots, x_n]]$ which represents a Cauchy sequence in R. For each ν, let $h_\nu \in \Bbbk[[x_1, \ldots, x_n]]$ be the normal form of g_ν mod I^e. By Lemma 4.7.2, given $\nu, k \geq 0$, the truncation $h_\nu^{(k)}$ coincides with the normal form of g_ν mod $I + \langle x_1, \ldots, x_n \rangle^{k+1}$. In particular, for each k, the sequence of polynomials $h_\nu^{(k)}$, $\nu \geq 0$, is ultimately constant, say $h_\nu^{(k)} = f_k$ for $\nu \gg 0$. Then $f_\ell - f_k \in \langle x_1, \ldots, x_n \rangle^k$ for $\ell \geq k$. We conclude that the f_k constitute a power series whose image under ϕ in $\widehat{R}$ coincides with the class represented by (g_ν). □

Exercise 4.7.4. Let R be a ring, let $\mathfrak{m}$ be an ideal of R, and let $\widehat{R}$ be the completion of R with respect to $\mathfrak{m}$. Show:

1. If R is Noetherian, then so is $\widehat{R}$.
2. If R is Hausdorff with respect to the $\mathfrak{m}$-adic topology, then $\widehat{R}$ is complete with respect to $\mathfrak{m}\widehat{R}$.
3. If $\mathfrak{m}$ is a maximal ideal, then $\widehat{R}$ is a local ring with maximal ideal $\mathfrak{m}\widehat{R}$. Furthermore, $\widehat{R} = \widehat{R}_{\mathfrak{m}}$, where $\widehat{R}_{\mathfrak{m}}$ denotes the completion of the local ring $R_{\mathfrak{m}}$ with respect to its maximal ideal. □

Now, we focus on the completion of $\mathcal{O}_{A,p}$ with respect to $\mathfrak{m}_{A,p}$, denoted $\widehat{\mathcal{O}}_{A,p}$. By translating p to the origin and by either imitating the proof of Proposition 4.7.3 or by combining the proposition with part 3 of the exercise, we get:

Corollary 4.7.5. *Let $A \subset \mathbb{A}^n$ be an algebraic set, and let $p = (a_1, \ldots, a_n) \in A$ be a point. Then*

$$\widehat{\mathcal{O}}_{A,p} \cong \mathbb{K}[[x_1 - a_1, \ldots, x_n - a_n]]/\mathrm{I}(A)\,\mathbb{K}[[x_1 - a_1, \ldots, x_n - a_n]].$$

□

With respect to dimension, we have:

Corollary 4.7.6. *Let $A \subset \mathbb{A}^n$ be an algebraic set, and let $p \in A$ be a point. Then*

$$\dim \mathcal{O}_{A,p} = \dim \widehat{\mathcal{O}}_{A,p}.$$

□

Exercise 4.7.7. Prove Corollary 4.7.6.
Hint. Consider systems of parameters in both rings $\mathcal{O}_{A,p}$ and $\widehat{\mathcal{O}}_{A,p}$. Furthermore, consider the natural projection $\mathbb{K}[[x_1 - a_1, \ldots, x_n - a_n]] \to \widehat{\mathcal{O}}_{A,p}$ from Corollary 4.7.5 and make use of Exercise 1.9.3. □

Our next result refines Proposition 4.6.24. In particular, we show once more that the local ring of an algebraic set at a smooth point is an integral domain.

Corollary 4.7.8. *Let $A \subset \mathbb{A}^n$ be an algebraic set, and let $p \in A$ be a point.*

1. *If p is a smooth point of A, then*

$$\widehat{\mathcal{O}}_{A,p} \cong \mathbb{K}[[t_1, \ldots, t_d]], \quad \textit{where} \quad d = \dim_p A = \dim \mathcal{O}_{A,p}.$$

2. *More generally, if p is arbitrary, we have a representation of $\widehat{\mathcal{O}}_{A,p}$ as a quotient*

$$\widehat{\mathcal{O}}_{A,p} \cong \mathbb{K}[[t_1, \ldots, t_e]]/J, \quad \textit{where} \quad e = \dim_{\mathbb{K}} T_p A,$$

and where J is an ideal of $\mathbb{K}[[t_1, \ldots, t_e]]$ such that $J \subset \langle t_1, \ldots, t_e \rangle^2$.

Proof. We assume that $p = o$ is the origin.

1. By part 1 and the principal ideal theorem, any quotient of $\mathbb{K}[[t_1, \ldots, t_d]]$ by a nonzero ideal J has dimension $< d$ since $\mathbb{K}[[t_1, \ldots, t_d]]$ is an integral domain. Hence, part 1 is a special case of part 2.

2. If $\mathrm{I}(A) = \langle f_1, \ldots, f_r \rangle$, then $T_p A = \mathrm{V}(d_p f_i \mid i = 1, \ldots, r) \subset \mathbb{A}^n$. We may, hence, choose coordinates $x_1, \ldots, x_n$ such that $d_p f_i = x_i$, for $i = 1 \ldots, n - e$, and such that $f_i \in \langle x_1, \ldots, x_n \rangle^2$, for $i > n - e$. Sending the t_i to the x_{n-e+i} and composing with the natural projection $\mathbb{K}[[x_1 - a_1, \ldots, x_n - a_n]] \to \widehat{\mathcal{O}}_{A,p}$ from Corollary 4.7.5, we get a ring homomorphism

$$\phi : \mathbb{K}[[t_1, \ldots, t_e]] \to \mathbb{K}[[x_1, \ldots, x_n]] \to \widehat{\mathcal{O}}_{A,o}.$$

To show that ϕ is surjective, fix a degree-anticompatible monomial order on $\mathbb{K}[x_1, \ldots, x_n]$. Given an element $\widehat{g} \in \widehat{\mathcal{O}}_{A,o}$, choose a power series $g \in \mathbb{K}[[x_1, \ldots, x_n]]$ representing $\widehat{g}$, and let h be the normal form of g mod $\mathrm{I}(A)$. Then h also represents $\widehat{g}$. Moreover, no term of h is contained in $\mathbf{L}(\mathrm{I}(A))$. Since $\mathbf{L}(f_i) = x_i$ for $i = 1, \ldots, n - e$, it follows that h is in the image of $\mathbb{K}[[t_1, \ldots, t_e]] \to \mathbb{K}[[x_1, \ldots, x_n]]$.

To finish the proof, we note that $J := \ker \phi$ is contained in $\langle t_1, \ldots, t_e \rangle^2$ since $f_{n-e+1}, \ldots, f_r \in \langle x_1, \ldots, x_n \rangle^2$. □

In the situation of the corollary, the number $e = \dim_{\mathbb{K}} T_p A$ is called the **embedding dimension** of the pair (A, p). Note that always $n \geq e$. We say that (A, p) is **minimally embedded** in $(\mathbb{A}^n, p)$ if $n = e$.

Exercise 4.7.9. For $\mathcal{O}_o$ and $\mathbb{K}[[x_1, \ldots, x_n]]$, formulate and prove statements analogous to those in Propositions 3.3.3 and 3.3.11 on Noether normalization respectively to those in the Unmixedness Theorem 3.3.12. □

Definition 4.7.10. *Given affine algebraic sets A, B and points $p \in A$, $q \in B$, we call the pairs (A,p) and (B,q)* **analytically isomorphic** *if $\widehat{\mathcal{O}}_{A,p} \cong \widehat{\mathcal{O}}_{B,q}$ as $\mathbb{K}$-algebras.* □

Example 4.7.11. In Example 4.7.1, the pairs (C,o) and (D,o) are analytically isomorphic. Indeed, by the formal inverse function theorem (see Exercise 4.4.30), the homomorphism

$$\phi : \mathbb{C}[[u,v]] \to \mathbb{C}[[x,y]]$$

obtained by substituting

$$u \mapsto x\sqrt{1+x} = x\sum_{k=0}^{\infty}\binom{1/2}{k}x^k,\ v \mapsto y,$$

is an isomorphism. Since ϕ maps v^2-u^2 to $y^2-x^2-x^3$, it induces the desired isomorphism

$$\widehat{\mathcal{O}}_{D,o} \cong \mathbb{C}[[u,v]]/\langle v^2-u^2\rangle \to \mathbb{C}[[x,y]]/\langle y^2-x^2-x^3\rangle \cong \widehat{\mathcal{O}}_{C,o}.$$

□

In particular, the analytic type is a coarser invariant than the local ring. It is finer than the tangent space: If $R = \widehat{\mathcal{O}_{A,p}}$, and $\mathfrak{m}$ is the maximal ideal of R, then $\mathfrak{m}/\mathfrak{m}^2 \cong \mathfrak{m}_{A,p}/\mathfrak{m}_{A,p}^2$. Indeed there is a well-defined map $\mathfrak{m}_{A,p} \to \mathfrak{m} \to \mathfrak{m}/\mathfrak{m}^2$ of $\mathcal{O}_{A,p}$-modules which is surjective with kernel $\mathfrak{m}_{A,p}^2$.

Remark 4.7.12. Let $\mathbb{K} = \mathbb{C}$, let A, B be analytic sets, and let $p \in A$, $q \in B$ be points. Suppose that (A,p), (B,q) are minimally embedded in $(\mathbb{A}^e, o)$. Moreover, suppose that (A,p) and (B,q) are analytically isomorphic, where the isomorphism $\widehat{\mathcal{O}_{B,q}} \to \widehat{\mathcal{O}_{A,p}}$ is given by an e-tuple of *convergent* power series $(z_1,\ldots,z_e)$. In this case, there are neighborhoods U of $p \in \mathbb{A}^e(\mathbb{C})$ and V of $q \in \mathbb{A}^e(\mathbb{C})$ in the Euclidean topology such that

$$z : U \to V,\ a \mapsto (z_1(a),\ldots,z_e(a)),$$

is biholomorphic, and with $z(A \cap U) = B \cap V$. □

Exercise 4.7.13. Let p be a point of a plane curve $C \subset \mathbb{A}^2$.

1. Assume $\operatorname{char}\mathbb{K} \neq 2$. Show that p is a node respectively a cusp of C iff (C,p) is analytically isomorphic to $\mathrm{V}(y^2-x^2)$ respectively $\mathrm{V}(y^2-x^3)$.
2. Show that p is an ordinary triple point iff (C,p) is analytically isomorphic to $\mathrm{V}(xy(x-y))$. □

The precise definition of a tacnode is as follows (see Examples 4.3.1 and 4.3.6):

Definition 4.7.14. Assume $\operatorname{char}\mathbb{K} \neq 2$. A point p of a plane curve $C \subset \mathbb{A}^2$ is called a **tacnode** if (C,p) is analytically isomorphic to $(\mathrm{V}(y^2-x^4), o)$. □

Exercise 4.7.15. Let $f \in \mathbb{K}[x,y]$ be a square-free polynomial, and let $C = \mathrm{V}(f) \subset \mathbb{A}^2$.

1. Show that C has at most nodes as singularities iff $\langle f, \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}\rangle \subset \mathbb{K}[x,y]$ is a radical ideal.
2. Show that C has at most double points as singularities iff
$$\langle f, \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}, \frac{\partial^2 f}{\partial x^2}, \frac{\partial^2 f}{\partial x \partial y}, \frac{\partial^2 f}{\partial y^2}\rangle = \langle 1\rangle \subset \mathbb{K}[x,y].$$
3. Formulate and prove a criterion for C to have at most nodes and cusps as singularities.
4. The curve defined by
$$f = x^4 + y^4 - 8x^3 + 18xy^2 + 18x^2 + \frac{27}{2}y^2 - 27$$
has only nodes and cusps as singularities. How many of each type are there? □

We, now, turn from the local ring to the tangent space. The drawback of T_pA is that it fails to approximate A near a singular point $p \in A$. In fact, in this case, the dimension of T_pA, which determines T_pA as a $\mathbb{K}$-vector space up to isomorphism, is simply too big. In this sense, T_pA is too coarse at a singular point. To overcome this failure, we introduce our second new invariant of A at p which is the tangent cone TC_pA. This coincides with T_pA at a smooth point, but is better behaved than T_pA at a singular point.

Recall that according to our definitions, the tangent space at a smooth point is the union of lines which can be seen as the analogue of limiting positions of secant lines in calculus. Mimicing this if A is not necessarily smooth at p gives the tangent cone.

We suppose for simplicity that $p = o = (0,\ldots,0) \in A$ is the origin. Then the lines through p admit parametrizations of type $t \to tv$, where $v \in \mathbb{A}^n$, and every secant line to A through p gives a point $tv \in A$ with $t \neq 0$. We are interested in what is happening if t tends to zero. Consider the set
$$B = \{(v,t) \in \mathbb{A}^n \times \mathbb{A}^1 \mid tv \in A\} \subset \mathbb{A}^n \times \mathbb{A}^1 \cong \mathbb{A}^{n+1}.$$
As we will see more clearly in the proof of proposition 4.7.16 below, B is an algebraic set. Obviously, $B_1 = \mathbb{A}^n \times \{o\}$ is an irreducible component of B (if $B \neq \mathbb{A}^n$). We write $B_2 = \overline{B \setminus B_1}$ for the residual algebraic set. The **tangent cone** of A at o is defined to be the algebraic set
$$TC_oA = B_1 \cap B_2 \subset \mathbb{A}^n \times \{o\} \cong \mathbb{A}^n.$$
In determining equations for the tangent cone, given a polynomial $f \in \Bbbk[x_1,\ldots,x_n]$, we write $m = \mathrm{mult}(f,o)$, and denote by f_i the homogeneous component of f of degree i.

Proposition 4.7.16. *Let $I \subset \Bbbk[x_1, \ldots, x_n]$ be an ideal, and let $A = \mathrm{V}(I) \subset \mathbb{A}^n$. Suppose that A contains the origin o. Then, with notation as above, the tangent cone $TC_oA \subset \mathbb{A}^n$ is the locus of zeros of the ideal*

$$J = \langle \{ f_m \mid f \in I \} \rangle.$$

Proof. The set $B \subset \mathbb{A}^n \times \mathbb{A}^1$ is the common vanishing locus of the polynomials

$$f(tx) = t^m f_m(x) + t^{m+1} f_{m+1}(x) + \ldots + t^d f_d(x), \quad f \in I$$

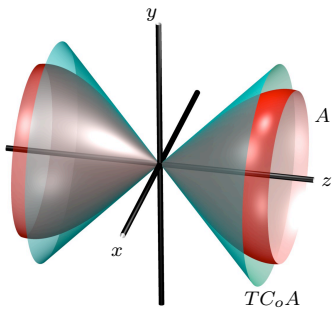
(note that $m \geq 1$ since $o \in A$). Saturating with respect to t, we obtain equations for the algebraic set residual to $B_1 = \mathrm{V}(t)$. That is, $B_2 \subset \mathbb{A}^n \times \mathbb{A}^1$ is the common vanishing locus of the polynomials

$$f_m(x) + t f_{m+1}(x) + \ldots + t^{d-m} f_d(x), \quad f \in I.$$

As a subset of $\mathbb{A}^n$, the intersection $B_1 \cap B_2 \subset \mathbb{A}^n \times \{o\} \cong \mathbb{A}^n$ is, then, defined by the ideal J. □

In particular, if $A = \mathrm{V}(f) \subset \mathbb{A}^n$ is a hypersurface with $o \in A$, then TC_oA is defined by the vanishing of the lowest degree part of f.

Example 4.7.17. If $A = \mathrm{V}(x^2 + y^2 - z^2 + z^4)$, then $TC_oA = \mathrm{V}(x^2 + y^2 - z^2)$.



□

Being defined by homogenous polynomials, TC_oA is the union of lines through the origin and, thus, indeed a cone: With notation as in the proposition, if $o \neq p \in TC_oA$ is a point, and $q = \lambda p$ is any point on the line $\overline{op}$, then $f_m(q) = \lambda^m f_m(p) = 0$ for all $f_m \in J$, so that $q \in TC_oA$ as well. See also Exercise 4.7.19, where we will give an alternative description of the tangent cone. Furthermore, note that TC_oA is contained in the tangent space T_oA. In fact, according to our definitions, if $I = \mathrm{I}(A) \subset \mathbb{K}[x_1, \ldots, x_n]$ is the vanishing ideal of A, then the linear polynomials in J define the tangent space T_oA.

Exercise 4.7.18. In the situation of the proposition, let $f_1, \ldots, f_r$ be a Gröbner basis for the ideal $I\mathcal{O}_o$ with respect to a degree-anticompatible monomial order on $\Bbbk[x_1, \ldots, x_n]$. Then show that $TC_oA = \mathrm{V}((f_1)_m, \ldots, (f_r)_m)$. □

Remark 4.7.19. In more abstract terms the ring of the tangent cone can be defined as the graded ring

$$grR = R/\mathfrak{m} \oplus \mathfrak{m}/\mathfrak{m}^2 \oplus \mathfrak{m}^2/\mathfrak{m}^3 \oplus \dots,$$

where R can be either the local ring or its completion. This shows that TC_pA depends only on $\widehat{\mathcal{O}_{A,p}}$. □

Example 4.7.20. Consider the algebraic set $A = \mathrm{V}(f_1, f_2, f_3, f_4) \subset \mathbb{A}^4$, where

$$\begin{aligned} f_1 &= x_2^3 - x_1^2x_3 + x_1x_2x_4 - x_1x_3x_4 - x_2x_4^2 - x_1x_2, \\ f_2 &= x_1x_2^2 - x_1x_3^2 + 2x_2x_3x_4 - x_3^2x_4 - x_2x_3, \\ f_3 &= x_1^3 - x_1x_2x_3 + x_2^2x_4 + x_1x_4^2 - x_4^3 - x_1x_4, \\ f_4 &= x_1^2x_3 - x_2x_3^2 + x_1x_2x_4 + 2x_3x_4^2 - x_3x_4. \end{aligned}$$

In the exercise below, we will show that these polynomials form a Gröbner basis with respect to $>_{\mathrm{ldrlex}}$. Thus, the tangent cone of A at the origin $o \in \mathbb{A}^4$ is defined by the ideal

$$\langle x_1x_2, x_2x_3, x_1x_4, x_3x_4\rangle = \langle x_1, x_3\rangle \cap \langle x_2, x_4\rangle$$

which gives two planes in $\mathbb{A}^4$ intersecting at o. □

Exercise 4.7.21. Check the assertion about the Gröbner basis in Example 4.7.20. Then show that (A, o) and (TC_pA, o) are analytically isomorphic. □

In general, a singularity p of an algebraic set A is called an **improper node** if (A, o) and (TC_pA, o) are analytically isomorphic.

Exercise 4.7.22. Show that an ordinary quadrupel point is analytically isomorphic to a curve of type

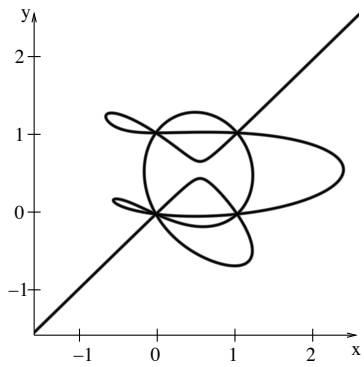
$$C_\lambda := \mathrm{V}(xy(y-x)(y-\lambda x)), \text{ where } \lambda \in \Bbbk \setminus \{0, 1\}.$$

Furthermore, show that two such curves C_λ and $C_{\lambda'}$ are analytically isomorphic iff

$$\lambda' \in \{\lambda,\ 1-\lambda,\ 1/\lambda, 1/(1-\lambda),\ (\lambda-1)/\lambda,\ \lambda/(\lambda-1)\}.$$ □

4.8 Additional Exercises

Exercise 4.8.1.
For the curve $\mathrm{V}(f) \subset \mathbb{A}^2(\mathbb{C})$ considered in part 2 of Exercise 4.1.5, determine the multiplicity at each singular point. Are all singular points ordinary multiple points?


y
2
1
0
−1
−1
0
1
2
x

□

Part II

Projective Algebraic Geometry

Chapter 5

Linear Systems of Plane Curves

This chapter provides a first impression of projective algebraic geometry. We will consider a new ambient space, projective n-space $\mathbb{P}^n(\Bbbk)$, which is obtained from affine n-space $\mathbb{A}^n(\Bbbk)$ by adding a "point at infinity in every direction". In this larger space, many geometric statements become simpler in that special cases are avoided.

The additional points form a hyperplane $H \subset \mathbb{P}^n(\Bbbk)$ which is often referred to as the "hyperplane at infinity". In fact, starting from a more formal definition of $\mathbb{P}^n(\Bbbk)$, we will see that there are many ways of writing $\mathbb{P}^n(\Bbbk)$ as the union of an "affine chart" $\mathbb{A}^n(\Bbbk)$ and a hyperplane at infinity. Local concepts can be extended from $\mathbb{A}^n(\Bbbk)$ to $\mathbb{P}^n(\Bbbk)$ by considering a covering of $\mathbb{P}^n(\Bbbk)$ by affine charts.

The introduction of homogeneous coordinates will allow us to define a projective algebraic set as the common locus of zeros of a collection of *homogeneous* polynomials. With respect to an affine chart, a projective algebraic set can be regarded as an affine algebraic set "completed" by adding relevant points at infinity (over the real or complex numbers, considering the Euclidean topology instead of the Zariski topology, the projective algebraic set is a natural compactification of the affine algebraic set). Postponing the general study of this and other facts about projective algebraic sets to the next chapter, we will, in this chapter, mainly focus on projective hypersurfaces, specifically on projective plane curves.

The natural parameter space for projective plane curves of a given degree d is a projective space itself. Its linear subspaces are classically known as linear systems of plane curves of degree d. They arise naturally in the context of a number of geometric questions. In fact, many geometric conditions on plane curves are linear in that the curves satisfying these conditions form a linear system. For instance, given a finite set of points in $\mathbb{P}^n(\Bbbk)$, we impose linear conditions by asking that the curves under consideration pass through these points (have multiplicities exceeding particular values at these points). After a basic treatment of linear systems in Section 5.3, we will use resultants to prove Bézout's theorem. Given two *projective* plane curves of degrees d, e

without a common component over an algebraically closed field, the theorem states that C and D intersect in $d \cdot e$ points, counted with multiplicity. As applications of Bézout's theorem, we will show how to bound the number of singular points of a plane curve and how to compute parametrizations of a rational plane curve with at most ordinary singularities.

In Section 5.5, we will treat Max Noether's fundamental theorem which, as we will see in Chapter 8, is central to the proof of the Riemann-Roch theorem given by Brill and Noether. Applications of Noether's result presented in this chapter are Pascal's theorem on the mystic hexagon and its generalizations.

In the final section of this chapter, we will define an addition law for points on cubic curves. We will use a general version of Pascal's theorem to show that this addition law is associative (and, thus, indeed a group law). We will, then, give a sketch of further results on cubic curves. In particular, we will adress the topology and the arithmetic of cubic curves.

5.1 Projective Space and Projective Algebraic Sets

In the *affine* plane, Bézout's theorem already fails in simple cases. For instance, two distinct circles have at most two points of intersection, even if we allow complex solutions and take multiplicities into account (see Exercise 5.3.10). Still simpler, two distinct lines do not intersect if they are parallel. The construction of the projective plane is custom-made to remedy the situation in the case of lines. As we will see in Section 5.4.8, it is universal enough to make Bézout's theorem hold in general.

Intuitively, we think of parallel lines as meeting at an "infinitely distant point" on the horizon (Renaissance painters referred to these points as *vanishing points* and used them as in Figure 5.2 to allow for perspective drawing):

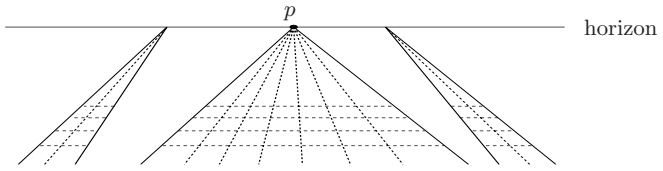


Fig. 5.1. *Vanishing points on the horizon*

Taking into account that the relation on lines in $\mathbb{A}^2(\mathbb{R})$ defined by 'is parallel to' is an equivalence relation, the idea is to require that all lines in a given equivalence class meet in the same point at infinity, with different classes corresponding to different points. Writing H for the set of all these points, we provisionally define the projective plane $\mathbb{P}^2(\mathbb{R})$ by setting

$$\mathbb{P}^2(\mathbb{R}) = \mathbb{A}^2(\mathbb{R}) \cup H.$$

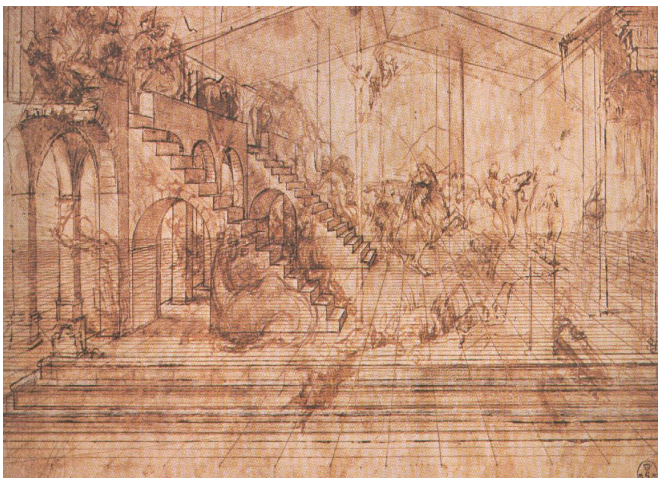


Fig. 5.2. *A sketch by Leonardo da Vinci*

A line in $\mathbb{P}^2(\mathbb{R})$ is, then, a line $L \subset \mathbb{A}^2(\mathbb{R})$ together with the common point at infinity of all lines parallel to L. Moreover, we regard H as a line in $\mathbb{P}^2(\mathbb{R})$, and call it the **line at infinity**. This makes sense since, now, any pair of distinct lines determines a unique point, and any pair of distinct points determines a unique line. Note that Figure 5.1 is somewhat inaccurate in that the horizon is not representing all points of H: It is missing the point at infinity of the lines "parallel to the horizon".

Our provisional definition makes it cumbersome to work with $\mathbb{P}^2(\mathbb{R})$ since the points of $\mathbb{P}^2(\mathbb{R})$ are not treated on equal footing. To motivate the formal definition below, we write x_0, x_1, x_2 for the coordinates on the affine 3-space $\mathbb{A}^3(\mathbb{R})$, and choose $\mathrm{V}(x_0 - 1) \subset \mathbb{A}^3(\mathbb{R})$ as a reference plane for $\mathbb{A}^2(\mathbb{R})$:
Each point of $\mathbb{A}^2(\mathbb{R})$ determines, then, a line in $\mathbb{A}^3(\mathbb{R})$ through the origin o. In this way, we get all lines through o, except those lying in the plane $\mathrm{V}(x_0)$. The latter lines, in turn, form a copy of H. Indeed, the span of a given line $L \subset \mathbb{A}^2(\mathbb{R})$ and o intersects $\mathrm{V}(x_0)$ in a line through o which only depends on the class of lines parallel to L. We make the following general definition:

Definition 5.1.1. The **projective n-space** over the field $\Bbbk$ is the set

$$\begin{aligned}\mathbb{P}^n(\Bbbk) &= \big\{\text{lines through the origin in } \mathbb{A}^{n+1}(\Bbbk)\big\} \\ &= \big\{\text{one-dimensional linear subspaces of } \Bbbk^{n+1}\big\}.\end{aligned}$$

□

Considering a line L through the origin $o \in \mathbb{A}^{n+1}(\Bbbk)$ as an element of the new space $\mathbb{P}^n(\Bbbk)$, we call it a **point** of $\mathbb{P}^n(\Bbbk)$. If p denotes this point, then p is determined (or represented) by any point $(a_0, \ldots, a_n) \in L \setminus \{o\}$. Accordingly, we write $p = [a_0 : \cdots : a_n]$, and call $a_0, \ldots, a_n$ a set of **homogeneous**

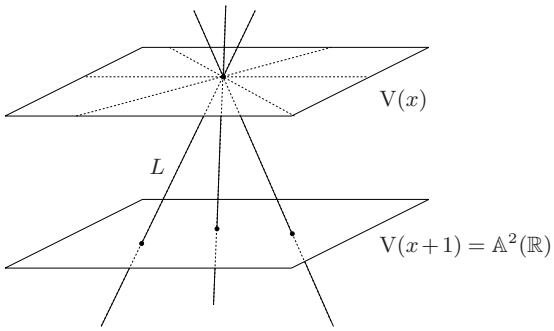


Fig. 5.3.

coordinates for p. Here, the colons and square brackets indicate that the homogeneous coordinates are determined up to a nonzero scalar multiple (if $a_i \neq 0$, the ratio $a_j : a_i$ depends on p only). Representing the points of $\mathbb{P}^n(\Bbbk)$ in this way means that we regard $\mathbb{P}^n(\Bbbk)$ as the quotient of $\mathbb{A}^{n+1}(\Bbbk) \setminus \{o\}$ modulo the equivalence relation defined by $(a_0, \ldots, a_n) \sim (b_0, \ldots, b_n)$ iff $(a_0, \ldots, a_n) = \lambda(b_0, \ldots, b_n)$ for some nonzero scalar λ:

$$\mathbb{P}^n(\Bbbk) \cong \big(\mathbb{A}^{n+1}(\Bbbk) \setminus \{o\}\big) / \sim,$$

and we have the canonical projection

$$\pi : \mathbb{A}^{n+1}(\Bbbk) \setminus \{o\} \to \mathbb{P}^n(\Bbbk),\ (a_0, \ldots, a_n) \mapsto [a_0 : \cdots : a_n].$$

Remark-Definition 5.1.2. 1. It is often useful to have a basis-free definition of $\mathbb{P}^n$. If W is any $\Bbbk$-vector space of dimension $n+1$, then

$$\mathbb{P}(W) = \big\{\text{one-dimensional linear subspaces of } W\big\}$$

is called the **projective space of lines in W**. Of course, after choosing a $\Bbbk$-basis for W, we can identify $\mathbb{P}(W)$ with $\mathbb{P}^n(\Bbbk)$, and regard the homogeneous coordinates on $\mathbb{P}^n(\Bbbk)$ as homogeneous coordinates on $\mathbb{P}(W)$.

2. If $(t_{ij}) \in \mathrm{GL}(n+1, \Bbbk)$ is an invertible matrix, the linear change of coordinates $x_i \mapsto \sum t_{ij} x_j$ induces a bijective map

$$T : \mathbb{P}^n(\Bbbk) \to \mathbb{P}^n(\Bbbk),\ [a_0 : \cdots : a_n] \mapsto (\sum t_{0j} a_j : \cdots : \sum t_{nj} a_j).$$

Any such map is called a **change of coordinates** of $\mathbb{P}^n(\Bbbk)$. Since multiples of the identity matrix act trivial, we are led to consider the group

$$\mathrm{PGL}(n+1, \Bbbk) := \mathrm{GL}(n+1, \Bbbk)/\Bbbk^*$$

which is called the **projective general linear group**. Later in the book, once we will have introduced morphisms between projective algebraic sets, we will see that any automorphism of $\mathbb{P}^n(\Bbbk)$ is an element of $\mathrm{PGL}(n+1, \Bbbk)$:

$$\mathrm{Aut}(\mathbb{P}^n(\Bbbk)) = \mathrm{PGL}(n+1, \Bbbk)$$

3. Two subsets $A, B \subset \mathbb{P}^n(\Bbbk)$ are called **projectively equivalent** if there is a change of coordinates T of $\mathbb{P}^n(\Bbbk)$ such that $T(A) = B$.
4. We say that $\mathbb{P}^1(\Bbbk)$ and $\mathbb{P}^2(\Bbbk)$ are the **projective line** and the **projective plane** over $\Bbbk$, respectively. □

In contrast to the affine case, the homogeneous coordinates do not constitute functions on $\mathbb{P}^n(\Bbbk)$. More generally, given any nonconstant polynomial $f \in \Bbbk[x_0, \ldots, x_n]$, the value $f(a_0, \ldots, a_n)$ depends on the choice of homogeneous coordinates for the point $p = [a_0 : \cdots : a_n] \in \mathbb{P}^n(\Bbbk)$ and can, therefore, not be called the value of f at p. Note, however, that if f is *homogeneous*, then $f(\lambda x_0, \ldots, \lambda x_n) = \lambda^{\deg(f)} f(x_0, \ldots, x_n)$ for all nonzero scalars λ, so that

$$f(a_0, \ldots, a_n) = 0 \iff \forall\, \lambda \in \Bbbk \setminus \{0\} :\ f(\lambda a_0, \ldots, \lambda a_n) = 0.$$

As a consequence, any homogeneous polynomial $f \in \Bbbk[x_0, \ldots, x_n]$ has a well-defined **locus of zeros** (or **vanishing locus**) $\mathrm{V}(f)$ in $\mathbb{P}^n(\Bbbk)$. If f is nonconstant, we say that $\mathrm{V}(f)$ is a **hypersurface** in $\mathbb{P}^n(\Bbbk)$. A hypersurface in $\mathbb{P}^2(\Bbbk)$ is called a **projective plane curve**.

More generally, if $T \subset \Bbbk[x_1, \ldots, x_n]$ is any subset of homogeneous polynomials, its **locus of zeros** (or **vanishing locus**) is the set

$$\mathrm{V}(T) = \{p \in \mathbb{A}^n(\Bbbk) \mid f(p) = 0 \text{ for all } f \in T\}.$$

If $T = \{f_1, \ldots, f_r\}$ is finite, we write $\mathrm{V}(f_1, \ldots, f_r) = \mathrm{V}(T)$.

Definition 5.1.3. A subset $A \subset \mathbb{P}^n(\Bbbk)$ is called an **algebraic subset** if $A = \mathrm{V}(T)$ for some subset $T \subset \Bbbk[x_0, \ldots, x_n]$ of homogeneous polynomials. A **projective algebraic set** is an algebraic subset of some $\mathbb{P}^n(\Bbbk)$. □

Remark-Definition 5.1.4. As for $\mathbb{A}^n(\Bbbk)$, the **distinguished open sets**

$$\mathrm{D}(f) := \mathbb{P}^n(\Bbbk) \setminus \mathrm{V}(f), \quad f \in \Bbbk[x_0, \ldots, x_n] \text{ homogeneous},$$

form the basis for a topology on $\mathbb{P}^n(\Bbbk)$ whose closed sets are the algebraic subsets of $\mathbb{P}^n(\Bbbk)$. This topology (the topology induced on any subset) is called the **Zariski topology** on $\mathbb{P}^n(\Bbbk)$ (on the subset). An algebraic subset of $\mathbb{P}^n(\Bbbk)$ is called **irreducible** (a **subvariety** of $\mathbb{P}^n(\Bbbk)$) if it cannot be written as a union of two strictly smaller closed subsets. A **projective variety** is a subvariety of some $\mathbb{P}^n(\Bbbk)$. Every nonempty Zariski open subset of a projective variety A is Zariski dense in A (see Proposition 1.11.8 and its proof). □

If not otherwise mentioned, subsets of $\mathbb{P}^n(\Bbbk)$ will carry the Zariski topology.

Exercise* 5.1.5. Recall that a map between topological spaces is said to be **open** if it sends open sets to open sets. Show: The canonical projection $\pi : \mathbb{A}^{n+1}(\Bbbk) \setminus \{o\} \to \mathbb{P}^n(\Bbbk)$ is continous and open with regard to the respective Zariski topologies. □

Remark-Definition 5.1.6. Given a subset of homogeneous polynomials $T \subset \Bbbk[x_0, \ldots, x_n]$, rather than looking at the vanishing locus $A = \mathrm{V}(T) \subset \mathbb{P}^n$, we might also look at the vanishing locus of T in $\mathbb{A}^{n+1}$. This locus is a cone with vertex o: It is the union of all lines in $\mathbb{A}^{n+1}$ through o which correspond to points in A. We call this cone the **affine cone** over A, written $C(A)$. □

Classically, homogenous polynomials are known as **forms**. The adjectives **linear**, **quadratic**, **cubic**, **quartic**, **quintic** refer to forms of degree 1,2,3,4,5, respectively.

Example 5.1.7. The subsets of $\mathbb{P}^n(\Bbbk)$ defined by linear forms are precisely the subsets $\mathbb{P}(W) \subset \mathbb{P}^n(\Bbbk)$, where $W \subset \Bbbk^{n+1}$ is a linear subspace. Every such subset is called a **linear subspace** of $\mathbb{P}^n(\Bbbk)$ of dimension $\dim_{\Bbbk} W - 1$. Any two linear subspaces of the same dimension are projectively equivalent. Given a subset $\emptyset \neq X \subset \mathbb{P}^n(\Bbbk)$, there is a smallest linear subspace of $\mathbb{P}^n(\Bbbk)$ containing X. This subspace is called the **span** of X. A **line** in $\mathbb{P}^n(\Bbbk)$ is a linear subspace of dimension 1. A **plane** in $\mathbb{P}^n(\Bbbk)$ is a linear subspace of dimension 2. A **hyperplane** in $\mathbb{P}^n(\Bbbk)$ is a linear subspace of dimension $n-1$. □

Exercise 5.1.8. Let $p_0, \ldots, p_n, p_{n+1} \in \mathbb{P}^n(\Bbbk)$ be a collection of $n+2$ points such that no subset of $n+1$ points is contained in a hyperplane. Show that there is a unique change of coordinates T of $\mathbb{P}^n(\Bbbk)$ such that

$$T(p_0) = [1 : 0 : \cdots : 0], \ldots, T(p_n) = [0 : \cdots : 0 : 1],$$
$$\text{and } T(p_{n+1}) = [1 : \cdots : 1].$$

The points $[1 : 0 : \cdots : 0], \ldots, [0 : \cdots : 0 : 1]$ are known as the **coordinate points** of $\mathbb{P}^n(\Bbbk)$, and $[1 : \cdots : 1]$ is the **scaling point**. □

Just as in our provisional definition of the real projective plane, we can write $\mathbb{P}^n(\Bbbk)$ as the union of $\mathbb{A}^n(\Bbbk)$ and a **hyperplane at infinity**:

$$\mathbb{P}^n(\Bbbk) = U_0 \cup H_0 \cong \mathbb{A}^n(\Bbbk) \cup \mathbb{P}^{n-1}(\Bbbk),$$

where

$$U_0 := \mathrm{D}(x_0) = \{[a_0 : \cdots : a_n] \in \mathbb{P}^n(\Bbbk) \mid a_0 \neq 0\},$$

and H_0 is the complement $H_0 = \mathbb{P}^n(\Bbbk) \setminus U_0 = \mathrm{V}(x_0)$. We identify H_0 with $\mathbb{P}^{n-1}(\Bbbk)$ by disregarding the first coordinate, and U_0 with $\mathbb{A}^n(\Bbbk)$ via

$$\varphi_0 : U_0 \to \mathbb{A}^n(\Bbbk),\ [a_0 : \cdots : a_n] = [1 : \tfrac{a_1}{a_0} : \ldots, \cdots : \tfrac{a_n}{a_0}]$$
$$\mapsto (\tfrac{a_1}{a_0}, \ldots, \ldots, \tfrac{a_n}{a_0}).$$

This map is bijective, with inverse

$$\mathbb{A}^n(\Bbbk) \to U_0,\ (b_1, \ldots, b_n) \mapsto [1 : b_1 : \cdots : b_n].$$

Given a point $p = [a_0 : \cdots : a_n] \in U_0$, the ratios a_i/a_0 are sometimes called the **affine coordinates** for p in U_0.

Example 5.1.9. In the special case of $\mathbb{P}^1(\mathbb{R})$, the map φ_0 sends a point $p = [a_0 : a_1] \in U_0$ to the slope a_1/a_0 of the line in $\mathbb{A}^2(\mathbb{R})$ corresponding to p.

The point [0:1] is the single point at infinity. It corresponds to the x_1-axis which is vertical and has, thus, slope ∞. □

The proof of our next proposition exhibits the geometric meaning of dehomogenization and homogenization.

Proposition 5.1.10. *The map $\varphi_0 : U_0 \to \mathbb{A}^n(\Bbbk)$ is a homeomorphism with regard to the respective Zariski topologies.*

Proof. Let $A \subset \mathbb{P}^n(\Bbbk)$ be a projective algebraic set. Then $A = \mathrm{V}(T)$ for some subset of homogeneous polynomials $T \subset \Bbbk[x_0, \ldots, x_n]$. Let $T_a \subset \Bbbk[x_1, \ldots, x_n]$ be obtained from T by dehomogenizing each element of T with respect to x_0. Then it is immediate from the definitions that $\varphi_0(A \cap U_0)$ is the algebraic set $\mathrm{V}_a(T_a) \subset \mathbb{A}^n(\Bbbk)$, where $\mathbf{V_a}$ indicates that we look at the **affine vanishing locus**. Since the closed subsets of U_0 arise as intersections of type $A \cap U_0$, the map φ_0 is closed.

Conversely, let $A \subset \mathbb{A}^n(\Bbbk)$ be an affine algebraic set. Then $A = \mathrm{V}_a(T_a)$ for some subset of polynomials $T_a \subset \Bbbk[x_1, \ldots, x_n]$, and it is easy to check that $\varphi_0^{-1}(A)$ is the closed subset $\mathrm{V}(T_a^h) \cap U_0$ of U_0, where $T_a^h \subset \Bbbk[x_0, \ldots, x_n]$ is obtained from T_a by homogenizing each element of T_a with respect to x_0. Hence, the inverse map φ_0^{-1} is also closed. We conclude that φ_0 is a homeomorphism. □

Given an algebraic subset A of $\mathbb{P}^n(\Bbbk)$, we will identify $A \cap U_0$ with the algebraic set $\varphi_0(A \cap U_0) \subset \mathbb{A}^n(\Bbbk)$. Conversely, we will identify an algebraic subset A of $\mathbb{A}^n(\Bbbk)$ with $\varphi_0^{-1}(A) \subset \mathbb{P}^n(\Bbbk)$. Hence, the following definition makes sense:

Definition 5.1.11. If $A \subset \mathbb{A}^n(\Bbbk) \cong U_0$ is an algebraic subset, its Zariski closure $\overline{A}$ in $\mathbb{P}^n(\Bbbk)$ is said to be the **projective closure** of A. □

Remark 5.1.12. In Section 6.2, considering the homogenization of ideals, we will show how to compute the projective closure. In the special case of a hypersurface, if $f \in \Bbbk[x_1, \ldots, x_n]$ is any nonconstant polynomial, and f^h is its homogenization with respect to x_0, the argument will show that

$$\overline{\mathrm{V}_a(f)} = \mathrm{V}(f^h) \subset \mathbb{P}^n(\Bbbk).$$

□

In accordance with our provisional definition of $\mathbb{P}^2(\mathbb{R})$, we have:

Example 5.1.13. In $\mathbb{P}^2(\Bbbk)$, the projective closure of a line in $\mathbb{A}^2(\Bbbk) \cong \mathrm{D}(x_0)$ with equation $x_2 = mx_1 + b$ is defined by the equation $x_2 = mx_1 + bx_0$. It intersects the line $\mathrm{V}(x_0)$ at infinity in the point $[0 : 1 : m]$. A line with equation $x_1 = c$ is completed by adding the point $[0 : 1 : 0]$. □

In the discussion above, there is nothing special with x_0: For $0 \leq i \leq n$, we define U_i, H_i and φ_i by using x_i instead of x_0. Then the U_i, which are known as the **(affine) coordinate charts** of $\mathbb{P}^n(\Bbbk)$, cover $\mathbb{P}^n(\Bbbk)$:

$$\mathbb{P}^n(\Bbbk) = \bigcup_{i=0}^{n} U_i.$$

Hence, $\mathbb{P}^n(\Bbbk)$ looks locally like $\mathbb{A}^n(\Bbbk)$, and we may study a projective algebraic set $A \subset \mathbb{P}^n(\Bbbk)$ by examining the different intersections $A \cap U_i$.

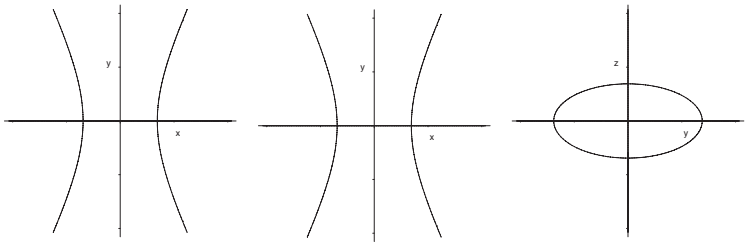
Example 5.1.14. Let $\Bbbk = \mathbb{R}$.

1. The projective closure C of the affine conic

   $$\mathrm{V}(x^2 - 1/4y^2 - 1) \subset \mathbb{A}^2(\mathbb{R}) \cong \mathrm{D}(z)$$

   is defined by the quadratic form $x^2 - 1/4y^2 - z^2 = 0$. We show C in all three coordinate charts:

   $z = 1$ $\qquad$ $y = 1$ $\qquad$ $x = 1$

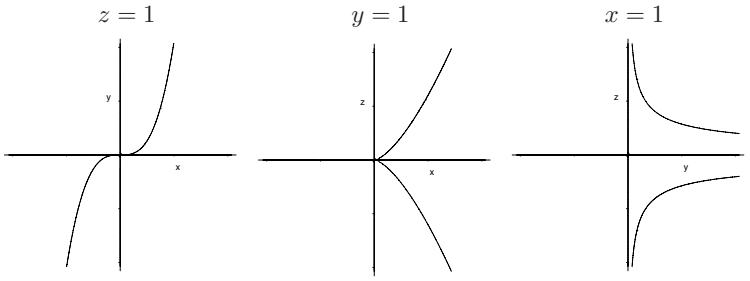
   

   $x^2 - 1/4y^2 = 1$ $\qquad$ $x^2 - z^2 = 1/4$ $\qquad$ $1/4y^2 + z^2 = 1$

2. Similarly, starting from the affine curve

   $$\mathrm{V}(y - x^3) \subset \mathbb{A}^2(\mathbb{R}) \cong \mathrm{D}(z),$$

   we get the pictures below:



□

Exercise 5.1.15. Draw the curve $\mathrm{V}(zy^2 - x^2z + x^3) \subset \mathbb{P}^2(\mathbb{R})$ in all three coordinate charts. For each chart, determine the points of the curve which lie on the line at infinity. Similarly for the curves in the previous example. □

Exercise 5.1.16. A **conic** in $\mathbb{P}^2(\Bbbk)$ is defined by a nonzero quadratic form.

1. Show: A conic in $\mathbb{P}^2(\mathbb{R})$ is projectively equivalent to one of the following:

a)	$\mathrm{V}(x^2 + y^2 - z^2)$	(nondegenerate conic)
b)	$\mathrm{V}(x^2 + y^2 + z^2)$	(empty set)
c)	$\mathrm{V}(x^2 - y^2)$	(pair of lines)
d)	$\mathrm{V}(x^2 + y^2)$	(single point)
e)	$\mathrm{V}(x^2)$	("double" line).

2. Similarly, show that there are three classes of conics in $\mathbb{P}^2(\mathbb{C})$:

a)	$\mathrm{V}(x^2 + y^2 + z^2)$	(nondegenerate conic)
b)	$\mathrm{V}(x^2 + y^2)$	(pair of lines)
c)	$\mathrm{V}(x^2)$	("double" line).

3. More generally, show that quadric hypersurfaces in $\mathbb{P}^n(\mathbb{C})$ are classified by their rank. For this, recall that every quadratic form $f \in \mathbb{C}[x_0, \ldots, x_n]$ may be written as
$$f(\boldsymbol{x}) = \boldsymbol{x}^t \cdot A \cdot \boldsymbol{x},$$
where $\boldsymbol{x}$ is the column vector with entries $x_0, \ldots, x_n$, and where $A = (a_{ij})$ is a symmetric $(n+1) \times (n+1)$ matrix of scalars $a_{ij} \in \mathbb{C}$. The **rank** of the corresponding quadric $Q = \mathrm{V}(f) \subset \mathbb{P}^2(\mathbb{C})$ is defined to be the rank of A. Now show that Q has rank r iff it is projectively equivalent to a quadric with defining equation
$$\sum_{i=0}^{r} x_i^2 = 0.$$
If $r = n + 1$, then Q is **nondegenerate**.

4. Exactly, what invariants classify quadratic forms over $\mathbb{R}$?

By comparing the projective classification of conics with the classification of conics in the respective affine planes (work this out), you will find another example of how geometric statements become simpler if we pass from affine to projective geometry. In particular, as should be already clear from Example 5.1.14 and Figure 5.5, the difference between ellipses, parabolas, and hyperbolas disappears in the projective setting. □

Remark 5.1.17. In parts 2 and 3 of Exercise 5.1.16, we may replace $\mathbb{C}$ by any algebraically closed field of characteristic $\neq 2$. □

Before we go further, we adopt a convention which extends Convention 2.7.2:

Convention 5.1.18. *From now on, $\mathbb{K}$ will be an algebraically closed extension field of $\Bbbk$. We will write $\mathbb{P}^n := \mathbb{P}^n(\mathbb{K})$. If $T \subset \Bbbk[x_0, \ldots, x_n]$ is a set of homogeneous polynomials, then $A = \mathrm{V}(T)$ will be its vanishing locus in $\mathbb{P}^n$. We will, then, say that $\Bbbk$ is a **field of definition** of A, or that A is* **defined over** *$\Bbbk$. A **$\Bbbk$-rational point** of A is a point of the intersection*

$$A(\Bbbk) := A \cap \mathbb{P}^n(\Bbbk).$$

*Furthermore, an element of $\mathrm{PGL}(n+1, \Bbbk) \subset \mathrm{PGL}(n+1, \mathbb{K})$ will be called an **automorphism** of $\mathbb{P}^n$ **defined over** $\Bbbk$.* □

Remark 5.1.19. Convention 5.2.1 is justified by the projective Nullstellensatz which will be proved in the next chapter. The Nullstellensatz says, in particular, that hypersurfaces in $\mathbb{P}^n$ correspond to nonconstant square-free forms in $\mathbb{K}[x_0, \ldots, x_n]$, where the form f is uniquely determined by the hypersurface H up to multiplication by a nonzero scalar. Then H is irreducible iff f is irreducible, and the degree of f is also called the **degree** of H. A hypersurface is a **quadric**, **cubic**, **quartic**, **quintic** if its degree is 2,3,4,5, respectively. □

As for the elements of the polynomial ring $\mathbb{K}[x_0, \ldots, x_n]$, most elements of the rational function field $\mathbb{K}(x_0, \ldots, x_n)$ cannot be regarded as functions in the projective context. However, if $g, h \in \mathbb{K}[x_0, \ldots, x_n]$ are *forms* of the *same degree* d, then $f = g/h$ defines a function on $\mathrm{D}(h) \subset \mathbb{P}^n$. Indeed, in this case, substituting the homogeneous coordinates of a point $p \in \mathrm{D}(h)$ for the x_i in g and h gives a well-defined value $f(p)$:

$$\frac{g(\lambda x_0, \ldots, \lambda x_n)}{h(\lambda x_0, \ldots, \lambda x_n)} = \frac{\lambda^d g(x_0, \ldots, x_n)}{\lambda^d h(x_0, \ldots, x_n)} = \frac{g(x_0, \ldots, x_n)}{h(x_0, \ldots, x_n)}.$$

Specific examples are the affine coordinate functions x_j/x_i on $U_i = \mathrm{D}(x_i)$. The **rational function field** of $\mathbb{P}^n$ is the subfield

$$\mathbb{K}(\mathbb{P}^n) = \{g/h \in \mathbb{K}(x_0, \ldots, x_n) \mid g, h \text{ forms of the same degree}\}$$

of $\mathbb{K}(x_0, \ldots, x_n)$. Equivalently, $\mathbb{K}(\mathbb{P}^n)$ is the rational function field of any coordinate chart $U_i \cong \mathbb{A}^n$ (dehomogenize respectively homogenize to show that the two definitions give isomorphic fields). Similarly, we may define the **local ring of $\mathbb{P}^n$ at a point** $p \in \mathbb{P}^n$ either as the subring

$$\mathcal{O}_{\mathbb{P}^n,p} = \{g/h \in \mathbb{K}(\mathbb{P}^n) \mid \mathrm{D}(h) \ni p\} \subset \mathbb{K}(\mathbb{P}^n),$$

or as the local ring at p of any coordinate chart containing p. Concepts formulated in terms of the local ring can, then, be directly extended from the affine to the projective case. For instance, if $f \in \Bbbk[x_0, \ldots, x_n]$ is a nonconstant form, and $p \in \mathbb{P}^n$ is a point, the **multiplicity of f at p**, written $\mathrm{mult}(f, p)$, is well-defined as the multiplicity at p of the dehomogenization of f in any chart U_i containing p. Similarly for the **intersection multiplicity** $i(f, g; p)$ of two nonconstant forms $f, g \in \Bbbk[x, y, z]$.

More generally, the local ring $\mathcal{O}_{A,p}$ of any projective algebraic set $A \subset \mathbb{P}^n$ at a point $p \in A$ can be defined in an analogous way, and in accordance with what is happening in the affine charts (we will treat this more systematically in Chapter 6). It makes, then, sense to say that p is a **smooth point** of A if $\mathcal{O}_{A,p}$ is a regular local ring. Equivalently, if U_i is any coordinate chart containing p, the affine algebraic set $A \cap U_i$ is smooth at p. The notions **singular point** and A_{sing} are as before.

Recall that $A \cap U_i$ is singular at p if the dimension of the tangent space to $A \cap U_i$ at p is strictly larger than the local dimension of $A \cap U_i$ at p. Though this can be checked in the chart U_i, it is occassionally useful to have a projective version of the tangent space:

Definition 5.1.20. Let $A \subset \mathbb{P}^n$ be a projective algebraic set, and let $p = [a_0 : \cdots : a_n] \in A$ be a point. The **projective tangent space to A at p** is the linear subspace $T_pA \subset \mathbb{P}^n$ defined as follows: If A is a hypersurface, and $f \in \mathbb{K}[x_0, \ldots, x_n]$ is a square-free form such that $A = \mathrm{V}(f)$, set

$$T_pA = \mathrm{V}\left(\sum_{i=0}^{n} \frac{\partial f}{\partial x_i}(a_0, \ldots, a_n) \cdot x_i\right) \subset \mathbb{P}^n.$$

In the general case, let T_pA be the intersection of all projective tangent spaces at p to hypersurfaces containing A. □

Exercise* 5.1.21. If $f \in \mathbb{K}[x_0, \ldots, x_n]$ is a square-free form, and $A = \mathrm{V}(f) \subset \mathbb{P}^n$, use Euler's rule to show:

1. If U_i is any coordinte chart containing p, then T_pA is the projective closure of the tangent space to the affine algebraic set $A \cap U_i$ at p.
2. If $C(A) \subset \mathbb{A}^{n+1}$ is the affine cone over A, and $q \in C(A)$ is any point representing p, the tangent space to $C(A)$ at q passes through the origin. It is, thus, a linear subspace W of $\mathbb{K}^{n+1}$. Furthermore, W is independent of the choice of q, and $T_pA = \mathbb{P}(W)$. □

For a hypersurface $A = \mathrm{V}(f)$ as in the exercise, p is a smooth point of A iff T_pA is a hyperplane. That is,

$$A_{\mathrm{sing}} = \mathrm{V}\left(f, \frac{\partial f}{\partial x_0}, \ldots, \frac{\partial f}{\partial x_n}\right).$$

If $\mathrm{char}\,\Bbbk$ does not divide $\deg f$, it is clear from Euler's rule that only the partial derivatives need to be considered.

Exercise 5.1.22. Determine the singular points of the curves in Example 5.1.14 and Exercise 5.1.15. □

In the discussion above, there is no need to restrict ourselves to coordinate charts: We may take any hyperplane H to be the hyperplane at infinity, regarding its complement U as affine n-space, and calling U an **affine chart**. Explicitly, if $H = \mathrm{V}(\sum \lambda_i x_i)$, where at least one λ_j is nonzero, identify

$$U \cong \mathbb{A}^n(\Bbbk)$$

via

$$[a_0 : \cdots : a_n] \mapsto \left(\frac{a_0}{\sum \lambda_i a_i}, \ldots, \widehat{\frac{a_j}{\sum \lambda_i a_i}}, \ldots, \frac{a_n}{\sum \lambda_i a_i}\right).$$

This is useful since a convenient choice of chart may ease explicit computations. Given any collection $y_0, \ldots, y_n$ of linearly independent linear forms, the $\mathrm{D}(y_i)$ form a covering of $\mathbb{P}^n(\Bbbk)$ which is obtained from the one given by the $\mathrm{D}(x_i)$ by a projective change of coordinates.

In Renaissance texts on perspective, the idea of considering different affine charts is a central theme. We illustrate this in Figure 5.5, where the reader may think of one chart as the floor in a medieval palace, of the other chart as the canvas of a painter, and of the origin $o \in \mathbb{A}^3(\mathbb{R})$ as the artist's eye.

In case $\Bbbk = \mathbb{R}$ respectively $\Bbbk = \mathbb{C}$, the projective space $\mathbb{P}^n(\Bbbk)$ also carries an Euclidean topology, namely the quotient topology induced from the Euclidean topology on $\Bbbk^{n+1} \setminus \{0\}$ via the canonical projection $\Bbbk^{n+1} \setminus \{0\} \to \mathbb{P}^n(\Bbbk)$.

Remark 5.1.23. 1. Let $\Bbbk = \mathbb{R}$ respectively $\Bbbk = \mathbb{C}$. Then $\mathbb{P}^n(\Bbbk)$ carries an Euclidean topology, namely the quotient topology induced by the canonical projection $\Bbbk^{n+1} \setminus \{0\} \to \mathbb{P}^n(\Bbbk)$. With respect to this topology, the coordinate charts exhibit $\mathbb{P}^n(\Bbbk)$ as a real respectively complex manifold, which is, in fact, compact. Indeed, we may regard $\mathbb{P}^n(\Bbbk)$ as the quotient

$$\mathbb{P}^n(\Bbbk) \cong S^n / \sim,$$

where

$$S = \{x \in \Bbbk^{n+1} \mid ||x|| = 1\}$$

is the (compact) unit sphere, and where $\sim$ refers to identifying antipodal points.

Compactness follows since $\mathbb{P}^n(\mathbb{R})$ is the image of the compact unit sphere

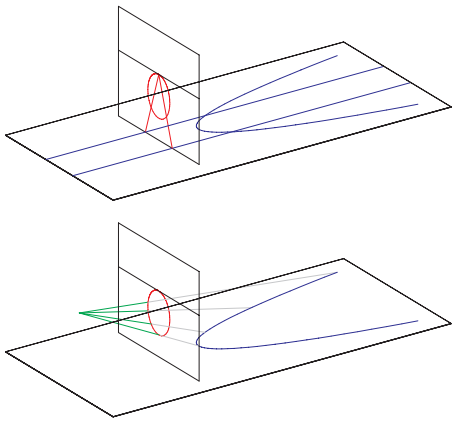


Fig. 5.4. *Different charts in perspective drawing.*

$$S = \{x \in \Bbbk^{n+1} \mid ||x|| = 1\} \subset \mathbb{R}^{n+1}.$$

In case $\Bbbk = \mathbb{C}$, $\mathbb{P}^n(\mathbb{C})$ is the image of the $2n+1$-dimensional unit sphere in $\mathbb{C}^{n+1}$.

2. Let $\Bbbk = \mathbb{C}$. If $f \in \mathbb{C}[x_1, \ldots, x_n\}$ ia a polynomial, then $\mathrm{V}(f^h)$ is not only the Zariski closure of $\mathrm{V}(f) \subset U_0 \subset \mathbb{P}^n(\mathbb{C})$, but also the closure of $\mathrm{V}(f)$ with respect to the Euclidian topology. To see this we may assume that f is irreducible. Then all affine hypersurface $\mathrm{V}(f^h) \cap U_i$ are irreducible hence path connected by Theorem 6.7.13 in Chapter
. The claim follows since the $\bigcup_i U_i$ covers $\mathbb{P}^n$. In particular we see that a projective hypersurface equipped with the Euclidean topology is compact as a closed subset of the compact manifold $\mathbb{P}^n(\mathbb{C})$. □

We will discuss the structure of the differentiable maps $S^n \to \mathbb{P}^n(\mathbb{R})$ and $S^{2n+1} \to \mathbb{P}^n(\mathbb{C})$ for small $n = 2$ respectively $n = 1$.

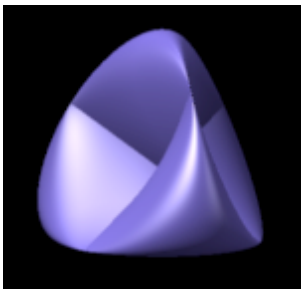
In the last two remarks of this section, we discuss the construction of $\mathbb{P}^2(\mathbb{R})$ and $\mathbb{P}^1(\mathbb{C})$ by focusing on their Euclidean topology. These considerations will not play a role in subsequent parts of the book.

Remark 5.1.24. The real projective plane $\mathbb{P}^2(\mathbb{R})$ has an interesting structure as a 2-dimensional real manifold. Every line through the origin in $\mathbb{R}^3$ intersects the unit sphere $S^2 = \{(x_0, x_1, x_2 \in \mathbb{R}^3 \mid x_0^2 + x_1^2 + x_2^2 = 1\}$ in two points. Thus

$$\mathbb{P}^2(\mathbb{R}) = S^2/\sim,$$

where the equivalence relation $\sim$ identifies antipodal points. Thus as real manifold we obtain $\mathbb{P}^2(\mathbb{R})$ by gluing the Moebius strip, which is the image of

a belt around the equator in S^2, with a disc, which is the image of the cap around the north (or south) pole. Hence, the manifold $\mathbb{P}^2(\mathbb{R})$ is not orientable. In particular, we cannot embed $\mathbb{P}^2(\mathbb{R})$ into $\mathbb{R}^3$. There are however models of $\mathbb{P}^2(\mathbb{R})$ in $\mathbb{R}^3$, if we allow self-intersections. The Steiner roman surface discussed in Example 2.6.6 ,

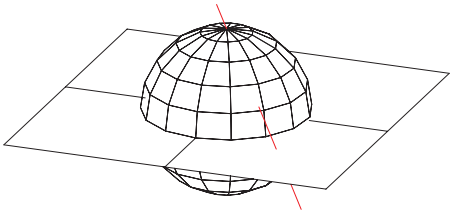


is such an example, because

$$S^2 \to \mathbb{R}^3,\ (x_0, x_1, x_2) \mapsto (x_1x_2, x_0x_2, x_0x_1)$$

factors over $\mathbb{P}^2(\mathbb{R})$. The map $\varphi : \mathbb{P}^2(\mathbb{R}) \to \mathbb{R}^3$ is an **immersion** at all points $p \in \mathbb{P}^2(\mathbb{R})$ except at the 6 pinch points on the coordinate axes. (A map between $\varphi : M \to N$ differential manifolds is a immersion at $p \in M$, if the induced map on the tangent spaces $d_p\varphi : T_pM \to T_pN$ is an inclusion. An immersion is a map which is an immersion everywhere). An immersion of $\mathbb{P}^2(\mathbb{R}) \to \mathbb{R}^3$ is given by the Boy surface.

Remark 5.1.25. For the complex projective line we have established two points of view. We can regard $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \infty \cong S^2$ via the projection from the north pole onto the Gaussian number plane.

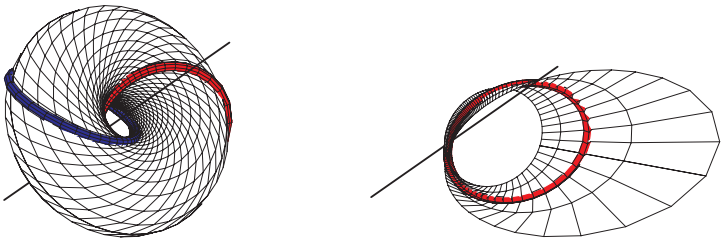


The other description realizes $\mathbb{P}^1(\mathbb{C})$ as the complex lines in $\mathbb{C}^2$. On the unit sphere $S^3 \subset \mathbb{C}^2$ every point in $\mathbb{P}^1$ has an $S^1 \cong \{z \in \mathbb{C} \mid |z| = 1\}$ of representatives. Combining both descriptions, we find a map

$$h : S^3 \to S^2,$$

whose fibers are S^1's, the **Hopf fibration**.

Identifying $S^3 = \mathbb{R}^3 \cup \{(1 + i0, 0 + i0)\}$ via stereographic projection, we find that $\mathbb{R}^3$ is fibered into an $\mathbb{R}^2$ of circles and a line.



Exercise 5.1.26. Prove that there is no continues section $\sigma\colon S^2 \to S^3$ of h, but that there exists a continues section of $h\colon S^3 \setminus h^{-1}(\infty) \to \mathbb{C}$. What is the closure of the graph in your example? □

5.2 The Extension of Basic Concepts

Coordinate charts allow us to extend concepts such as function fields, local rings, smoothness, tangent spaces, and dimension with almost no extra effort to the projective case. In this section, we will give some examples of how this works. First of all, we adopt a convention which adds to Convention 2.7.2:

Convention 5.2.1. *From now on, $\mathbb{K}$ will be an algebraically closed extension field of $\Bbbk$. We will write $\mathbb{P}^n := \mathbb{P}^n(\mathbb{K})$. If $T \subset \Bbbk[x_0, \ldots, x_n]$ is a set of homogeneous polynomials, then $A = \mathrm{V}(T)$ will be its vanishing locus in $\mathbb{P}^n$. We will, then, say that $\Bbbk$ is a **field of definition** of A, or that A is* **defined over** *$\Bbbk$. A **$\Bbbk$-rational point** of A is a point of the intersection*

$$A(\Bbbk) := A \cap \mathbb{P}^n(\Bbbk).$$

*Furthermore, an element of $\mathrm{PGL}(n+1, \Bbbk) \subset \mathrm{PGL}(n+1, \mathbb{K})$ will be called an **automorphism** of $\mathbb{P}^n$ **defined over** $\Bbbk$.* □

Remark 5.2.2. Convention 5.2.1 is justified by the projective Nullstellensatz which will be proved in the next chapter. The Nullstellensatz says, in particular, that hypersurfaces in $\mathbb{P}^n$ correspond to nonconstant square-free forms in $\mathbb{K}[x_0, \ldots, x_n]$, where the form f is uniquely determined by the hypersurface H up to multiplication by a nonzero scalar. Then H is irreducible iff f is irreducible, and the degree of f is also called the **degree** of H. A hypersurface is a **quadric**, **cubic**, **quartic**, **quintic** if its degree is 2,3,4,5, respectively. □

As for the elements of the polynomial ring $\mathbb{K}[x_0, \ldots, x_n]$, most elements of the rational function field $\mathbb{K}(x_0, \ldots, x_n)$ cannot be regarded as functions in the projective context. However, if $g, h \in \mathbb{K}[x_0, \ldots, x_n]$ are *forms* of the *same degree* d, then $f = g/h$ defines a function on $\mathrm{D}(h) \subset \mathbb{P}^n$. Indeed, in this case,

substituting the homogeneous coordinates of a point $p \in \mathrm{D}(h)$ for the x_i in g and h gives a well-defined value $f(p)$:

$$\frac{g(\lambda x_0, \ldots, \lambda x_n)}{h(\lambda x_0, \ldots, \lambda x_n)} = \frac{\lambda^d g(x_0, \ldots, x_n)}{\lambda^d h(x_0, \ldots, x_n)} = \frac{g(x_0, \ldots, x_n)}{h(x_0, \ldots, x_n)}.$$

Specific examples are the affine coordinate functions x_j/x_i on $U_i = \mathrm{D}(x_i)$.

Definition 5.2.3. The **rational function field** of $\mathbb{P}^n$ is the subfield

$$\begin{aligned}\mathbb{K}(\mathbb{P}^n) &= \{g/h \in \mathbb{K}(x_0, \ldots, x_n) \mid g, h \text{ forms of the same degree}\} \\ &\subset \mathbb{K}(x_0, \ldots, x_n).\end{aligned}$$

The **local ring of $\mathbb{P}^n$ at a point** $p \in \mathbb{P}^n$ is the subring

$$\mathcal{O}_{\mathbb{P}^n,p} = \{g/h \in \mathbb{K}(\mathbb{P}^n) \mid \mathrm{D}(h) \ni p\} \subset \mathbb{K}(\mathbb{P}^n). \qquad \square$$

Note that $\mathcal{O}_{\mathbb{P}^n,p}$ is indeed a local ring. Note also that the definition of $\mathcal{O}_{\mathbb{P}^n,p}$ is consistent with our definition in the affine case: If U_i is a coordinate chart containing p, then $\mathcal{O}_{\mathbb{P}^n,p}$ is isomorphic to the local ring of $\mathbb{A}^n \cong U_i$ at p (dehomogenize; for the inverse map, homogenize).

Concepts formulated in terms of the local ring can, thus, be directly extended from the affine to the projective case. For instance, if $f \in \Bbbk[x_0, \ldots, x_n]$ is a nonconstant form, and $p \in \mathbb{P}^n$ is a point, the **multiplicity of f at p**, written $\mathrm{mult}(f, p)$, is well-defined as the multiplicity at p of the dehomogenization of f in any chart U_i containing p. In the same way, given two nonconstant forms $f, g \in \Bbbk[x, y, z]$ and a point $p \in \mathbb{P}^2$, we define the **intersection multiplicity of f and g at p**, written $i(f, g; p)$. As in Chapter 4, these notions carry over to hypersurfaces (plane curves) by considering square-free forms defining the hypersurfaces (plane curves).

More generally, the local ring $\mathcal{O}_{A,p}$ of any projective algebraic set $A \subset \mathbb{P}^n$ at a point $p \in A$ can be defined in an analogous way, and such that the definition is consistent with that in the affine case (we will treat this more systematically in Chapter 6). It makes, then, sense to say that p is a **smooth point** of A if $\mathcal{O}_{A,p}$ is a regular local ring. Equivalently, if U_i ia any coordinate chart containing p, the affine algebraic set $A \cap U_i$ is smooth at p. Otherwise, p is a **singular point** of A. As before, we write A_{sing} for the set of these points.

Recall that $A \cap U_i$ is singular at p if the dimension of the tangent space to $A \cap U_i$ at p is strictly larger than the local dimension of $A \cap U_i$ at p. Though this can be checked in the chart U_i, it is occassionally useful to have a projective version of the tangent space. Here is the definition in the hypersurface case (see Chapter 6 for the general case):

Definition 5.2.4. Let $A \subset \mathbb{P}^n$ be a hypersurface, let $p = [a_0 : \cdots : a_n] \in A$ be a point, and let $f \in \mathbb{K}[x_0, \ldots, x_n]$ be a square-free form such that $A = \mathrm{V}(f)$. The **projective tangent space T_pA to A at p** is the linear subspace

$$T_pA = \mathrm{V}\left(\sum_{i=0}^{n} \frac{\partial f}{\partial x_i}(a_0, \ldots, a_n) \cdot x_i\right) \subset \mathbb{P}^n. \qquad \square$$

Exercise* **5.2.5.** In the situation of the definition, use Euler's rule to show:

1. If U_i is any coordinte chart containing p, then T_pA is the projective closure of the tangent space to the affine algebraic set $A \cap U_i$ at p.
2. If $C(A) \subset \mathbb{A}^{n+1}$ is the affine cone over A, and $q \in C(A)$ is any point representing p, the tangent space to $C(A)$ at q passes through the origin. It is, thus, a linear subspace W of $\mathbb{K}^{n+1}$. Furthermore, W is independent of the choice of q, and $T_pA = \mathbb{P}(W)$. □

With notation as in the definition, p is a smooth point of A iff T_pA is a hyperplane. That is,

$$A_{\text{sing}} = \mathrm{V}\left(f, \frac{\partial f}{\partial x_0}, \ldots, \frac{\partial f}{\partial x_n}\right).$$

If $\operatorname{char}\Bbbk$ does not divide $\deg f$, it is clear from Euler's rule that only the partial derivatives need to be considered.

Exercise 5.2.6. Determine the singular points of the curves in Example 5.1.14 and Exercise 5.1.15. □

With regard to local studies, there is no need to restrict ourselves to coordinate charts: We may take any hyperplane H to be the hyperplane at infinity, regarding its complement U as affine n-space, and calling U an **affine chart**. Explicitly, if $H = \mathrm{V}(\sum \lambda_i x_i)$, where at least one λ_j is nonzero, identify

$$U \cong \mathbb{A}^n(\Bbbk)$$

via

$$[a_0 : \cdots : a_n] \mapsto \left(\frac{a_0}{\sum \lambda_i a_i}, \ldots, \widehat{\frac{a_j}{\sum \lambda_i a_i}}, \ldots, \frac{a_n}{\sum \lambda_i a_i}\right).$$

This is useful since a convenient choice of chart may ease explicit computations. Given any collection $y_0, \ldots, y_n$ of linearly independent linear forms, the $\mathrm{D}(y_i)$ form a covering of $\mathbb{P}^n(\Bbbk)$ which is obtained from the one given by the $\mathrm{D}(x_i)$ by a projective change of coordinates.

In Renaissance texts on perspective, the idea of considering different affine charts is a central theme. We illustrate this in Figure 5.5, where the reader may think of one chart as the floor in a medieval palace, of the other chart as the canvas of a painter, and of the origin $o \in \mathbb{A}^3(\mathbb{R})$ as the artist's eye.

5.3 Linear Systems of Plane Curves

The concept of linear systems is a classical concept of algebraic geometry. In this section, we study the special case of linear systems of plane curves. As motivation for this, we consider the following question:

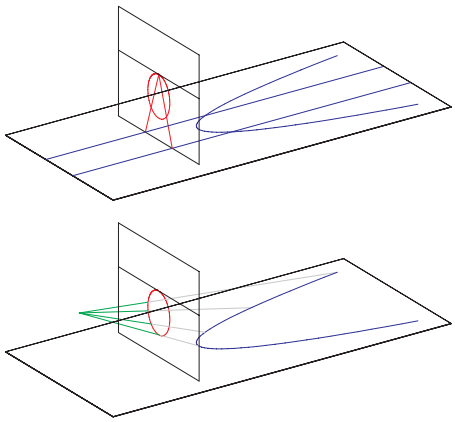


Fig. 5.5. *Different charts in perspective drawing.*

Given $d \geq 1$ and finitely many points in the projective plane, how many curves of degree d pass through these points? (5.1)

To give the question a precise meaning, we describe the curves with the help of equations. We denote the coordinates by x, y, z. Recall from Remark 5.2.2 that each curve $C \subset \mathbb{P}^2$ of degree d is defined by a square-free form $f \in \mathbb{K}[x, y, z]$ of degree d, where f is determined up to multiplication by a nonzero scalar. In other words, C defines a point in the projective space $\mathbb{P}(L(d))$, where

$$L(d) = \mathbb{K}[x, y, z]_d = \{f \in \mathbb{K}[x, y, z] \mid f \text{ is homogenous of degree } d\}.$$

In $\mathbb{P}(L(d))$, there are also points corrsponding to polynomials with multiple factors. Nevertheless, we prefer to work with this space since the subset defined by the square-free polynomials is difficult to handle. By abuse of notation, we refer to every point of $\mathbb{P}(L(d))$ as a **projective plane curve of degree d**, and to $\mathbb{P}(L(d))$ itself as a **parameter space for the plane curves of degree d**. In speaking of components, of curves passing through a point, and of curves intersecting at a point, we extend the terminology introduced in Section 4.3 from the affine to the projective case.

Note that $\mathbb{P}(L(d))$ is a projective space of dimension

$$\binom{d+2}{2} - 1 = \frac{d(d+3)}{2}.$$

In fact, since the monomials of degree d form a $\mathbb{K}$-basis for $L(d)$, we may regard the coefficients of the polynomials in $L(d)$ as homogeneous coordinates on $\mathbb{P}(L(d))$ (listed in some order). Note that every change of coordinates of $\mathbb{P}^2$ induces a change of coordinates of $\mathbb{P}(L(d))$ (in the obvious way).

We can, now, illustrate question (5.1) by an example:

Example 5.3.1. Consider the four points

$$p_1 = [0:0:1],\ p_2 = [1:0:1],\ p_3 = [0:1:1],\ p_4 = [1:1:1] \in \mathbb{P}^2.$$

To describe the conics passing through these points, note that a quadratic polynomial

$$f = f_{20}x^2 + f_{11}xy + f_{10}xz + f_{02}y^2 + f_{01}yz + f_{00}z^2$$

vanishes at p_1, p_2, p_3, p_4 iff

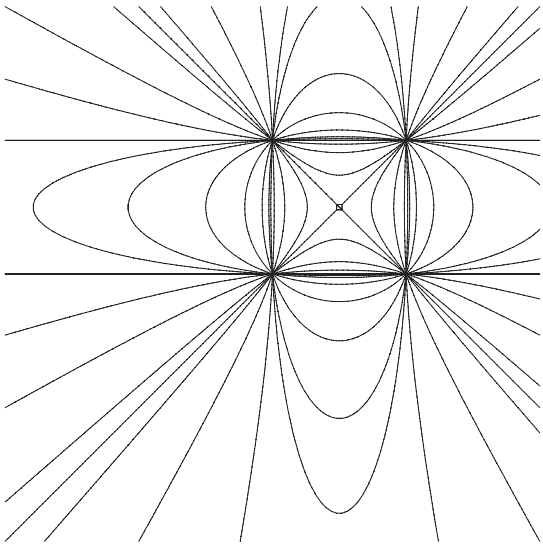
$$f_{00} = 0,\ f_{20} + f_{10} = 0,\ f_{02} + f_{01} = 0,\ f_{20} + f_{11} + f_{10} + f_{02} + f_{01} = 0.$$

This gives four linear conditions on the coefficients of f which are, in fact, independent – the conditions determine the two-dimensional linear subspace

$$L = \{\lambda x(x-z) + \mu y(y-z) \mid \lambda, \mu \in \mathbb{K}\} \subset \mathbb{K}[x,y,z]_2.$$

Geometrically, the generators $x(x-z)$ and $y(y-z)$ of L define two pairs of lines in $\mathbb{P}^2$ which, considered as points of $L(2)$, span the line $\mathbb{P}(L) \subset L(2)$. This line parametrizes the conics passing through p_1, p_2, p_3, p_4 – there is a $\mathbb{P}^1$ of such conics.

The following real picture shows the conics in the affine chart $\mathrm{D}(z)$:



□

It is clear from the example that "passing through a point $p \in \mathbb{P}^2$" imposes one linear condition on the curves of degree d – the curves passing through p form a hyperplane in $\mathbb{P}(L(d))$. More generally, as we will see in Proposition 5.3.3 below, we impose linear conditions by asking that the multiplicities of the curves at p exceed a given value r.

Definition 5.3.2. Let $d \geq 1$ be an integer.

1. A **linear system** of curves of degree d in $\mathbb{P}^2$ is a linear subspace $\mathbb{P}(L) \subset \mathbb{P}(L(d))$. A point $p \in \mathbb{P}^2$ is a **base point** of $\mathbb{P}(L)$ if every curve in $\mathbb{P}(L)$ passes through p. The words **pencil**, **net**, and **web** refer to a linear system of dimension 1,2, and 3, respectively.
2. If $p_1, \ldots, p_s \in \mathbb{P}^2$ are distinct points, and $r_1, \ldots, r_s \geq 1$ are integers, we write

$$L(d; r_1p_1, \ldots, r_sp_s) := \{f \in L(d) \mid \text{mult}(f, p_i) \geq r_i \text{ for all } i\},$$

and call

$$\mathbb{P}(L(d; r_1p_1, \ldots, r_sp_s)) \subset \mathbb{P}(L(d))$$

the **linear system of curves of degree d with multiplicity at least r_i at p_i, for all i**. Moreover, we say that $p_1, \ldots, p_s$ are the **assigned base points** of $\mathbb{P}(L(d; p_1, \ldots, p_s))$. □

Proposition 5.3.3. *Let $p_1, \ldots, p_s \in \mathbb{P}^2$ be distinct points, and let $r_1, \ldots, r_s \geq 1$ be integers. Then $L(d; r_1p_1, \ldots, r_sp_s)$ is a linear subspace of $L(d)$ of dimension*

$$\dim_{\mathbb{K}} L(d; r_1p_1, \ldots, r_sp_s) \geq \binom{d+2}{2} - \sum_i \binom{r_i+1}{2}. \tag{5.2}$$

Proof. Since $L(d; r_1p_1, \ldots, r_sp_s) = \bigcap_i L(d; r_ip_i)$, it suffices to treat the points seperately. After a change of coordinates, we may suppose that the given point is the point $p = [0 : 0 : 1]$. Then, a polynomial $f = \sum f_{\alpha\beta} x^\alpha y^\beta z^{d-\alpha-\beta} \in L(d)$ vanishes at p with multiplicity at least r iff $f_{\alpha\beta} = 0$ for all α, β with $\alpha + \beta < r$. The result follows since there are $\binom{r+1}{2}$ monomials $x^\alpha y^\beta$ with $\alpha + \beta < r$. □

Whether equality or strict inequality holds in (5.2) depends on whether the conditions imposed by the different points are linearly independent or not. Both cases do occur. In the example below, which illustrates this, we say that three or more points $p_1, \ldots, p_s \in \mathbb{P}^2$ are **collinear** if the points lie on a line.

Example 5.3.4. For four distinct points $p_1, \ldots, p_4 \in \mathbb{P}^2$, (5.2) gives

$$\dim_{\mathbb{K}} L(2; p_1, \ldots, p_4) \geq 2.$$

If no three of these points are collinear, equality holds (make use of a suitable change of coordinates to reduce to the case treated in Example 5.3.1). If three of the points are collinear, say $p_1, p_2, p_3 \in L$, where $L \subset \mathbb{P}^2$ is a line, then L must be a component of any conic containing p_1, p_2, p_3 (one way of seeing this

is to apply Bézout's theorem which will be proved in the next section). Hence, a conic through p_1, p_2, p_3 is determined by the component residual to L, which may be any line. If we require that the conic also contains p_4, and if $p_4 \notin L$, the residual line must pass through p_4 which imposes one extra linear condition. If $p_4 \in L$, there is no extra condition. We conclude that $\dim_{\mathbb{K}} L(2; p_1, \ldots, p_4) = 2$ iff $p_1, \ldots, p_4$ are not collinear, and that $\dim_{\mathbb{K}} L(2; p_1, \ldots, p_4) = 3$ if the four points lie on a line. □

In the example, the dimension of the linear system under consideration depends on the position of the points in the plane – for "almost all" collections of four points, the dimension is 2, and it is 3 only in the special case where the four points are collinear. To give "almost all" a more precise meaning, we say that a condition on a collection of points is satisfied for points $p_1, \ldots, p_s$ in general position if the points for which the condition is satisfied can be chosen in the following way: if $p_1, \ldots, p_r$, $r < s$, are already given, there is a nonempty Zariski open (hence dense) subset $U \subset \mathbb{P}^2$ such that we can choose p_{r+1} from among the points in U (in the example, if p_1, p_2, p_3 are not collinear, take $U = \mathbb{P}^2$; if p_1, p_2, p_3 lie on a line L, take $U = \mathbb{P}^2 \setminus L$). With this notation, we have:

Proposition 5.3.5. *Let $p_1, \ldots, p_s \in \mathbb{P}^2$ be distinct points in general position. If $\binom{d+2}{2} \geq s$, then*

$$\dim_{\mathbb{K}} L(d; p_1, \ldots, p_s) = \binom{d+2}{2} - s.$$

Proof. The result follows from the lemma below by induction on s. □

Lemma 5.3.6. *Let $\mathbb{P}(L) \subset \mathbb{P}(L(d))$ be a nonempty linear system. Then there is a nonempty Zariski open subset $U \subset \mathbb{P}^2$ such that $L \cap L(d; p) \subset L$ has codimension 1 for all $p \in U$.*

Proof. Since $L(d; p)$ is a hyperplane in $L(d)$, the linear subspace $L \cap L(d; p)$ of L has codimension one iff $L \not\subset L(d; p)$. But if f is any nonzero polynomial in L, then $f \notin L(d; p)$ for any point $p \in U := \mathbb{P}^2 \setminus \mathrm{V}(f)$. □

In the case where not each $r_i = 1$, it is an open problem to determine the tupels $(d, r_1, \ldots, r_n)$ for which the analogue of Proposition 5.3.5 holds (see Ciliberto and Miranda (2000) for some recent research).

Example 5.3.7. For five distinct points $p_1, \ldots, p_5 \in \mathbb{P}^2$, inequality (5.2) gives

$$\dim_{\mathbb{K}} L(4; 2p_1, \ldots, 2p_5) \geq 0.$$

However, we always have the sharper estimate

$$\dim_{\mathbb{K}} L(4; 2p_1, \ldots, 2p_5) \geq 1.$$

Indeed, since $\dim_{\mathbb{K}} L(2; p_1, \ldots, p_5) \geq 1$, there is a conic $\mathrm{V}(f)$ passing through all 5 points, and $f^2 \in L(4; 2p_1, \ldots, 2p_5)$. □

The remark below contains a simple example which prepares for the subsequent exercises:

Remark 5.3.8. If $p = [a_0 : a_1 : a_2],\ q = [b_0 : b_1 : b_2] \in \mathbb{P}^2(\Bbbk)$ are two distinct points, the unique line passing through p and q is defined by the determinantal equation

$$\det \begin{pmatrix} x_0 & x_1 & x_2 \\ a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 \end{pmatrix} = 0.$$

□

Exercise 5.3.9. If $p_1, \ldots, p_5 \in \mathbb{P}^2$ are five distinct points such that no three are collinear, show that there is a unique conic passing through the five points, show that this conic is nondegenerate, and give a determinantal equation for the conic. What happens if we only suppose that no four of the points are collinear? □

Exercise 5.3.10. If $p_1, p_2, p_3 \in \mathbb{R}^2$ are three points not lying on a line, show that there is a unique circle passing through these points, and give a determinantal equation for the circle.
Hint. Note that the set of all circles is an affine chart of a 3-dimensional linear system $L \subset \mathbb{P}(\mathbb{R}[x, y]_{\leq 2}) = \mathbb{P}(\mathbb{R}[x, y, z]_2)$. The base points of this system in $\mathbb{P}^2(\mathbb{C})$ are known as the **circle points**. Where do these points lie? □

If d is large enough, we always get the dimension expected from (5.2):

Proposition 5.3.11. *Let $p_1, \ldots, p_s \in \mathbb{P}^2$ be distinct points, and let $r_1, \ldots, r_s$ be integers ≥ 1. If $d \geq (\sum_i r_i) - 1$, then*

$$\dim_{\mathbb{K}} L(d; r_1 p_1, \ldots, r_s p_s) = \binom{d+2}{2} - \sum_i \binom{r_i + 1}{2}.$$

Proof. We do induction on $m := (\sum_i r_i) - 1$. If $m \leq 1$, then either $s = 1$, or $s = 2$ and $r_1 = r_2 = 1$. In both cases, the result is clear. We may, hence, suppose that $d \geq m > 1$. In the induction step, we distinguish two cases.

Case 1. Suppose that each $r_i = 1$. Choose a linear form l_0 not vanishing at any p_i (this is possible since "not vanishing at a point" imposes a Zariski open (dense) condition on lines). In addition, for $i = 1, \ldots, s-1$, choose linear forms l_i such that $p_i \in \mathrm{V}(l_i)$, but $p_j \notin \mathrm{V}(l_i)$ for $j \neq i$. Then $f := l_1 \cdots l_{s-1} \cdot l_0^{d-s+1} \in L(d; p_1, \ldots, p_{s-1}) \setminus L(d; p_1, \ldots, p_s)$. This shows that $L(d; p_1, \ldots, p_s) \subsetneq L(d; p_1, \ldots, p_{s-1})$, and we are done by applying the induction hypothesis.

Case 2. Now, suppose that not all $r_i = 1$, say $r := r_1 > 1$. Assume that $p_1 = [0 : 0 : 1]$, and set $L_0 = L(d; (r_1 - 1)p_1, r_2 p_2, \ldots, r_s p_s)$. Then, for any $f \in L_0$, the dehomogenization $f(x, y, 1)$ is of type

$$f(x, y, 1) = \sum_{i=0}^{r-1} f_i x^i y^{r-1-i} + \text{ terms of higher degree.}$$

Setting $L_i = \{f \in L_0 \mid f_j = 0 \text{ for all } j < i\}$, we get a filtration

$$L_0 \supset L_1 \supset \ldots \supset L_r = L(d; r_1p_1, \ldots, r_sp_s).$$

Since the induction hypothesis applies to L_0, it suffices to show that $L_i \supsetneq L_{i+1}$, $i = 0, \ldots, r-1$. For this, set $W_0 = L(d-1; (r-2)p_1, r_2p_2, \ldots, r_sp_s)$. Following the recipe above, define a filtration

$$W_0 \supset W_1 \supset \ldots \supset W_{r-1} = L(d-1; (r-1)p_1, r_2p_2, \ldots, r_sp_s).$$

By the induction hypothesis, $W_i \supsetneq W_{i+1}$, $i = 0, \ldots, r-2$. Choosing polynomials $f_i \in W_i \setminus W_{i+1}$, we have $yf_i \in L_i \setminus L_{i+1}$, $i = 0, \ldots, r-2$, and $xf_{r-2} \in L_{r-1} \setminus L_r$. This concludes the proof. □

Exercise 5.3.12. For each set of integers $r_1, \ldots, r_s \geq 1$, show by example that the conclusion of the proposition may be wrong if $d = (\sum r_i) - 2$. □

5.4 Bézout's Theorem and Applications

The projective plane has been constructed such that any two distinct lines intersect in a unique point. The theorem of Bézout says that much more is true: given two curves in $\mathbb{P}^2$ of arbitrary degrees $d, e \geq 1$, the curves intersect in $d \cdot e$ points, counted with multiplicity. The proof of the theorem, which will be given in this section, is an application of elimination: we proceed by projecting the intersection points to a line. For this, we will consider the resultant which is a classical tool in elimination theory (its use can be traced back to work of Leibniz, Newton, Euler, and others – see the accounts in Kline (1972) and von zur Gathen and Gerhard (1999)).

Given two univariate polynomials f, g, the resultant of f and g is a polynomial expression in the coefficients of f and g which vanishes iff f and g have a nontrivial common factor (see Theorem 5.4.3 below). In the classical papers, the authors obtained the resultant by different ways of eliminating the variable from the system $f = g = 0$. Accordingly, there are different ways of representing the resultant. We will define it, here, as the determinant of the Sylvester matrix which provides one natural way of introducing linear algebra into the common factor problem.

Let R be a ring, and let

$$\begin{aligned} f = &\quad a_0x^d + a_1x^{d-1} + \ldots + a_d, \\ g = &\quad b_0x^e + b_1x^{e-1} + \ldots + b_e \quad \in R[x] \end{aligned} \tag{5.3}$$

be two polynomials of degrees $d, e \geq 1$. Then the **Sylvester matrix** of f and g is the matrix

$$\mathrm{Syl}(f,g) = \begin{pmatrix} a_0 & 0 & \dots & 0 & b_0 & 0 & \dots & 0 \\ a_1 & a_0 & & \vdots & b_1 & b_0 & & \vdots \\ \vdots & a_1 & \ddots & \vdots & \vdots & b_1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & a_0 & \vdots & \vdots & \ddots & b_0 \\ a_d & & & a_1 & b_e & & & b_1 \\ 0 & a_d & & \vdots & 0 & b_e & & \vdots \\ \vdots & & \ddots & \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & a_d & 0 & 0 & \dots & b_e \end{pmatrix}.$$

Note that $\mathrm{Syl}(f,g)$ is a square matrix of size $d+e$: there are e colums containing a_i's, and d columns containing b_j's.

Definition 5.4.1. With notation as above, the **resultant** of f and g is the determinant

$$\mathrm{Res}(f,g) = \det \mathrm{Syl}(f,g) \in R. \qquad \square$$

Remark 5.4.2. No matter what ring we are considering, the resultant as a determinant can always be computed using the same recipe. We conclude that the construction of the resultant is universal in the following sense: If S is the polynomial ring

$$S = \mathbb{Z}[u_i, v_j \mid i = 0, \dots, d,\ j = 0, \dots, e]$$

in $d + e + 2$ variables with integer coefficients, and

$$\begin{aligned} F = &\quad u_0 x^d + u_1 x^{d-1} + \cdots + u_d, \\ G = &\quad v_0 x^e + v_1 x^{e-1} + \cdots + v_e \quad \in S[x] \end{aligned}$$

are the "generic" polynomials in x of degrees d, e, then for any ring R and any two polynomials f, g as in (5.3), $\mathrm{Res}(f,g)$ is obtained from $\mathrm{Res}(F,G)$ by substituting the a_i, b_j for the u_i, v_j. $\square$

Theorem 5.4.3. *Let R be a UFD, and let $f, g \in R[x]$ be polynomials of degrees $d, e \geq 1$. Then f and g have a common factor of degree ≥ 1 iff* $\mathrm{Res}(f,g) = 0$.

Proof. Consider the "linear combination map"

$$\phi : R[x]_{<e} \oplus R[x]_{<d} \to R[x]_{<d+e},\ (A,B) \mapsto Af + Bg.$$

This is a map between two free R-modules of rank $d + e$ which, with respect to the R-bases

$$(x^{e-1}, 0), (x^{e-2}, 0), \dots, (1,0), (0, x^{d-1}), \dots, (0,1)$$

and

$$x^{d+e-1}, \ldots, x, 1,$$

is represented by the Sylvester matrix $\mathrm{Syl}(f,g)$. We conclude that ϕ is injective iff $\mathrm{Res}(f,g) \neq 0$. On the other hand, since R is a UFD, ϕ is injective iff $\mathrm{GCD}(f,g) = 1$. Indeed, if $h := \mathrm{GCD}(f,g) \neq 1$, then $(-g/h, f/h) \in \ker\phi$. Conversely, suppose that $\mathrm{GCD}(f,g) = 1$, and let $(A,B)^t \in \ker\phi$ be a syzygy on f,g. Then $Af = -Bg$, which implies that B is a multiple of f. By degree reasoning, B and, thus, A are zero. □

Note that if $R = \Bbbk$ is a field, then f and g have a nontrivial common factor iff they have a common root in some algebraically closed extension field of $\Bbbk$. It was precisely the search for common (complex) roots which led the classical authors to consider the resultant.

Example 5.4.4. Computing the resultant of the two polynomials

$$f = 3x^2 + 5x - 2, \quad g = 7x^3 + x + 4 \in \mathbb{Q}[x],$$

we get

$$\mathrm{Res}(f,g) = \det \mathrm{Syl}(f,g) = \det \begin{pmatrix} 3 & 0 & 0 & 7 & 0 \\ 5 & 3 & 0 & 0 & 7 \\ 2 & 5 & 3 & 1 & 0 \\ 0 & 2 & 5 & 4 & 1 \\ 0 & 0 & 2 & 0 & 4 \end{pmatrix} = 1142792 \neq 0.$$

Hence, f and g do not have a common root in $\mathbb{C}$. □

Exercise 5.4.5. Let R be an integral domain, and let $f, g \in R[x]$ be two polynomials of degrees ≥ 1. Then show that

$$\mathrm{Res}(f,g) \in \langle f, g\rangle \cap R. \tag{5.4}$$

More precisely, show that there are polynomials $A, B \in R[x]$ such that $Af + Bg = \mathrm{Res}(f,g)$, $\deg A < \deg g$, and $\deg B < \deg f$. □

It is property (5.4) which links the resultant to elimination. Here are the details: Given two polynomials $f, g \in \Bbbk[x_1, \ldots, x_n]$ of degree ≥ 1 in x_1, we may associate a resultant to f,g and the variable $x = x_1$ by regarding f,g as univariate polynomials in x_1. To indicate the distinguished variable, we, then, write $\mathrm{Syl}(f,g,x_1)$ for the Sylvester matrix and $\mathrm{Res}(f,g,x_1)$ for the resultant. Note that $\mathrm{Res}(f,g,x_1)$ is a polynomial in $R = \Bbbk[x_2, \ldots, x_n]$ which, by (5.4), is contained in the first elimination ideal of $\langle f,g\rangle \subset \Bbbk[x_1, \ldots, x_n]$. Moreover, if $(a_2, \ldots, a_n) \in \mathbb{A}^{n-1}(\Bbbk)$ is a point such that neither of the leading coefficients of $f, g \in R[x_1]$ vanishes at $(a_2, \ldots, a_n)$, then, by Remark 5.4.2,

$$\mathrm{Res}(f,g,x_1)(a_2, \ldots, a_n) = \mathrm{Res}(f(x_1, a_2, \ldots, a_n), g(x_1, a_2, \ldots, a_n)). \tag{5.5}$$

The following exercise illustrates the use of this by an example which, at the same time, shows that $\mathrm{Res}(f,g,x_1)$ may fail to generate the elimination ideal.

Exercise 5.4.6. Consider the polynomials

$$f = xy^2 - xy - y^3 + 1, \;\; g = x^2y^2 - x^2y + xy - 1 \in \mathbb{Q}[x, y].$$

1. Compute that

$$\begin{aligned}\mathrm{Res}(f, g, x) &= \det \begin{pmatrix} y^2 - y & 0 & y2 - y \\ -y^3 + 1 & y^2 - y & y \\ 0 & -y^3 + 1 & -1 \end{pmatrix} \\ &= y^8 - y^7 + y^6 - 3y^5 + y^4 + y^3 + y^2 - y \\ &= y(y-1)^2(y^5 + y^4 + 2y^3 - y - 1).\end{aligned}$$

   Since the resultant is contained in the elimination ideal $\langle f, g\rangle \cap \mathbb{Q}[y]$, the y-values of the complex solutions of $f = g = 0$ must be among its roots. This gives eight candidates for the y-values.
2. If $\pi : \mathbb{A}^2 \to \mathbb{A}^1$ is projection onto the y-component, show that

$$\pi(\mathrm{V}(f, g)) \subsetneq \mathrm{V}(\mathrm{Res}(f, g)).$$

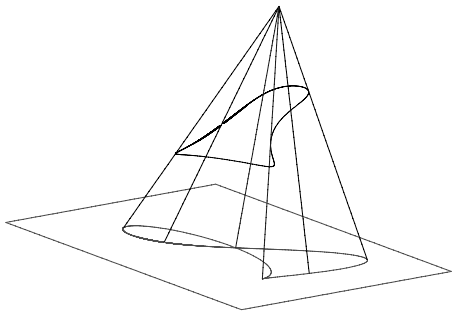
   Exactly, what y-value does not have a preimage point?
3. Use Gröbner bases to compute that the elimination ideal $\langle f, g\rangle \cap \mathbb{Q}[y]$ is generated by the polynomial $(y-1)^2(y^5 + y^4 + 2y^3 - y - 1)$. Compare this with the result of the previous part. □

Exercise* 5.4.7. Let $f, g \in \Bbbk[x_1, \ldots, x_n]$ be forms of degrees $d, e \geq 1$. Suppose that both $f(1, 0, \ldots, 0)$ and $g(1, 0, \ldots, 0)$ are nonzero. That is, the leading coefficients of f and g – regarded as polynomials in x_1 – are nonzero constants. Then show that $\mathrm{Res}(f, g, x_1)$ is homogeneous of degree $d \cdot e$. □

In the projective setting, there is no value for the point $p = [1 : 0 : \cdots : 0] \in \mathbb{P}^n$ under projection onto the last n components. We are, thus, led to consider the projection map

$$\pi : \mathbb{P}^n \setminus \{p\} \to \mathbb{P}^{n-1}, \; [a_0 : \cdots : a_n] \mapsto [a_1 : \cdots : a_n].$$

More geometrically, think of $\mathbb{P}^{n-1}$ as the hyperplane $H_0 = \mathrm{V}(x_0) \subset \mathbb{P}^n$. Then the image of a point $q \in \mathbb{P}^n \setminus \{p\}$ under π is the intersection of the line spanned by p and q with H_0. More generally, if $H \subset \mathbb{P}^n$ is any hyperplane, and $p \in \mathbb{P}^n \setminus H$ is any point, the same recipe gives a map from $\mathbb{P}^n \setminus \{p\}$ to $H \cong \mathbb{P}^{n-1}$. This map is called **projection from p to H**.



We can, now, prove Bézout's theorem:

Theorem 5.4.8 (Bézout). *Let $f, g \in \Bbbk[x, y, z]$ be forms of degrees $d, e \geq 1$. Assume that f and g have no common component. Then*

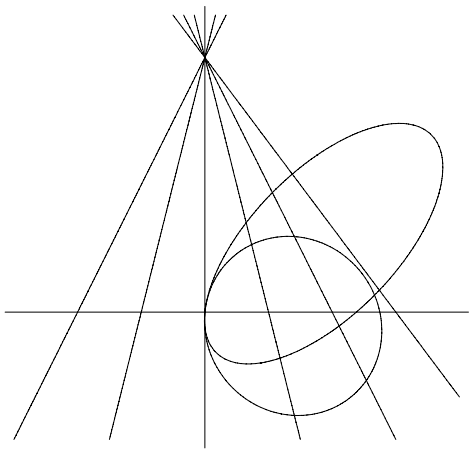
$$\sum_{p \in \mathbb{P}^2} i(f, g; p) = d \cdot e. \tag{5.6}$$

Proof. Step 1. It follows from the assumption on f, g and property 2 of intersection multiplicities (see Theorem 4.3.18) that $i(f, g; p) < \infty$ for each point p. Using the assumption again, we find that there are only finitely many intersection points of f and g (apply Exercise 1.7.13 in each coordinate chart). Since $i(f, g; p) \neq 0$ iff $p \in \mathrm{V}(f) \cap \mathrm{V}(g)$ (this is property 1 of intersection multiplicities), we conclude that the sum on the left hand side of (5.6) makes sense.

Step 2. Since $\mathrm{V}(f) \cup \mathrm{V}(g)$ is strictly contained in $\mathbb{P}^2$ by the Nullstellensatz, we may choose the coordinates such that the point $[0 : 1 : 0] \notin \mathrm{V}(f) \cup \mathrm{V}(g)$. That is, we may assume the leading coefficients of the forms f, g – regarded as polynomials in y – are nonzero constants. Let

$$\pi : \mathbb{P}^2 \setminus [0 : 1 : 0] \to \mathbb{P}^1, \ [a : b : c] \mapsto [a : c],$$

be projection from $[0 : 1 : 0]$ to the line $\mathrm{V}(y) \cong \mathbb{P}^1$:



Then a point $q = [a : c] \in \mathbb{P}^1$ is the image of a point $p \in \mathrm{V}(f) \cap \mathrm{V}(g)$ iff $f(a, y, c)$ and $g(a, y, c)$ have a common factor. Equivalently, by Theorem 5.4.3, the resultant

$$F := \mathrm{Res}(f, g, y) \in \Bbbk[x, z]$$

vanishes at $[a : c]$. By Exercise 5.4.7, F is a form of degree $d \cdot e$ which by Theorem 5.4.3 and the assumption on f, g, is nonzero. It follows that

$$\sum_{q \in \mathbb{P}^1} \mathrm{mult}(F, q) = d \cdot e$$

(counted with multiplicity, there are $\deg F(x, 1)$ zeros of F in the affine chart $\mathrm{D}(z)$ of $\mathbb{P}^1$, whereas $\mathrm{mult}(F, [1 : 0]) = \deg F - \deg F(x, 1)$).

To prove (5.6), it remains to show that the relevant multiplicities match: We claim that

$$\mathrm{mult}(F, q) = \sum_{\substack{p \in \mathrm{V}(f) \cap \mathrm{V}(g) \\ \pi(p) = q}} i(f, g; p),$$

for all points $q \in \mathbb{P}^1$ with $F(q) = 0$.

Step 3. Given a point $q \in \mathbb{P}^1$ as above, we may suppose after a further projective change of coordinates that $q = [0 : 1]$. Then all intersection points mapped to q lie in the affine chart $U = \mathrm{D}(z) \cong \mathbb{A}^2$ of $\mathbb{P}^2$. Thus, writing $f^a = f(x, y, 1)$, $g^a = g(x, y, 1)$, and $\mathcal{O}_p = \mathcal{O}_{\mathbb{A}^2, p}$, the claim from Step 2 reads

$$\mathrm{mult}(F(x, 1), 0) = \dim_{\mathbb{K}} \prod_{\substack{p \in \mathrm{V}(f) \cap \mathrm{V}(g) \\ \pi(p) = q}} \mathcal{O}_p / \langle f^a, g^a \rangle \mathcal{O}_p.$$

Step 4. Since there are only finitely many intersection points, Corollary 4.6.17 gives us an isomorphism of $\mathbb{K}$-algebras

$$M := \mathbb{K}[x,y]/\langle f^a, g^a\rangle \cong \prod_{p\in \mathrm{V}(f)\cap\mathrm{V}(g)\cap U} \mathcal{O}_p/\langle f^a, g^a\rangle\mathcal{O}_p. \tag{5.7}$$

Step 5. To relate (5.7) to the claim in Step 3, we have to get rid of the intersection points which are not mapped to q. For this, we localize: Let $h \in \Bbbk[x]$ be a generator for $\langle F(x,1)\rangle : x^\infty$. Then h vanishes precisely at the points of $\mathrm{V}(f)\cap\mathrm{V}(g)\cap U \setminus \pi^{-1}(q)$. In algebraic terms, for $p \in \mathrm{V}(f)\cap\mathrm{V}(g)\cap U$, the residue class of h in $\mathcal{O}_p/\langle f^a, g^a\rangle\mathcal{O}_p$ is a unit if $p \in \pi^{-1}(q)$, and is nilpotent otherwise (recall from Step 1 that $\dim_{\mathbb{K}} \mathcal{O}_p/\langle f^a, g^a\rangle\mathcal{O}_p < \infty$). Hence, after inverting h on both sides of (5.7), we have

$$M[h^{-1}] := \mathbb{K}[x,y,h^{-1}]/\langle f^a, g^a\rangle \cong \prod_{\substack{p\in \mathrm{V}(f)\cap\mathrm{V}(g)\\ \pi(p)=q}} \mathcal{O}_p/\langle f^a, g^a\rangle\mathcal{O}_p. \tag{5.8}$$

Step 6. Since M is generated by (the residue class of) y as a $\mathbb{K}[x]$-algebra, and since the leading coefficients of the forms f, g – regarded as polynomials in y – are nonzero constants, the powers $1, y, \ldots, y^{\min(d,e)-1}$ generate M as a $\mathbb{K}[x]$-module. Working with the larger set of generators $y^{d+e-1}, \ldots, y, 1$, and writing $R = \mathbb{K}[x]$, we get the free presentation

$$R[y]_{<e} \oplus R[y]_{<d} \xrightarrow{\phi} R[y]_{<d+e} \to M \to 0,$$

where ϕ is the linear combination map

$$(A, B) \mapsto Af + Bg.$$

This map is represented by the Sylvester matrix $\mathrm{Syl}(f^a, g^a, y)$ which, then, is also a representation matrix for $M[h^{-1}]$ considered as an $R[h^{-1}] = \mathbb{K}[x, h^{-1}]$-module. Since $R[h^{-1}]$ is a PID, and $M[h^{-1}]$ is annihilated by a power of x (this is clear from the right hand side of (5.8)), the structure theorem for modules over PID's gives that $\mathrm{Syl}(f^a, g^a, y)$ has a Smith normal form of type

$$\mathrm{Syl}(f^a, g^a, y) \underset{R}{\sim} \begin{pmatrix} x^{m_1} & 0 & \ldots & 0 \\ 0 & x^{m_2} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & x^{m_{d+e}} \end{pmatrix}$$

(see Example 2.8.8, Definition 2.8.9, and Exercise 2.8.10). We conclude that

$$\mathrm{mult}(F(x,1),0) = \mathrm{mult}(\det \mathrm{Syl}(f^a, g^a), 0) = \sum_{i=1}^{e+d} m_i = \dim_{\mathbb{K}} M[h^{-1}].$$

This finishes the proof. □

Example 5.4.9. Consider the quadratic forms

$$f = x^2 + y^2 - xz, \quad g = (x-y)^2 + 2(y+x)^2 - 3xz.$$

Then $[0:1:0] \notin \mathrm{V}(f) \cup \mathrm{V}(g)$. With notation as in the proof above, we have

$$\mathrm{Syl}(f^a, g^a, y) = \begin{pmatrix} 1 & 0 & 3 & 0 \\ 0 & 1 & 2x & 3 \\ x^2 - x & 0 & 3x^2 - 3x & 2x \\ 0 & x^2 - x & 0 & 3x^2 - 3x \end{pmatrix} \underset{\mathbb{K}[x]}{\sim} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & x & 0 \\ 0 & 0 & 0 & x^2(x-1) \end{pmatrix},$$

so that, as $\mathbb{K}[x]$-modules,

$$M = \operatorname{coker} \mathrm{Syl}(f^a, g^a, y) \cong \mathbb{K}[x]/\langle x \rangle \oplus \mathbb{K}[x]/\langle x^2 \rangle \oplus \mathbb{K}[x]/\langle x - 1 \rangle$$

(see Exercise 2.8.10). From this decomposition, it is clear that f and g intersect with multiplicity one at a point p_1 of type $p_1 = [1 : \beta_1 : 1]$, and one might be tempted to believe that there are two *distinct* intersection points $p_{2/3}$ of type $p_j = [0 : \beta_j : 1]$. This naive guess, however, is not true. One way of seeing this is to interchange the role of x and y in the proof of Bézout's theorem (note that $[1:0:0] \notin \mathrm{V}(f) \cup \mathrm{V}(g)$):

$$\mathrm{Syl}(f^a, g^a, x) = \begin{pmatrix} 1 & 0 & 3 & 0 \\ -1 & 1 & 2y - 3 & 3 \\ y^2 & -1 & 3y^2 & 2y - 3 \\ 0 & y^2 & 0 & 3y^2 \end{pmatrix} \underset{\mathbb{K}[y]}{\sim} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & y & 0 \\ 0 & 0 & 0 & y^3 \end{pmatrix}.$$

Now, we conclude, that there is an intersection point p_2 of multiplicity at least three of type $p_2 = [\alpha_2 : 0 : 1]$ (and possibly another intersection point of the same type). Taking Bézout's Theorem into account and comparing with what we got above, we find that

$$\mathrm{V}(f) \cap \mathrm{V}(g) = \{[1:0:1], [0:0:1]\},$$

with intersection multiplicities

$$i(f, g; p_1) + i(f, g; p_2) = 1 + 3 = 4 = \deg C \cdot \deg D.$$

□

Exercise 5.4.10. Let $f, g \in \Bbbk[x, y, z]$ be nonconstant forms. Show that f and g intersect transversally at each point of $\mathrm{V}(f) \cap \mathrm{V}(g) \cap \mathrm{D}(z)$ iff, with notation as in the proof of Bézout's theorem, every elementary divisor of $\mathrm{Syl}(f^a, g^a, y)$ over $\mathbb{K}[x]$ is square-free. □

Exercise 5.4.11. Let $p_1, \ldots, p_4 \in \mathbb{A}^2$ be four points in the affine plane such that no three are collinear. Then show that there is a parabola passing through these points iff $p_1, \ldots, p_4$ do not form a parallelogram.
Hint: A parabola in $\mathbb{A}^2$ is the affine part of a nondegenerate conic in $\mathbb{P}^2$ which intersects the line at infinity in a single point with multiplicity 2. □

As an application of Bézout's Theorem, we give a bound on the number of singular points of a plane curve:

Theorem 5.4.12. *Let $C \subset \mathbb{P}^2$ be a curve of degree $d \geq 1$. If r_p denotes the multiplicity of C at a point $p \in \mathbb{P}^2$, then:*

1. *C has at most $\binom{d}{2}$ singular points. More precisely,*

$$\sum_{p \in C} \binom{r_p}{2} \leq \binom{d}{2}.$$

2. *If C is irreducible, then C has at most $\binom{d-1}{2}$ singular points. More precisely,*

$$\sum_{p \in C} \binom{r_p}{2} \leq \binom{d-1}{2}.$$

Proof. If $d = 1$, then C is a line, and there is nothing to show. We may, hence, assume that $d \geq 2$. Let $p_1, \ldots, p_s$ be the distinct singular points of C, and write $r_i = r_{p_i}$. Moreover, let $f \in \mathbb{K}[x, y, z]$ be a square-free form defining C.

1. Since f is square-free, not all formal partial derivatives of f vanish, and we may suppose that $\frac{\partial f}{\partial x} \neq 0$. Then f and $\frac{\partial f}{\partial x}$ have no common component. Applying Bézout's theorem, we conclude that f and $\frac{\partial f}{\partial x}$ intersect in $d(d-1)$ points, counted with multiplicity. On the other hand, $\operatorname{mult}(\frac{\partial f}{\partial x}, p_i) \geq \operatorname{mult}(f, p_i) - 1 = r_i - 1$ for all i. Taking property 3 of intersection multiplicities into account (see Theorem 4.3.18), we get, as desired:

$$d(d-1) = \sum_i i(f, \frac{\partial f}{\partial x}, p_i) \geq \sum_i \operatorname{mult}(f, p_i) \cdot \operatorname{mult}(\frac{\partial f}{\partial x}, p_i) \geq \sum_i r_i(r_i - 1).$$

2. By Proposition 5.3.3 and part 1,

$$\dim_{\mathbb{K}} L(d-1; (r_1-1)p_1, \ldots, (r_s-1)p_s) \geq \binom{d+1}{2} - \sum_i \binom{r_i}{2} \geq d.$$

In particular, $t := \binom{d+1}{2} - \sum \binom{r_i}{2} - 1 \geq 1$, and we may choose smooth points $q_1, \ldots, q_t \in C$. Once more applying Proposition 5.3.3, we see that we can find a nonzero form $g \in L(d-1; (r_1-1)p_1, \ldots, (r_s-1)p_s, q_1, \ldots, q_t)$. Since, by assumption, f is irreducible, the forms f and g have no component in common. Making use of Bézout's theorem and arguing as in part 1, we get

$$d(d-1) \geq \sum_i r_i(r_i-1) + t = \sum_i r_i(r_i-1) + \frac{d^2+d-2}{2} - \sum_i \binom{r_i}{2}.$$

The desired bound follows. □

Theorem 5.4.13. *Let $C \subset \mathbb{P}^2$ be an irreducible curve of degree $d \geq 1$ such that $\binom{d-1}{2} = \sum_{p \in C} \binom{r_p}{2}$. Then C admits a rational parametrization.*

Proof. The basis idea is the same as in the proof of part 2 of Theorem 5.4.12. If we choose $t-1 = \binom{d+1}{2} - \sum \binom{r_i}{2} - 2$ addititional points $q_1, \ldots, q_{t-1}$ on C then

$$\mathbb{P}(L(d-1; (r_1-1)p_1, \ldots, (r_s-1)p_s, q_1, \ldots, q_{t-1})) = \mathbb{P}(\langle g_0, g_1 \rangle)$$

is a pencil of curves, whose intersection points except one with C are known to us. Thus, if $p(t_0, t_1)$ denotes the moving intersection point of $C \cap \mathrm{V}(t_0 g_0 + t_1 g_1)$ then

$$\mathbb{P}^1 \to C,\ [t_0 : t_1] \mapsto p(t_0, t_1)$$

is the desired parmetrization. This proves the Theorem for algebraically closed fields. Before we complete the proof for arbitrary fields, we discuss the resulting algorithm.

Remark 5.4.14. Suppose that C contains a smooth $\Bbbk$-rational point. Then C can be parametrized by rational functions defined over $\Bbbk$. □

Remark 5.4.15. Using the concept of the bihomogeneous coordinate ring $R = \Bbbk[x_0, x_1, x_2, t_0, t_1]$ of $\mathbb{P}^2 \times \mathbb{P}^1$, which we will introduce properly in Section 6, we can compute the parametrization explicitely as follows.

Let f be the equation of C. The zero locus of the ideal $J = \langle f, t_0 g_0 + t_1 g_1 \rangle \subset R$ decompose into

$$\mathrm{V}(J) = (B \times \mathbb{P}^1) \cup C' \subset \mathbb{P}^2 \times \mathbb{P}^1,$$

where $B = \mathrm{V}(g_1, g_2) \cap C \subset \mathbb{P}^2$ is the base loci of the pencil on C. The component C' is the graph of the desired parmetrization. Note that the two hypersufaces $C \times \mathbb{P}^1$ and $\mathrm{V}(t_0 g_0 + t_1 g_1)$ intersect transversally along $(C' \setminus B) \times \mathbb{P}^1$, because the additional intersection is simple. Thus, if we saturate J in $\langle g_0, g_1 \rangle$ and $\langle t_0, t_1 \rangle$, we obtain the bihomogeneous ideal of $C' \subset \mathbb{P}^2 \times \mathbb{P}^1$:

$$\mathrm{I}(C') = (\langle f, t_0 g_0 + t_1 g_1 \rangle : \langle g_0, g_1 \rangle^N) : \langle t_0, t_1 \rangle^N \subset R$$

for N large enough. On the other hand, the rational map

$$\mathbb{P}^1 \to C,\ [t_0 : t_1] \mapsto p(t_0, t_1) = [\varphi_0(t_0, t_1) : \varphi_1(t_0, t_1) : \varphi_2(t_0, t_1)],$$

is defined by three forms $\varphi_0, \varphi_1, \varphi_2 \in \Bbbk[t_0, t_1]$ of degree d. So $\mathrm{I}(C')$ contains the minors of the matrix

$$\begin{pmatrix} x_0 & x_1 & x_2 \\ \varphi_0 & \varphi_1 & \varphi_2 \end{pmatrix}.$$

Since there cannot be more than 3 equations of bi-degree $(1, d)$ in $\mathrm{I}(C')$, we can get the bi-graded piece $\mathrm{I}(C')_{(1,d)}$ spanned by these minors from $\mathrm{I}(C')$. Finally, to compute ${}^t(\varphi_0, \varphi_1, \varphi_2)$ from the space of minors $\langle m_0, m_1, m_2 \rangle$, we calculate the syzygy of the matrix $(\frac{\partial m_i}{\partial x_j})_{i,j=0,1,2}$.

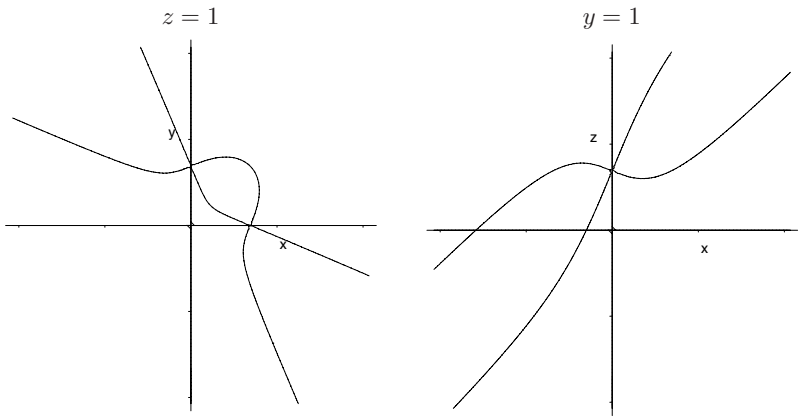
Returning to the proof of the theorem, suppose that the field of definition of C is $\Bbbk = \mathbb{Q}$. Then we would like the polynomials $\varphi_0, \varphi_1, \varphi_2 \in \mathbb{Q}[t_0, t_1]$ such that $\mathbb{P}^1(\mathbb{Q})$ parametrizes $C(\mathbb{Q})$ with perhaps of the exception of a few singular points. For this we need that $L(d-1; (r_1-1)p_1, \ldots, (r_s-1)p_s, q_1, \ldots, q_{t-1})$ is defined over $\mathbb{Q}$. For the singular points this is no problem: They might not be defined individually over $\mathbb{Q}$, but the collection $Sing_r = \{p \in C \mid \text{mult}(C,p) = r\}$ is defined over $\mathbb{Q}$. So we need to find additional points $q_1, \ldots, q_{t-1}$ in C which are defined over $\mathbb{Q}$. A single point suffices if we alter the pencil.

Let $q \in C$ be a smooth point defined over $\mathbb{Q}$. Consider

$$L = \{g \in L(d-1; (r_1-1)p_1, \ldots, (r_s-1)p_s) \mid v_q(g) \geq t-1\}.$$

Then L has codimension at most $t-1$ in $L(d-1; (r_1-1)p_1, \ldots, (r_s-1)p_s))$ and $i(g, f; q) \geq t-1$ for every $g \in L$. Thus L is a pencil, again there is only one free intersection point and we obtain a parametrization defined over $\mathbb{Q}$. The same argument works for arbitrary fields of definition. □

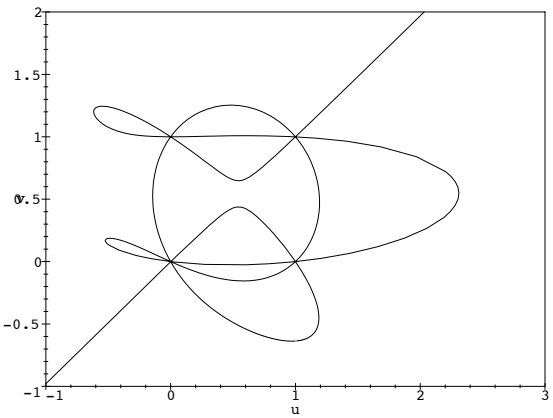
Exercise 5.4.16. Parametrize $V(2x^2y^2 - y^2(z-x-y)^2 - (z-x-y)^2x^2)$ over $\mathbb{Q}$.



□

Remark 5.4.17. In view of the application it is inconvenient, that we need a smooth rational point. Indeed this can be avoided as proved by Hilbert and Hurwitz [19xx]. A computer implementation of this algorithm was given in Maple packages [Winkler,19xx] and [?] and in Singular []. In general curves of odd degree defined over $\mathbb{Q}$ with $\binom{d-1}{2} = \sum_{p \in C} \binom{r_p}{2}$ always allow a $\mathbb{Q}$-rational parametrization. For even degree a quadratic field extension might be necessary, as we can see from the example of the conic $V(x^2 + y^2 + z^2)$, which has no real point, hence also no rational point.

Exercise 5.4.18. Compute a rational parametrization of the curve from Example 1.4.4,



$$11\,y^7 + 7\,y^6x + 8\,y^5x^2 - 3\,y^4x^3 - 10\,y^3x^4 - 10\,y^2x^5 - x^7 - 33\,y^6 - 29\,y^5x$$
$$-13\,y^4x^2 + 26\,y^3x^3 + 30\,y^2x^4 + 10\,yx^5 + 3\,x^6 + 33\,y^5 + 37\,y^4x - 8\,y^3x^2$$
$$-33\,y^2x^3 - 20\,yx^4 - 3\,x^5 - 11\,y^4 - 15\,y^3x + 13\,y^2x^2 + 10\,yx^3 + x^4 = 0$$

without using additional rational points except the 4 singular points.

Hint: Use a suitable pencil of curves of degrees $\leq d-1$. □

5.5 Max Noether's Fundamental Theorem

Let $f, g \in \Bbbk[x, y, z]$ be two forms of degrees ≥ 1 without common components. Then f and g intersect in finitely many points, and we could ask: which other forms pass through these points? Of course, there are the obvious forms of type $h = Af + Bg$. In the special case where f and g intersect in $\deg f \cdot \deg g$ *distinct* points, it follows from Max Noether's theorem that there are no other possibilities. More generally, if we allow arbitrary intersection multiplicities, the theorem tells us that a form h is contained in the image of the linear combination map $(A, B) \mapsto Af + Bg$ iff this containment condition is fulfilled locally at each intersection point of f and g.

In formulating a precise statement, we use the following notation. Given a form $f \in \Bbbk[x, y, z]$ and a point $p \in \mathbb{P}^2$, choose a coordinate chart U containing p and set $f_p = f^a \in \mathcal{O}_p$, where f^a is the dehomogenization of f in U. Then f_p depends on the choice of U, but only up to multiplication by a unit in $\mathcal{O}_p$. Hence, the local conditions in Max Noether's theorem below make sense.

Theorem 5.5.1 (Max Noether's Fundamental Theorem). *Let f, g, h be forms of degrees ≥ 1 in $\Bbbk[x, y, z]$. Assume that f and g have no common component. Then there is an expression*

$$h = Af + Bg,$$

with forms $A, B \in \mathbb{K}[x, y, z]$ of degrees $\deg h - \deg f$, $\deg h - \deg g$, iff

$$h_p \in \langle f_p, g_p \rangle \subset \mathcal{O}_p$$

for every point $p \in \mathrm{V}(f) \cap \mathrm{V}(g)$.

Proof. Clearly, the global condition in the theorem implies the local ones. For the converse, arguing as is in the proof of Proposition 5.3.11, we can find a linear form not vanishing at any of the finitely many intersection points of f ang g. We may, hence, choose the coordinates such that $\mathrm{V}(f) \cap \mathrm{V}(g) \cap \mathrm{V}(z) = \emptyset$. That is, to work with the local conditions, we may dehomogenize with respect to z. We give the remaining part of the proof in two steps, consisting of an affine and projective argument, respectively.

Step 1. We write $f^a = f(x, y, 1)$, $g^a = g(x, y, 1) \in \mathbb{K}[x, y]$ and consider the composite map

$$\phi : \mathbb{K}[x, y, z] \to \mathbb{K}[x, y] \to \bigoplus_{p \in \mathrm{V}(f) \cap \mathrm{V}(g)} \mathcal{O}_p / \langle f_p, g_p \rangle$$

defined by

$$h \mapsto h^a = h(x, y, 1) \mapsto (h_p + \langle f_p, g_p \rangle)_{p \in \mathrm{V}(f) \cap \mathrm{V}(g)}.$$

The local conditions in the theorem imply $\phi(h) = 0$, so that $h^a \in \langle f^a, g^a \rangle$ by Corollary 4.6.17. Homogenizing, we get an equation of type

$$z^k h = A' f + B' g,$$

for some k and some forms $A', B' \in \mathbb{K}[x, y, z]$. The theorem will follow once we show that multiplication by z is injective on $\mathbb{K}[x, y, z]/\langle f, g \rangle$.

Step 2. Let an equation of type $zh' = A'f + B'g$ in $\mathbb{K}[x, y, z]$ be given. We show that $h' \in \langle f, g \rangle$. For this, if $E \in \mathbb{K}[x, y, z]$ is any polynomial, we write $E_0 = E(x, y, 0)$. We, then, have $A'_0 f_0 + B'_0 g_0 = 0$. On the other hand, since f and g have no common zero on the line $\mathrm{V}(z)$, the polynomials f_0 and g_0 have no common factor. It follows that $(A'_0, B'_0) = c \cdot (-g_0, f_0)$ for some $c \in \mathbb{K}[x, y]$. Setting $A'' = A' + cg$ and $B'' = B' - cf$, we have $A''_0 = B''_0 = 0$, so that $A'' = zA$ and $B'' = zB$ for some forms A and B. Since $zh' = A'f + B'g = A''f + B''g = z(Af + Bg)$, we conclude that $h' = Af + Bg$, as desired. □

Remark 5.5.2. Nowadays, Max Noether's theorem is usually not treated in textbooks on algebraic curves since it can be easily deduced from the cohomological vanishing result

$$\mathrm{H}^1(\mathbb{P}^2, \mathcal{O}(h-d-e)) = 0.$$

In this first course on algebraic curves, we will not develop the machinery of sheaves and cohomology. In a second course, Max Noether's theorem may serve as a motivation for the interest in vanishing theorems. □

Corollary 5.5.3. *Let $f, h \in \Bbbk[x,y,z]$ be forms of degrees ≥ 1 which intersect in $\deg f \cdot \deg h$ distinct points. Let $g \in \Bbbk[x,y,z]$ be a form of degree ≥ 1 passing through $\deg f \cdot \deg g$ of these points. Then there is a form of degree $h-e$ in x,y,z passing through the residual $\deg f \cdot (\deg h - \deg g)$ points.*

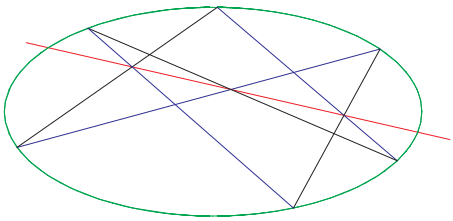
Proof. The conditions $h_p \in \langle g_p, f_p \rangle$ are satisfied, because g and f intersect transversally by Bézout's Theorem. Thus

$$h = af + bg$$

by Noether's Theorem. The polynomial b defines the curve of degree $h-e$, which contains the remaining $d \cdot (h-e)$ intersection points. □

A special case of the Corollary is Pascal's Theorem.

Example 5.5.4 (Pascal's Theorem). Consider a hexagon with vertices $p_1, \ldots, p_6 \in \mathbb{P}^2$ and the three intersection points $q_1 = \overline{p_1p_2} \cap \overline{p_4p_5}, q_2 = \overline{p_2p_3} \cap \overline{p_5p_6}, q_3 = \overline{p_3p_4} \cap \overline{p_6p_1}$ of the opposite lines. Then $p_1, \ldots, p_6$ lie on a conic iff q_1, q_2, q_3 lie on a line.



To prove this, we consider the cubic curves $C = \overline{p_1p_2} \cup \overline{p_3p_4} \cup \overline{p_5p_6}$ and $H = \overline{p_2p_3} \cup \overline{p_4p_5} \cup \overline{p_6p_1}$, which intersect in $\{p_1, \ldots, p_6\} \cup \{q_1, q_2, q_3\}$.
The statement for hexagons with vertices on a reducible conic is known as Pappus' Theorem.

5.6 Cubic Curves

Let $C = \mathrm{V}(f) \subset \mathbb{P}^2$ be an absolutely irreducible cubic. Given two points $p, q \in C$, we can construct another point on C as the third intersection point of the line $\overline{p,q}$ with C. We denote this point momentarily by $\neg(p \vee q)$. Similarly for a single smooth point $p \in C$, the third intersection point of the projective tangent line $T_pC \subset \mathbb{P}^2$ with C gives another point, momentarily called $\neg(p \vee p)$. With this secant-tangent construction, we can give C the structure of an abelian group as follows:

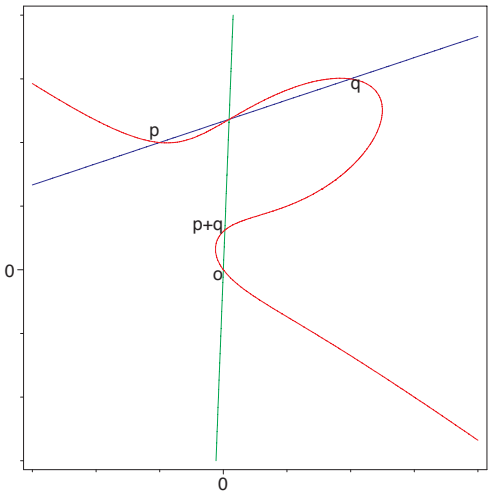
Fix a smooth point $o \in C$, which will serve as the "zero" element in the group. The group law is defined as

$$p + q := \neg((\neg(p \vee q)) \vee o),$$

that is the third intersection point of C with the line $\overline{\neg(p \vee q), o}$. We illustrate the group law on the curve given by the affine equation

$$11x^3 - 4xy^2 + 23y^3 - 6x^2 - 32xy - 67y^2 + 43x + 32y = 0$$

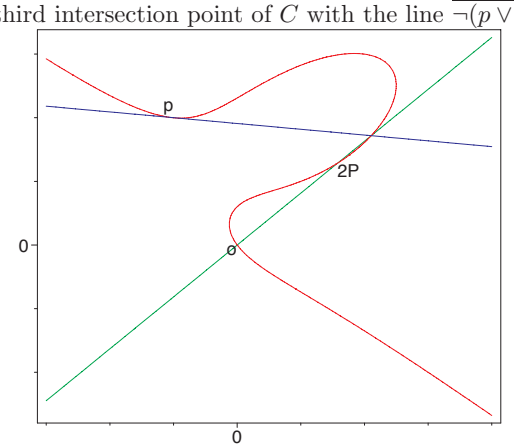
and points o, p, q with affine integral coordinates.



Similarly, replacing the secant by the tangent, we define

$$2p := \neg((\neg(p \vee p)) \vee o),$$

that is the third intersection point of C with the line $\overline{\neg(p \vee p), o}$.

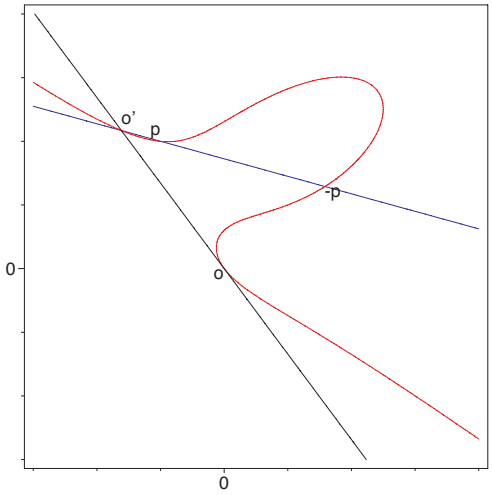


Theorem 5.6.1. *Let $\Bbbk$ be a not necessarily algebraically closed field. Let C be an absolutely irreducible cubic, let $C^0 = C \setminus Sing\, C$ denote the set of non-singular points, and let $o \in C^0$ be a fixed point. The binary operation*

$$C^0 \times C^0 \to C^0,\ (p, q) \mapsto p + q$$

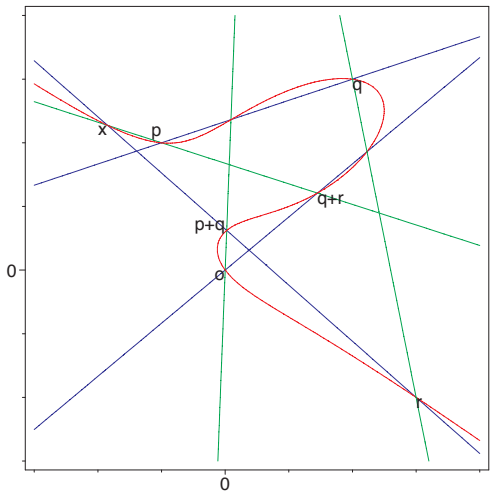
defined above, gives C^0 the structure of an abelian group with $o \in C$ as zero element. If $o \in C(\Bbbk)$ then $C^0(\Bbbk) \subset C^0$ forms a subgroup.

Proof. All is clear except the associativity law. For example, the statement about the subgroup follows, because a cubic polynomial in one variable with two $\Bbbk$-rational roots has all three roots $\Bbbk$-rational. For the negative of a point $p \in C^0$, we consider the third intersection o' of C with $T_o C$. Then $-p$ is the third intersection of C with $\overline{o', p}$.



Note that we get only smooth points, because a secant or tangent through smooth points cannot intersect C in a singular point by Bézout's Theorem and Proposition 4.3.18.3.

To prove $(p + q) + r = p + (q + r)$, we consider all lines involved in the construction. We have to prove that the lines $\overline{p + q, r}$ and $\overline{p, q + r}$ intersect in a point of C.



For this we consider the cubics C and $\overline{p,q} \cup \overline{p+q,r} \cup \overline{o,q+r}$, which intersect in the nine points

$$p, q, \neg(p \vee q), p+q, r, x = \neg((p+q) \vee r), o, q+r, \text{ and } \neg(q \vee r),$$

which we assume to be different. Out of these, the following six $q, r, \neg(q \vee r), o, p+q, \neg(p \vee q)$ lie on the quadric $\overline{q,r} \cup \overline{o,q+q}$. Thus, the remaining three $p, q+r, \neg((p+q) \vee r)$ lie on the line $\overline{p,q+r}$ by Corollary 5.5.3, and the points

$$\neg((p+q) \vee r) \text{ and } \neg(p \vee (q+r))$$

coincide. To prove $2p+q = p+(p+q)$ or other cases, where some of the points coincide, we argue with continuity. So far, we have proved that $\neg((p+q) \vee r) = \neg(p \vee (q+r))$ holds for an non-empty Zariski open subset of triples $(p,q,r) \in C^0 \times C^0 \times C^0$. We will define the Zariski toplogy on $C \times C \times C$ in Chapter 6 precisely. It is clear, that iff some of the points in the construction come together, some secant lines might become tangent lines, and that some lines might coincide as well. The condition $\neg((p+q) \vee r) = \neg(p \vee (q+r))$ is an algebraic condition on the irreducible algebraic set $C^0 \times C^0 \times C^0$. Since it holds on a non-empty Zariski open subset, it holds everywhere. □

The negative in the group law becomes particularly simple, if we can choose a flex as the origin o. In that case o and o' coincide, and $-p$ is the third intersection of $\overline{o,p}$ with C.

Definition 5.6.2. *Let $p \in C \subset \mathbb{P}^2$ be a smooth point on a curve. The point $p \in C$ is a* **flex** *of C, if $i(T_pC, C; p) \geq 3$. The multiplicity of the flex is $i(T_pC, C; p) - 2$.*

Thus, every point on a line is a flex. A smooth conic has no flexes at all by Bézout's Theorem.

To determine the flexes of a curve $C(f)$ defined by a square-free polynomial $f \in \Bbbk[x,y,z]$, we consider the **Hessian** and the Hessian matrix. We abbreviate $f_x = \frac{\partial f}{\partial x}$ and so on. Then

$$Hess(f) = \det \begin{pmatrix} f_{xx} & f_{xy} & f_{xz} \\ f_{xy} & f_{yy} & f_{yz} \\ f_{xz} & f_{yz} & f_{zz} \end{pmatrix}.$$

Note, that the Hessian curve $H = \mathrm{V}(Hess(f))$ is independent of the choice of the coordinate system, because a change coordinates $(x,y,z)^t = A(u,v,w)^t$ amounts to the multiplication with the matrices A^t and A.

Proposition 5.6.3. *Assume* $\operatorname{char}\Bbbk = 0$ *and that* $f \in \Bbbk[x,y,z]$ *is square-free. Then* $C = \mathrm{V}(f)$ *and* $H = \mathrm{V}(Hess(f))$ *intersect in the singular points of* C *and in the flexes. More precisely,*

$$i(C, T_pC; p) - 2 = i(C, H; p)$$

for smooth points of $p \in C$*.*

Proof. We may assume that $d = \deg C \geq 2$. That H and C intersect in singular points of C follows with the **Euler relation:**

$$xg_x + yg_y + zg_z = \deg g \cdot g,$$

for g **homogeneous. Thus**

$$(d-1)\begin{pmatrix} f_x \\ f_y \\ f_z \end{pmatrix} = \begin{pmatrix} f_{xx} & f_{xy} & f_{xz} \\ f_{xy} & f_{yy} & f_{yz} \\ f_{xz} & f_{yz} & f_{zz} \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

Since f_x, f_y, f_z **vanish at singular points of** C**, we conclude that at a singular point** $[\alpha:\beta:\gamma]$ **of** C **the Hessian matrix has a nonzero kernel, hence determinant zero. For a smooth point** $p \in C$**, we consider appropriate coordinates. Suppose** $p = [0:0:1]$ **and** $T_pC = \mathrm{V}(y)$**. Then the affine equation of** C **is of the form**

$$f(x,y,1) = yu(x,y) + x^k g(x) \text{ with } k \geq 2$$

with $u(0,0) \neq 0$, $g(0) \neq 0$**. Homogenization gives**

$$f(x,y,z) = yu(x,y,z) + x^k g(x,z)$$

for suitable homogeneous polynomials u, g **with** $u(0,0,1), u_z(0,0,1)$ **and** $g(0,1) \neq 0$**. We evaluate the vanishing order** $v_p(Hess(f))$ **at** p **on** C**. Since** $v_p(y) = k$ **and** $v_p(x) = 1$**, we find that** $v_p(f_{xx}) = v_p(yu_{xx} + k(k-1)x^{k-2}g + 2kx^{k-1}g_x + x^k g_{xx}) = k-2$ **and** $v_p(f_{yz}) = v_p(u_z) = 0$**. It follows that**

$$i(C,H;p) = v_p(Hess(f)) = v_p(-f_{xx}f_{yz}^2) = k-2 = i(C,T_pC;p)-2,$$

since all other terms in the Laplace expansion of the Hessian have higher vanishing order. □

Corollary 5.6.4. *Let* $\operatorname{char}\Bbbk = 0$. *A smooth curve* C *of degree* d *has* $3d(d-2)$ *flexes counted with multiplicity.*

Proof. The degree of the Hessian is 3(d-2). □

Exercise 5.6.5. Suppose $\operatorname{char}\Bbbk = 0$. Let $C \subset \mathbb{P}^2$ be a curve with singularities. Prove:

1. $i(C, Hess(C), p) = 6$, for $p \in C$ an ordinary node,
2. $i(C, Hess(C), p) = 8$, for $p \in C$ an ordinary cusp.

Conclude that a curve with δ ordinary nodes and κ ordinary cusps as its only singularities has

$$f = 3d(d-2) - 6\delta - 8\kappa$$

flexes counted with multiplicities. □

A smooth cubic curve can have only simple flexes by Bézout. Analysing in the proof the assumption $\operatorname{char}\Bbbk = 0$, we find for cubic curves

Corollary 5.6.6. *If* $\operatorname{char}\Bbbk \neq 2,3$ *then a smooth cubic curve has precisely 9 flexes.*

Corollary 5.6.7. *Suppose that* $\operatorname{char}\Bbbk \neq 2,3$. *Then, after a change of coordinates, any smooth cubic curve* $C \subset \mathbb{P}^2$ *can be defined by an equation*

$$y^2z = x^3 + axz^2 + bz^3$$

with coefficients a, b. *Conversely, the cubic defined by such an equation is smooth iff the disriminant* $27a^3 + 4b^2 \neq 0$.

Proof. We may change coordinates such, that $o = [0:1:0]$ is a flex, and that $T_oC = \mathrm{V}(z)$. Then the affine equation of C has shape

$$a_0'y^2 + a_1'xy + a_2' = x^3 + b_1'x^2 + b_2'x^2 + b_3'$$

Taking a_0' into z, we arrive at

$$y^2 + a_1xy + a_2y = x^3 + b_1x^2 + b_2x + b_3.$$

Finally, substituting first $y = y - a_1/2x - a_2/2$ and then $x = x - b_1''/3$, we arrive at

$$y^2 = x^3 + ax + b.$$

The curve defined by such an equation is singular iff x^3+ax+b has a multiple root iff $27a^3 + 4b^2 = 0$. Note that this change of coordinates is defined over the ground field iff the flex is a $\Bbbk$-rational point. □

Definition 5.6.8. *An* **elliptic curve in Weierstrass normal form** *is a smooth cubic curve E defined by an affine* **Weierstrass equation**

$$y^2 + a_1xy + a_2y = x^3 + b_1x^2 + b_2x + b_3.$$

The curve E carries a group structure with the single intersection point $o = [0:1:0]$ of E and the line at infinity as Null in the group. If $\operatorname{char}\Bbbk \neq 2, 3$ *then the equation can be simplified to*

$$y^2 = x^3 + ax + b.$$

The main difference between a smooth cubic and an elliptic curve is, that an elliptic curve has a $\Bbbk$-rational point over its field of definition. We will see in Chapter 8, that indeed any smooth cubic curve C with a $\Bbbk$-rational point is isomorphic to a cubic in Weierstrass normal form. However, in general the isomorphism is not induced by a linear automorphism of $\mathbb{P}^2$.

Exercise 5.6.9. Suppose that $\operatorname{char}\Bbbk \neq 2, 3$. Prove that the secant line through two flexes of an irreducible cubic curve intersects the curve in a further flex. *Hint:* Choose one of the flexes as the Null in the group, and consider the 3-torsion elements of the group. □

Exercise 5.6.10. Proove that the incidence correspondence between flexes and secant lines joining them, coincides with the incidence configuration of $\mathbb{F}_3$-rational points and lines in $\mathbb{A}^2(\mathbb{F}_3)$. □

Exercise 5.6.11. Prove that for an irreducible cubic defined over $\mathbb{R}$, at most three of the flexes can be real. □

Exercise 5.6.12. Let $C = \mathrm{V}(f)$ be a cubic defined by an affine Weierstrass equation

$$y^2 = x^3 + ax + b.$$

Choose as Null the single intersection point $o = [0:1:0]$ of C with the line at infinity. Prove the following formulas for the group law on C^0:

1. $-(x, y) = (x, -y)$
2. $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ with

$$x_3 = (\frac{y_2 - y_1}{x_2 - x_1})^2 - x_1 - x_2 \text{ and } y_3 = (\frac{y_2 - y_1}{x_2 - x_1})(x_3 - x_1) + y_1$$

3. $2(x_1, y_1) = (x_3, y_3)$ with

$$x_3 = (\frac{3x_1 + a}{2y_1})^2 - 2x_1 \text{ and } y_3 = (\frac{3x_1 + a}{2y_1})(x_3 - x_1) + y_1$$

□

Exercise 5.6.13. Let C be the projective closure of $\mathrm{V}(y^2 - x^3)$ and the Null $o \in C$ as in Exercise 5.6.12. Prove that

$$C^0(\Bbbk) \cong (\Bbbk, +).$$

Let C be the projective closure of $\mathrm{V}(y^2 - x^3 - x^2)$ and the Null $o \in C$ as in Exercise 5.6.12. Prove that

$$C^0(\Bbbk) \cong (\Bbbk^*, *).$$

□

Remark 5.6.14. Elliptic curves E defined over the finite field $\mathbb{F}_q$ with q elements recently found applications in cryptography, see Koblitz [1994]. Choosing an elliptic curve over $\mathbb{F}_q$ at random, is like choosing a random abelian group of size $\approx q + 1$ by the famous Hasse-Weil Theorem. Let $\sharp E(\mathbb{F}_q)$ denote the number of $\mathbb{F}_q$-rational points.

Theorem 5.6.15 (Hasse-Weil Theorem). *Let E be a smooth elliptic curve defined over $\mathbb{F}_q$. Then the number of $\mathbb{F}_q$-rational points is estimated by*

$$|\sharp E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}.$$

We will prove a more general formula for arbitrary smooth curves in Chapter 8, Theorem 8.8.24. A plausibility argument runs as follows: $E(\mathbb{F}_q)$ contains the point o at infinity. All other points project onto a point of $\mathbb{A}^1(\mathbb{F}_q) \subset \mathbb{P}^1(\mathbb{F}_q)$. There are q points in $\mathbb{A}^1(\mathbb{F}_q)$. Over the possible three roots α of $x^3 + ax + b$ in $\mathbb{A}^1(\mathbb{F}_q)$ we have precisely one point $[\alpha : 0 : 1]$ in $E(\mathbb{F}_q)$. Over the other points $\alpha \in \mathbb{A}^1(\mathbb{F}_q)$, we find either two or no point depending on whether $\alpha^3 + a\alpha + b \in (\mathbb{F}_q^*)^2$ or not. If we assume that the map

$$D(x^3 + ax + b)(\mathbb{F}_q) \to \mathbb{F}_q^*/(\mathbb{F}_q^*)^2,\ \alpha \mapsto \alpha^3 + a\alpha + b$$

behaves like a random function then we can model $\sharp E(\mathbb{F}_q) - q - 1$ with a random path with steps ± 1 of length q. Then the expectation value of $\sharp E(\mathbb{F}_q)$ is $q + 1$ and the expectation value of $|\sharp E(\mathbb{F}_q) - q - 1|$ is $\approx \sqrt{q}$.

A much more precise statemant about the distribution of the orders $\sharp E(\mathbb{F}_q)$ of elliptic curves over $\mathbb{F}_q$, when E runs through the finite set of elliptic curves over $\mathbb{F}_q$, can be found in [Gekeler, 2003].

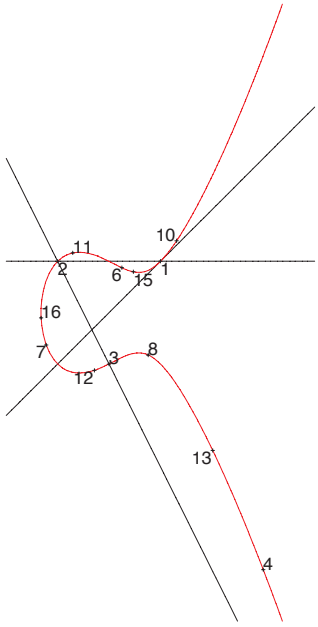
A different application of elliptic curves over finite fields due to Lenstra and Lenstra concerns integer factorization and primality tests, see **?** and **?**.

Elliptic curves over number fields are an intense area of current research. To start, we have Mordell's Theorem:

Theorem 5.6.16 (Mordell, 1922). *Let E be an elliptic curve defined over $\mathbb{Q}$. Then $E(\mathbb{Q})$ is a finitely generated group.*

Thus, every $\mathbb{Q}$-rational point on E can be constructed via the tangent-secant construction from finitely many points. For a proof we refer to Silverman [1986].

Example 5.6.17. The point $p = (1, 1)$ on the elliptic curve E defined by $y^2 = x^3 - x + 1$ generates an infinite subgroup of $E(\mathbb{Q})$.



The torsion part of $E(\mathbb{Q})$ was clarified by the celebrated Theorem of Mazur.

Theorem 5.6.18 (Mazur, 1976). *Let E be an elliptic curve over $\mathbb{Q}$. Then $E(\mathbb{Q})_{tors}$ is one of the following groups*

$$\mathbb{Z}/n \text{ with } 1 \leq n \leq 10 \text{ or } n = 12$$

or

$$\mathbb{Z}/2 \times \mathbb{Z}/2n \text{ with } 1 \leq n \leq 4.$$

On the other hand, the rank of $E(\mathbb{Q})$ is the topic of one of most famous conjectures in Mathematics. Let $E(\mathbb{Q})$ be a smooth elliptic curve with defining equation in $\mathbb{Z}[x, y]$. Then for almost all prime numbers p, we obtain a smooth cubic curve $E \mod p$ over the finite field $\mathbb{F}_p = \mathbb{Z}/p$. Write its number of points in the form

$$E(\mathbb{F}_p) = 1 - a_p + p.$$

A more precise version of the Hasse-Weil Theorem (Theorem 8.8.25) says that the reciprocal roots $\alpha, \overline{\alpha}$ of

$$1 - a_p t + pt^2 = (1 - \alpha t)(1 - \overline{\alpha} t)$$

are integral algebraic numbers of absolute value $|\alpha| = \sqrt{p}$.

We collect the local information of $E \mod \mathbb{F}_p$ with an Euler product to an analytic function: The **Hasse-Weil L-function** of E is defined by

$$L(E/\mathbb{Q}; s) = \frac{\zeta(s)\zeta(1-s)}{\prod_p (1 - a_p p^{-s} + p^{1-2s})}$$

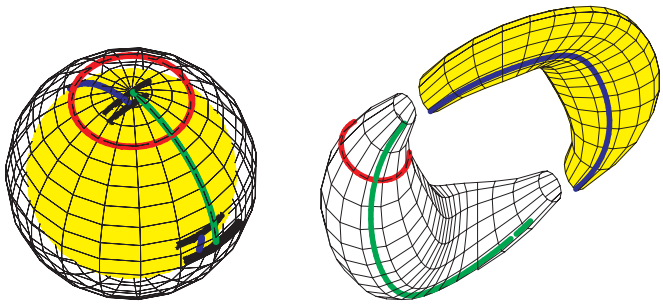
where $\zeta(s) = \prod_p (1 - p^{-s})^{-1} = \sum_n n^{-s}$ denotes the Riemann zeta function. The product of the denominators of $L(E/\mathbb{Q}, s)$ converges to an holomorphic function of s for s with real part $Re\, s > 1$. As the Riemann zeta function, the function $L(E/\mathbb{Q}, s)$ should have an analytic continuation.

Conjecture 5.6.19 (Birch and Swinnerton-Dyer, 1963, 1965). The Hasse-Weil L-function has an analytic continuation to the whole complex plane, and $\operatorname{rank} E(\mathbb{Q})$ equals the vanishing order of $L(E/\mathbb{Q}, s)$ at the critical point $s = 1$.

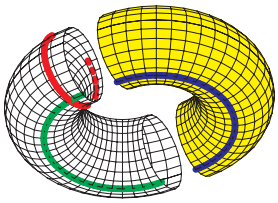
They also conjecture a precise statement about the leading coefficient. For reading on this fascinating topic in number theory we recommend Silverman [1986] or Husemöller [1986].

We now turn to the complex analytic side of the story about elliptic curves. One way to think about the elliptic curve $E \subset \mathbb{P}^2(\mathbb{C})$ defined by $y^2 = x^3 + ax + b$ over $\mathbb{C}$ is as the Riemann surface of the 2-valued analytic function $\sqrt{x^3 + ax + a}$. This amount to study E via the projection from $o = [0 : 1 : 0]$. The image of o will be the point at infinity $\infty = [1 : 0] \in \mathrm{V}(y) \cong \mathbb{P}^1$. Moreover, this is a ramification point, because o is a flex. The other ramification points lie on the line $\mathrm{V}(y)$. The three roots ρ_1, ρ_2, ρ_3 of $x^3 + ax + a$ give us three further ramification points $p_j = [\rho_j : 0 : 1] \in E$.

We can make $\sqrt{x^3 + ax + a}$ to a single valued function, if we restrict the domain of definition appropriately. Consider the line segment S_1 joining p_1 and p_2 and a half-line S_2, disjoint from S_1, which connects p_3 with ∞ on the Riemann number sphere $\mathbb{P}^1(\mathbb{C})$. Then $\sqrt{x^3 + ax + a}$ is single valued on $\mathbb{P}^1(\mathbb{C}) \setminus (S_1 \cup S_2)$, and the Riemann surface E is obtained by gluing two copies of $\mathbb{P}^1(\mathbb{C}) \setminus (S_1 \cup S_2)$ crosswise along the cuts.



It is easier to understand the Euclidean topology globally, if we draw the spheres not in each other and deform them a little bit. Note that the angle of two arcs ending at one of the branch point get divided by 2. Thus the angle of 360^o of the cut gives an angle of 180^o and thus a smooth arc. We conclude that the Riemann surface E is homeomorphic to a torus.



The universal covering space $\widetilde{E}$ of E is $\mathbb{C}$ as Riemann surface and

$$E = \mathbb{C}/\Lambda,$$

where $\Lambda \subset \mathbb{C}$ is a lattice. We see the group structure on E very clearly from this: $(E, +)$ is the quotiont group of $(\mathbb{C}, +)$ by the subgroup $(\Lambda, +)$. To prove $\widetilde{E} \cong \mathbb{C}$, one considers the elliptic integral

$$\int \frac{dx}{\sqrt{x^3 + ax + b}}.$$

$$\omega = \frac{dx}{\sqrt{x^3 + ax + b}} = \frac{dx}{y} = \frac{2dy}{\sqrt{3x^2 + a}}$$

is a nowhere vanishing holomorphic 1-form, because $y = \sqrt{x^3 + ax + b}$ and $x^3 + ax + b$ has no multiple roots. Thus we can define the integral

$$\int_o^p \frac{dx}{\sqrt{x^3 + ax + b}}$$

by choosing an arbitrary path from o to p, and the result is well defined up to a period, that is the integral of ω along a closed path. The first homology

group $H_1(E,\mathbb{Z})$ has as basis represented by the red and blue/green paths γ_1, γ_2 indicated above.

One can prove that the periods

$$\lambda_j = \int_{\gamma_j} \omega$$

are $\mathbb{R}$-linearly independent. Thus $\Lambda = \mathbb{Z}\lambda_1 \oplus \mathbb{Z}\lambda_2$ is a lattice, and integration defines an unramified holomorphic map

$$\int_o : E \to \mathbb{C}/\Lambda,\ p \mapsto \int_o^p \omega \mod \Lambda$$

The inverse is given by the Weierstraß $\wp$-function and its derivative. Recall from the theory of complex function in one variable that

$$\wp(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}$$

defines a meromorphic function with poles of order 2 at the lattice points. Moreover, the $\wp$-function and its derivative

$$\wp'(z) = \sum_{\lambda \in \Lambda} \frac{1}{(z-\lambda)^3}$$

are double periodic and satisfy the functional equation

$$(\wp')^2 = 4\wp^3 + g_2\wp + g_3$$

with $g_2 = \frac{1}{60}\sum'_{\lambda\in\Lambda} \frac{1}{\lambda^4}$ and $g_3 = \frac{1}{140}\sum'_{\lambda\in\Lambda} \frac{1}{\lambda^6}$. The inverse of $\int_o : E \to \mathbb{C}/\Lambda$ is given by

$$\mathbb{C}/\Lambda \to E \subset \mathbb{P}^2,\ z \mapsto [\wp(z) : \wp'(z)/2 : 1]$$

In particular, we claim that $a = g_2/4$ and $b = g_3/4$ holds. We do not prove this fact, but refer to Silverman [1986] and Husemoeller [1986] for further reading.

Chapter 6

Projective Algebraic Sets and Morphisms

In this Chapter we study arbitrary subvarieties of $\mathbb{P}^n$. In the first section we develop the algebra geometry dictionary for the projective setting and settle the question, how to compute the projective closure of arbitrary algebraic sets.

The second section is devoted to the definitions of products and morphisms. The main result of this section is the fundamtental theorem of elimination theory, which says that the image of an algebraic set under a projective morphism is an algebraic set. As consequence we get that regular functions on absolutely irreducible algebraic varieties are constant.

In Section 6.4 we introduce the Hilbert polynomial, which allows to define the degree of algebraic sets of higher codimension. Using the Hilbert polynomial we prove another version of Bézout's Theorem for the intersection of projective varieties of arbitrary codimension with hypersurface

In Section 6.5 we prove the dimension bound for intersections and the semi-continuity of the fiber dimension in a projective morphism. Section 6.6 deals with Bertini's Theorem and projective duality. An appendix contains the monodromy arguments for the uniform position of a general hyperplane section of curves and the irreducible of general hyperplane sections of higher dimensional varieties over fields of characteristic zero.

6.1 The Projective Nullstellensatz

In this section, we will explain how to link algebraic sets to ideals in the projective case. Since projective algebraic sets are defined by *homogeneous* polynomials, the ideals under consideration will have *homogeneous* generators. The general context for such ideals is that of graded rings.

Definition 6.1.1. A **graded ring** is a ring S with a decomposition $S = \bigoplus_{d\geq 0} S_d$ as Abelian groups such that $S_d S_e \subset S_{d+e}$ for all d, e. A **homogeneous element** of S is an element f of some graded piece S_d, and d is then called the **degree** of f. If $f = f_0 + f_1 + f_2 + \dots$ is the unique decomposition of an element $f \in S$ into homogeneous summands f_i of degree i, the f_i are called the **homogeneous components** of f. A **homogeneous ideal** of S is an ideal generated by homogeneous elements. □

If $S = \bigoplus_{d\geq 0} S_d$ is a graded ring, then S_0 is a ring with $1 \in S_0$, and S is an S_0-algebra. Furthermore, $S_+ := \bigoplus_{d\geq 1} S_d$ is a homogeneous ideal. In the case where $S_0 = \Bbbk$ is a field, this ideal is maximal and contains all other homogenous ideals of S.

Proposition 6.1.2. *Let I be an ideal of a graded ring $S = \bigoplus_{d\geq 0} S_d$. Then the following are equivalent:*

1. *I is homogeneous.*
2. *For each $f \in I$, the homogeneous components of f are in I as well:*

$$I = \bigoplus_{d\geq 0} (I \cap S_d)$$

Proof. 1 $\implies$ 2: Let $\{f^{(\lambda)}\}$ be a set of homogenous generators for I, with $d_\lambda := \deg f^{(\lambda)}$ for all λ. Moreover, let $f \in I$, and let $f_m \neq 0$ be the homogenous component of f of least degree. The result will follow by induction once we show that $f - f_m \in I$. For this, we write f as a sum $f = g^{(\lambda_1)} f^{(\lambda_1)} + \dots + g^{(\lambda_r)} f^{(\lambda_r)}$. Then, with the obvious notation, $f_m = g^{(\lambda_1)}_{m-d_{\lambda_1}} f^{(\lambda_1)} + \dots + g^{(\lambda_r)}_{m-d_{\lambda_r}} f^{(\lambda_r)} \in I$.

2 $\implies$ 1: If condition 2 is satisfied, the homogeneous components of the elements of any given set of generators for I generate I, too. □

Exercise* **6.1.3.** Let S be a graded ring.

1. Show that the sum, product, intersection, ideal quotient, and radical of homogeneous ideals are homogeneous.
2. Show that a homogeneous ideal $\mathfrak{p} \subset S$ is prime iff for any two *homogeneous* elements $f, g \in S$ with $fg \in \mathfrak{p}$ we must have $f \in \mathfrak{p}$ or $g \in \mathfrak{p}$. □

It is clear from the proof of Proposition 6.1.2 that every homogeneous ideal of a *Noetherian* graded ring is generated by *finitely many* homogeneous elements. The polynomial ring $\Bbbk[x_0, \dots, x_n]$ with its natural grading by the degree of polynomials is our basic example of a Noetherian graded ring.

Exercise* 6.1.4 (Characterization of Noetherian Graded Rings). Let $S = \bigoplus_{d\geq 0} S_d$ be a graded ring. Show that the following are equivalent:

1. S is Noetherian.
2. S_0 is Noetherian and S_+ is a finitely generated ideal.
3. S_0 is Noetherian and S is a finitely generated S_0-algebra. □

At this point, setting up an I–V-correspondence between algebraic subsets of $\mathbb{P}^n(\Bbbk)$ and homogeneous ideals of $\Bbbk[x_0.\ldots,x_n]$, the reader will have no difficulty in verifying results analogous to those proved in Chapter 1. In particular, each algebraic set $A \subset \mathbb{P}^n(\Bbbk)$ is defined by finitely many homogeneous polynomials; it has finitely many **irreducible components**; and, it is irreducible iff $\mathrm{I}(A)$ is a prime ideal. Moreover, the Zariski closure of the difference of two projective algebraic sets is obtained as in Theorem 1.9.1. For the sake of brevity, we will only treat the projective version of the Nullstellensatz in some detail. In doing so, we will use I and V in accordance with Convention 5.2.1:

Definition 6.1.5. 1. If $I \subset \Bbbk[x_0,\ldots,x_n]$ is a homogeneous ideal, its **locus of zeros** (or **vanishing locus**) in $\mathbb{P}^n$ is the projective algebraic set

$$\mathrm{V}(I) := \{p \in \mathbb{P}^n \mid f(p) = 0 \text{ for all homogeneous } f \in I\}.$$

2. Let $S := \mathbb{K}[x_0,\ldots,x_n]$. If $A \subset \mathbb{P}^n$ is any subset, its **vanishing ideal** is the homogeneous ideal

$$\mathrm{I}(A) := \langle f \in S \mid f \text{ is homogeneous and } f(p) = 0 \text{ for all } p \in A\rangle.$$ □

Remark 6.1.6. Note that

$$\mathrm{I}(A) = \{f \in S \mid f(a_0,\ldots,a_n) = 0 \text{ for any } p \in A \text{ and any set } a_0,\ldots,a_n \text{ of homogeneous coordinates for } p\}.$$

Indeed, if $f = f_m + \ldots + f_d$ is an element of the ideal on the right hand side, where the f_i are homogenous of degree i, and $p = [a_0 : \cdots : a_n] \in A$, then

$$0 = f(\lambda a_0,\ldots,\lambda a_n) = \lambda^m f_m(a_0,\ldots,a_n) + \cdots + \lambda^d f_d(a_0,\ldots,a_n)$$

for all $\lambda \in \mathbb{K}$. Since $\mathbb{K}$ is infinite, this is only possible iff $f_i(a_0,\ldots,a_n) = 0$ for all i. It follows that $f \in \mathrm{I}(A)$. The reverse inclusion is clear. □

Theorem 6.1.7 (Projective Nullstellensatz). *Let $I \subset \Bbbk[x_0,\ldots,x_n]$ be a homogeneous ideal. Then:*

1. $\mathrm{V}(I) = \emptyset \iff I \supset \langle x_0,\ldots,x_n\rangle^d$ *for some* $d \geq 1$.
2. If $\mathrm{V}(I)$ *is nonempty, then*

$$\mathrm{I}(\mathrm{V}(I)) = \mathrm{rad}\,(I\,\mathbb{K}[x_0,\ldots,x_n]).$$

Proof. The theorem follows by applying the affine version of the Nullstellensatz to the affine cone $C(\mathrm{V}(I))$:

1. We have
$$\mathrm{V}(I) = \emptyset \iff C(\mathrm{V}(I)) \subset \{0\} \iff \mathrm{rad}\,(I) \supset \langle x_0, \ldots, x_n \rangle.$$
2. If $\mathrm{V}(I)$ is nonempty, we have
$$f \in \mathrm{I}(\mathrm{V}(I)) \iff f \in \mathrm{I}(C(\mathrm{V}(I))) \iff f \in \mathrm{rad}\,(I\,\mathbb{K}[x_0, \ldots, x_n]).$$

□

Corollary 6.1.8. *There is an inclusion-reversing one-to-one correspondence*

$$\{\textit{algebraic subsets of } \mathbb{P}^n\} \underset{\mathrm{V}}{\overset{\mathrm{I}}{\rightleftarrows}} \left\{ \begin{array}{c} \textit{homogeneous radical ideals} \\ \textit{of } \mathbb{K}[x_0, \ldots, x_n] \\ \textit{not equal to } \langle x_0, \ldots, x_n \rangle \end{array} \right\}.$$

Under this correspondence, subvarieties of $\mathbb{P}^n$ correspond to homogeneous prime ideals of $\mathbb{K}[x_0, \ldots, x_n]$ not equal to $\langle x_0, \ldots, x_n \rangle$. □

Since the ideal $\mathbb{K}[x_0, \ldots, x_n]_+ = \langle x_0, \ldots, x_n \rangle$ is missing in this correspondence, it is often called the **irrelevant ideal**.

Definition 6.1.9. The **homogeneous coordinate ring** of an algebraic set $A \subset \mathbb{P}^n$ is the quotient ring

$$\mathbb{K}[A] = \mathbb{K}[x_0, \ldots, x_n]/\mathrm{I}(A).$$

□

In terms of affine algebraic sets, $\mathbb{K}[A]$ is the coordinate ring of the affine cone $C(A) \subset \mathbb{A}^{n+1}$. Note that $\mathbb{K}[A]$ has a natural grading. In fact, if $S = \bigoplus_{d \geq 0} S_d$ is any graded ring, and $I = \bigoplus_{d \geq 0} (I \cap S_d)$ is any homogeneous ideal of S, then

$$S/I = \bigoplus_{d \geq 0} S_d/(I \cap S_d).$$

The relationship between algebraic subsets of A and homogeneous ideals of $\mathbb{K}[A]$ is analogous to Exercise 1.11.7.

Remark 6.1.10 (Buchberger's Algorithm and Homogeneous Ideals). With respect to computational aspects, we note that Buchberger's algorithm applied to homogeneous polynomials yields Gröbner basis elements which are homogeneous, too. In particular, given any global monomial order on $S = \Bbbk[x_0, \ldots, x_n]$, the elements of the reduced Gröbner basis for a homogeneous ideal I of S are homogeneous. Hence, the computational recipes given in Chapter 2 are valid in the projective case as well. □

We finish this section by defining the dimension of a projective algebraic set. One way of doing this is to extend the affine notion of dimension via coordinate charts (alternative ways will be discussed in subsequent sections):

Definition 6.1.11. The **dimension** of an algebraic subset $A \subset \mathbb{P}^n$, written $\dim A$, is defined to be the number

$$\dim A = \max\{A \cap U_i \mid i = 0, \ldots, n\}.$$

□

We will use the words **codimension**, **equidimensional**, **curve**, and **surface** exactly as in the affine case. It follows from that case that $\dim A$ is the maximum dimension of the irreducible components of A, and that A is a hypersurface iff it is equidimensional of dimension $n-1$. In algebraic terms, we will see in Corollary 6.4.19 that if $A \subset \mathbb{P}^n$ is any projective algebraic set, then

$$\dim A = \dim C(A) - 1 = \dim \mathbb{K}[A] - 1.$$

6.2 Computing the Projective Closure

To describe the projective closure of an affine algebraic set in algebraic terms, we introduce the following notation: The **homogenization** of an ideal $I \subset \Bbbk[x_1, \ldots, x_n]$ with respect to an extra variable x_0 is the ideal

$$I^h = \langle f^h \mid f \in I \rangle \subset \Bbbk[x_0, \ldots, x_n].$$

Theorem 6.2.1. *Let $I \subset \Bbbk[x_1, \ldots, x_n]$ be an ideal, and let I^h be its homogenization with respect to x_0. Then $\mathrm{V}(I^h) \subset \mathbb{P}^n$ is the projective closure of the affine algebraic set $\mathrm{V}_a(I) \subset \mathbb{A}^n \cong U_0 \subset \mathbb{P}^n$.*

Proof. First, it is clear that $\mathrm{V}(I^h)$ is an algebraic subset of $\mathbb{P}^n$ which contains $\mathrm{V}_a(I)$. To show that $\mathrm{V}(I^h)$ is the smallest such set, let $B \subset \mathbb{P}^n$ be any algebraic set containing $\mathrm{V}_a(I)$, and let $F \in \mathrm{I}(B) \subset \mathbb{K}[x_0, \ldots, x_n]$ be any form. Then the dehomogenization $f = F(1, x_1, \ldots, x_n)$ is contained in $\mathrm{I}_a(\mathrm{V}_a(I))$ (with obvious notation). Hence, by the affine Nullstellensatz, $f^m \in \mathrm{rad}\,(I\,\mathbb{K}[x_1, \ldots, x_n])$ for some m. This shows

$$(f^h)^m = (f^m)^h \in (I\,\mathbb{K}[x_1, \ldots, x_n])^h = I^h\,\mathbb{K}[x_1, \ldots, x_n] \subset \mathrm{I}(\mathrm{V}(I^h)).$$

Since $F = x_0^s f^h$ for some $s \geq 0$, it follows that $F \in \mathrm{I}(\mathrm{V}(I^h))$, as desired. □

Exercise* 6.2.2. Let $A \subset \mathbb{A}^n \cong U_0$ be an affine algebraic set, and let $\overline{A}$ be its projective closure in $\mathbb{P}^n$. Show:

1. A is irreducible iff $\overline{A}$ is irreducible.
2. If $A = V_1 \cup \cdots \cup V_r$ is the decomposition into irreducible components, then $\overline{A} = \overline{V}_1 \cup \cdots \cup \overline{V}_r$ is the decomposition into irreducible components.

In particular, no irreducible component of $\overline{A}$ is contained in the hyperplane at infinity. □

With respect to computing I^h, we note that the naive approach of just homogenizing the given generators for I may lead to the wrong ideal:

Example 6.2.3. Consider the ideal $I = \langle y - x^2, z - x^3 \rangle \subset \Bbbk[x, y, z]$, which defines the twisted cubic curve C in $\mathbb{A}^3$. Homogenizing the generators, we get the ideal $J = \langle wy - x^2, w^2 z - x^3 \rangle \subset \Bbbk[w, x, y, z]$, which decomposes as

$$J = \langle x^2 - wy, xy - wz, y^2 - xz \rangle \cap \langle x^2 - yw, xw, w^2 \rangle.$$

This shows that the line $\mathrm{V}(w, x)$, which is contained in the hyperplane at infinity, is an irreducible component of $\mathrm{V}(J) \subset \mathbb{P}^3$. Hence, J cannot be the homogenization of I (of course, this can also be seen directly by specifaying an element of I^h not contained in J). The projective closure of C, which is called the **twisted cubic curve in projective 3-space** $\mathbb{P}^3$, is defined by the ideal

$$J : \langle w, x \rangle = \langle x^2 - wy, xy - wz, y^2 - xz \rangle.$$

Note that the generators for this ideal are obtained by homogenizing the elements of the (reduced) Gröbner basis for I with respect to $>_{\mathrm{drlex}}$. □

In general, we have:

Proposition 6.2.4. *Let $I \subset \Bbbk[x_1, \ldots, x_n]$ be an ideal. Pick a degree-compatible (global) monomial order $>$ on $\Bbbk[x_1, \ldots, x_n]$, and set*

$$x^\alpha x_0^d >_h x^\beta x_0^e \iff x^\alpha > x^\beta \text{ or } (x^\alpha = x^\beta \text{ and } d > e).$$

Then $>_h$ is a global monomial order on $\Bbbk[x_0, \ldots, x_n]$. Moreover, when homogenizing with respect to x_0, the following holds: If $f_1, \ldots, f_r$ form a Gröbner basis for I with respect to $>$, then the homogenized polynomials $f_1^h, \ldots, f_r^h$ form a Gröbner basis for the homogenized ideal I^h with respect to $>_h$.

Proof. That $>_h$ is a global monomial order is immediate from the definitions. For the second statement, note that if $f \in \Bbbk[x_1, \ldots, x_n]$ is any nonzero polynomial, then $\deg \mathbf{L}_>(f) = \deg f$ since $>$ is degree-compatible. Hence, $\mathbf{L}_>(f)$ remains unchanged when we homogenize. According to how we defined $>_h$, it follows that $\mathbf{L}_{>_h}(f^h) = \mathbf{L}_>(f)$.

We use this to show that $\mathbf{L}(I^h) \subset \langle f_1^h, \ldots, f_r^h \rangle$ (the reverse inclusion is clear). Let $F \in I^h$. Since I^h is a homogeneous ideal, any homogeneous component of F is contained in I^h, and we may suppose that F itself is homeogeneous. Writing F as a $\Bbbk[x_0, \ldots, x_n]$-linear combination of polynomials g_j^h, with all $g_j \in I$, we find that the dehomogenization $f = F(1, x_1, \ldots, x_n)$ is a $\Bbbk[x_1, \ldots, x_n]$-linear combination of the g_j. In particular, $f \in I$. On the other hand, since F is homogeneous, we have $F = x_0^s f$ for some $s \geq 0$. Hence,

$$\mathbf{L}_{>h}(F) = x_0^s \cdot \mathbf{L}_{>h}(f^h) = x_0^s \cdot \mathbf{L}_>(f).$$

Since $\mathbf{L}_>(f)$ is a multiple of one of the $\mathbf{L}_>(f_i)$ by assumption, we conclude that $\mathbf{L}_{>h}(F)$ is a multiple of $\mathbf{L}_>(f_i) = \mathbf{L}_{>_h}(f_i^h)$, as required. □

Exercise 6.2.5. Let $d \geq 2$, and consider the image C of the parametrization

$$\mathbb{A}^1 \to \mathbb{A}^d,\ t \mapsto (t, t^2, \ldots, t^d).$$

The projectice closure $\overline{C} \subset \mathbb{P}^d$ is known as the **rational normal curve** in $\mathbb{P}^d$. Note that for $d = 2, 3$, we get a nondegenerate conic respectively the twisted cubic curve. In general, show that $\mathrm{I}(\overline{C})$ is generated by $\binom{d}{2}$ quadrics, and that there is no set of generators with fewer elements. Note that for $d \geq 3$, the number of generators is strictly larger than the codimension $d-1$. □

6.3 Products and Morphisms

We have seen in Exercise 1.11.5 that the product $A \times B$ of two affine algebraic sets $A \subset \mathbb{A}^n$ and $B \subset \mathbb{A}^m$ is an algebraic subset of $\mathbb{A}^n \times \mathbb{A}^m = \mathbb{A}^{n+m}$. In the projective setting, it is initially not even clear that $\mathbb{P}^n \times \mathbb{P}^m$ can be viewed as an algebraic set. There is, however, a natural way of doing this. The basic idea is to embed $\mathbb{P}^n \times \mathbb{P}^m$ in some $\mathbb{P}^N$ such that the image is a projective variety which locally, in the coordinate charts of $\mathbb{P}^N$, is isomorphic to the product $\mathbb{A}^n \times \mathbb{A}^m$. To make this precise, we note that sending $([a_0 : \cdots : a_n], [b_0 : \cdots : b_m])$ to $[a_0b_0 : \cdots : a_0b_m : a_1b_0 : \cdots : a_nb_m]$ gives a well-defined map

$$\sigma_{m,n} : \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^N, \quad \text{where} \quad N = (n+1)(m+1) - 1$$

(the map does not depend on the choice of homogeneous coordinates a_i, b_j, and at least one of the a_ib_j is nonzero). In studying $\sigma_{m,n}$, we denote the homogeneous coordinates on $\mathbb{P}^n$, $\mathbb{P}^m$, and $\mathbb{P}^N$ by $\boldsymbol{x} = x_0, \ldots, x_n$, $\boldsymbol{y} = y_0, \ldots, y_m$, and $\boldsymbol{z} = z_{00}, \ldots, z_{0m}, z_{10}, \ldots, z_{nm}$. Moreover, we say that a polynomial of type

$$f = \sum_{|\alpha|=d,\, |\beta|=e} c_\alpha x^\alpha y^\beta \in \Bbbk[\boldsymbol{x}, \boldsymbol{y}]$$

is **bihomogeneous (in $\boldsymbol{x}$ and $\boldsymbol{y}$, of bidegree $(\boldsymbol{d}, \boldsymbol{e})$)**.

Proposition 6.3.1. *The map $\sigma_{m,n}$ is injective, and its image $\Sigma_{m,n}$ is a subvariety of $\mathbb{P}^N$. The vanishing ideal $\mathrm{I}(\Sigma_{m,n})$ is generated by the 2×2 minors of the $(n+1) \times (m+1)$ matrix of coordinates (z_{ij}). In terms of coordinate charts, we have*

$$U_i \times U_j \cong \Sigma_{m,n} \cap U_{ij}.$$

Proof. It is clear that the minors vanish on $\Sigma_{m,n}$:

$$\det \begin{pmatrix} x_{i_1}y_{j_1} & x_{i_1}y_{j_2} \\ x_{i_2}y_{j_1} & x_{i_2}y_{j_2} \end{pmatrix} = 0. \tag{6.1}$$

Hence, if $A \subset \mathbb{P}^N$ denotes the algebraic set defined by the minors, then $\Sigma_{m,n} \subset A$. To show equality, we first intersect with the coordinate chart U_{00}. If $r =$

$[1 : c_{01} : \cdots : c_{ij} : \ldots] \in A \cap U_{00}$ is a point, then $c_{ij} = c_{i0}c_{0j}$. Hence, $([1 : c_{10} : \ldots : c_{n0}], [1 : c_{01} : \ldots : c_{0m}])$ is the unique pair of points $(p, q) \in U_0 \times U_0$ such that $\sigma_{m,n}\big((p, q)\big) = r$. We conclude that $\sigma_{m,n}$ restricts to an isomorphism $U_0 \times U_0 \cong A \cap U_{00}$ of affine varieties. Since the corresponding statement holds for the other coordinate charts, we have $\Sigma_{m,n} = A$, as desired. At the same time, the argument shows that $\sigma_{m,n}$ is injective.

The proposition will follow once we show that the ideal $I \subset \mathbb{K}[\boldsymbol{z}]$ generated by the minors is prime. For this, we show that I coincides with the kernel of the ring homomorphism

$$\phi : \mathbb{K}[\boldsymbol{z}] \to \mathbb{K}[\boldsymbol{x}, \boldsymbol{y}],\ z_{ij} \mapsto x_i y_j.$$

It is clear from (6.1) that $I \subset \ker \phi$. For the reverse inclusion, we use a counting argument which actually gives that the minors form a Gröbner basis for $\ker \phi$.

On $\mathbb{K}[\boldsymbol{z}]$, consider a global monomial order $>$ refining the partial order on the variables defined as follows:

$$\begin{array}{ccccc} z_{00} & > & z_{01} & > \ldots > & z_{0m} \\ \vee & & \vee & & \vee \\ z_{10} & > & z_{11} & > \ldots > & z_{1m} \\ \vee & & \vee & & \vee \\ \vdots & & \vdots & & \vdots \\ \vee & & \vee & & \vee \\ z_{n0} & > & z_{n1} & > \ldots > & z_{nm} \end{array}.$$

Then

$$\mathbf{L}(\det \begin{pmatrix} z_{i_1 j_1} & z_{i_1 j_2} \\ z_{i_2 j_1} & z_{i_2 j_2} \end{pmatrix}) = -z_{i_1 j_2} z_{i_2 j_1}$$

whenever $i_1 < i_2$ and $j_1 < j_2$. Hence, if $f \in \mathbb{K}[\boldsymbol{z}]$ is any polynomial, division with remainder yields a representation

$$f = g + h,$$

where g is a $\mathbb{K}[\boldsymbol{z}]$-linear combination of the minors, and such that h is a $\mathbb{K}$-linear combination of monomials of type

$$z_{i_1 j_1} z_{i_2 j_2} \cdot \ldots \cdot z_{i_d j_d},\ \text{ where }\ i_1 \le i_2 \le \ldots \le i_d \ \text{ and }\ j_1 \le j_2 \le \ldots \le j_d.$$

Then $\phi(g) = 0$. Since ϕ restricts to a bijection between the set of ordered monomials of degree d as above and the set of bihomogeneos monomials in $\mathbb{K}[\boldsymbol{x}, \boldsymbol{y}]$ of bidegree (d, d), we conclude that $\phi(f) = 0$ iff $\phi(h) = 0$ iff $h = 0$. Hence, as claimed, the minors form a Gröbner basis for $\ker \phi$. In particular, $I = \ker \phi$. Moreover, I is a prime ideal since $\mathbb{K}[\boldsymbol{z}]/\ker \phi$ is isomorpic to a subring of the integral domain $\mathbb{K}[\boldsymbol{x}, \boldsymbol{y}]$. □

Being defined by by the 2×2 minors of the matrix (z_{ij}), the Segre variety $\Sigma_{m,n}$ is sometimes called an example of a **determinantal variety**.

Exercise 6.3.2. In the situation of the proof above, describe the syzygies on the 2×2 minors arising from Buchberger's test. □

Definition 6.3.3. The map $\sigma_{m,n}$ is called the **Segre embedding** of $\mathbb{P}^n \times \mathbb{P}^m$ into $\mathbb{P}^N$. Its image $\Sigma_{m,n}$ is called the **Segre variety**. We give $\mathbb{P}^n \times \mathbb{P}^m$ the **structure of a projective variety** by identifying it with $\Sigma_{m,n}$. □

Example 6.3.4. The Segre variety $\Sigma_{1,1}$ is the image of the map

$$\sigma_{1,1} : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3,\ ([a_0 : a_1], [b_0 : b_1]) \mapsto [a_0b_0 : a_0b_1 : a_1b_0 : a_1b_1].$$

It is a quadric defined by the equation $z_{00}z_{11} - z_{01}z_{10} = 0$. Note that the fibers of either projection of $\mathbb{P}^1 \times \mathbb{P}^1$ onto $\mathbb{P}^1$ form a pencil of lines on $\Sigma_{1,1}$ such two different lines in the same pencil do not meet, and such that two lines from different pencils intersect in one point.

□

Now that we have given $\mathbb{P}^n \times \mathbb{P}^m$ the structure of a projective algebraic set, we wish to describe its algebraic subsets. In terms of the Segre embedding, a subset $A \subset \mathbb{P}^n \times \mathbb{P}^m \cong \Sigma_{n,m} \subset \mathbb{P}^N$ is closed iff it is the vanishing locus of finitely many polynomials $f_k \in \mathbb{K}[\boldsymbol{z}]$, where each f_k is homogenous of some degree d_k. For a characterization just in terms of $\mathbb{P}^n \times \mathbb{P}^m$, substitute the x_iy_j for the z_{ij} in the f_k as in the proof of Proposition 6.3.1. The resulting polynomials are bihomogeneous in $\boldsymbol{x}$ and $\boldsymbol{y}$, of bidegrees (d_k, d_k), and their common vanishing locus in $\mathbb{P}^n \times \mathbb{P}^m$ is A. In fact, *every* bihomogeneous polynomial $f \in \mathbb{K}[\boldsymbol{x}, \boldsymbol{y}]$ has a well-defined vanishing locus $\mathrm{V}(f)$ in $\mathbb{P}^n \times \mathbb{P}^m$, and we have:

Proposition 6.3.5. *A subset of $\mathbb{P}^n \times \mathbb{P}^m$ is algebraic iff it is the common vanishing locus of finitely many bihomogeneous polynomials in $\boldsymbol{x}$ and $\boldsymbol{y}$.*

Proof. The implication from left to right is clear from the discusion above. For the converse implication, let $f \in \mathbb{K}[\boldsymbol{x}, \boldsymbol{y}]$ be any bihomogeneous polynomial of any bidegree (d, e). We show that $\mathrm{V}(f)$ is an algebraic subset of $\mathbb{P}^n \times \mathbb{P}^m$. This is obvious if $d = e$ since, then, we may rewrite f as a homogeneous polynomial in the x_iy_j and, thus, in the z_{ij}. If $d \neq e$, say $e < d$, we get $\binom{n+d-e}{n}$ bihomogeneous polynomials of bidegree (d, d) by multiplying f with each of the monomials in $\boldsymbol{y}$ of degree $d-e$. Since the common vanishing locus of these polynomials equals $\mathrm{V}(f)$, we are done. □

If $f \in \mathbb{K}[\boldsymbol{x}, \boldsymbol{y}]$ is a nonconstant polynomial of bidegree (d, e), then its vanishing locus $\mathrm{V}(f)$ in $\mathbb{P}^n \times \mathbb{P}^m$ is called a **hypersurface of bidegree (d, e)**.

Example 6.3.6. The equation $z_{00}z_{11} - z_{01}z_{10} = 0$ of the quadric $\Sigma_{1,1} \subset \mathbb{P}^3$ is one of the equations of the twisted cubic curve C in $\mathbb{P}^3$ which is, thus, contained in $\Sigma_{1,1}$. Taking the other two defining quadrics of C as in Example 6.2.3 and substituting, we get the bihomogeneous polynomials $x_0(x_0y_1^2 - x_1y_0^2)$ and $x_1(x_1y_0^2 - x_0y_1^2)$. Hence, $C \subset \mathbb{P}^1 \times \mathbb{P}^1$ is defined by the single equation $x_0y_1^2 - x_1y_0^2 = 0$. It is a hypersurface of bidegree (1,2). □

Given algebraic subsets $A \subset \mathbb{P}^n$ and $B \subset \mathbb{P}^m$, it is, now, clear that the product $A \times B \subset \mathbb{P}^n \times \mathbb{P}^m$ is an algebraic subset as well: If $A = \mathrm{V}(f_1, \ldots, f_r)$ and $B = \mathrm{V}(g_1, \ldots, g_s)$, with homogeneous f_k and g_ℓ, then the f_k and g_ℓ considered as bihomogeneous polynomials in $\boldsymbol{x}$ and $\boldsymbol{y}$ of bidegrees $(\deg f_k, 0)$ and $(0, \deg g_\ell)$ define $A \times B$. We call

$$\mathrm{I}(A \times B) = \langle f \in \mathbb{K}[\boldsymbol{x}, \boldsymbol{y}] \text{ bihomogeneous } \mid f(p) = 0 \text{ for all } p \in A \times B \rangle$$

the **bihomogenous ideal** and $\mathbb{K}[\boldsymbol{x}, \boldsymbol{y}]/\mathrm{I}(A \times B)$ the **bihomogeneous coordinate ring** of $A \times B$.

Exercise* **6.3.7.** In the situation above, show:

1. $\mathrm{I}(A \times B) = \big((\mathrm{I}(A)\,\mathbb{K}[\boldsymbol{x}, \boldsymbol{y}] + \mathrm{I}(B)\,\mathbb{K}[\boldsymbol{x}, \boldsymbol{y}]) : \langle \boldsymbol{x} \rangle^\infty\big) : \langle \boldsymbol{y} \rangle^\infty \subset \mathbb{K}[\boldsymbol{x}, \boldsymbol{y}]$.
2. The Zariski topology on $A \times B$ is not the product of the Zariski topologies on A and B, except when one of A and B is a finite set of points. □

Identifying $\mathbb{A}^m$ with the affine chart U_0 of $\mathbb{P}^m$, the product $\mathbb{P}^n \times \mathbb{A}^m$ inherits a Zariski topology from $\mathbb{P}^n \times \mathbb{P}^m$. With respect to this topology, a subset $A \subset \mathbb{P}^n \times \mathbb{A}^m$ is closed iff there are finitely many polynomials in $\mathbb{K}[x_0, \ldots, x_n, y_1, \ldots, y_m]$ which are homogeneous in $x_0, \ldots, x_n$, and such that their common vanishing locus is A. Here, any polynomial of type

$$f = \sum_{|\alpha|=d} x^\alpha h_\alpha(y_1, \ldots, y_m) \in \mathbb{K}[x_0, \ldots, x_n, y_1, \ldots, y_m],$$

with polynomials $h_\alpha(y_1, \ldots, y_m) \in \mathbb{K}[y_1, \ldots, y_m]$, is called **homogeneous in $\boldsymbol{x_0, \ldots, x_n}$ (of degree $\boldsymbol{d}$)**. Note that every such polynomial f has a well-defined vanishing locus $\mathrm{V}(f)$ in $\mathbb{P}^n \times \mathbb{A}^m$.

Our next objective is to define morphisms between projective algebraic sets. Among the maps introduced so far in the projective setting are the coordinate maps $\varphi_i : U_i \to \mathbb{A}^n$, the canonical projection $\mathbb{A}^{n+1} \setminus \{o\} \to \mathbb{P}^n$, and the projection maps $\mathbb{P}^n \setminus \{p\} \to \mathbb{P}^{n-1}$. To include these and other natural maps in our treatment of morphisms, we work with a class of sets which embraces the affine and projective algebraic sets, and all open subsets of these.

Definition 6.3.8. An open subset of an affine algebraic set is called a **quasi-affine algebraic set**. Similarly, we have the notion of a **quasi-projective algebraic set**. □

Remark 6.3.9. The product of two quasi-affine (quasi-projective) algebraic sets is quasi-affine (quasi-projective) as well:

$$(A_1 \setminus A_2) \times (B_1 \setminus B_2) = (A_1 \times B_1) \setminus ((A_1 \times B_2) \cup (A_2 \times B_1)) .$$ □

As in Section 1.11, our discussion of morphisms begins with the study of admissible functions. For quasi-affine algebraic sets, these have been introduced in Definition 4.2.25. Adapting this definition, we get well-defined functions in the quasi-projective case:

Remark-Definition 6.3.10. Let $A \subset \mathbb{P}^n$ be a quasi-projective algebraic set. A function $f : A \to \mathbb{K}$ is called **regular at a point** $p \in A$ if there are *homogeneous* polynomials $g, h \in \mathbb{K}[x_0, \ldots, x_n]$ *of the same degree* such that $h(p) \neq 0$ and f agrees with the function g/h on some open neighborhood of p in A. We say that f is **regular on** $\boldsymbol{A}$ if it is regular at every point of A. The set $\mathcal{O}(A)$ of all regular functions on A becomes a ring, with pointwise defined algebraic operations. □

The definition is natural in that locally, in the coordinate charts of $\mathbb{P}^n$, we get the notion already familiar to us:

Exercise 6.3.11. Let $f : A \to \mathbb{K}$ be a function on a quasi-projective algebraic set $A \subset \mathbb{P}^n$. Show that the following are equivalent:

1. f is regular.
2. If $\pi : \mathbb{A}^{n+1} \setminus \{o\} \to \mathbb{P}^n$ is the canonical projection, then $f \circ \pi : \pi^{-1}(A) \to \mathbb{K}$ is regular in the sense of Definition 4.2.25.
3. For each coordinate chart U_i, the composition $f \circ \varphi_i^{-1} : \varphi_i(A \cap U_i) \to \mathbb{K}$ is regular in the sense of Definition 4.2.25. □

We use the regular functions to define morphisms:

Definition 6.3.12. Let A be a quasi-affine or quasi-projective algebraic set.

1. Let $B \subset \mathbb{A}^m$ be a quasi-affine algebraic set. A map $\varphi : A \to B$ is called a **morphism** if it is given by a tuple of regular functions: There exist functions $f_1, \ldots, f_m \in \mathcal{O}(A)$ such that
$$\varphi(q) = (f_1(q), \ldots, f_m(q)) \text{ for all } q \in A.$$
2. Let $B \subset \mathbb{P}^m$ be a quasi-projective algebraic set. A map $\varphi : A \to B$ is called a **morphism** if it is *locally* given by a tuple of regular functions: For any $p \in A$, there exist an open neighborhood U of p in A and functions $f_0, \ldots, f_m \in \mathcal{O}(U)$ such that
$$\varphi(q) = [f_0(q) : \cdots : f_m(q)] \text{ for all } q \in U.$$ □

As we will see in Example 6.3.19 below, the neighborhood U and the f_j in part 2 of Definition 6.3.12 may well depend on the point p. That is, the functions giving φ may not exist *globally*.

Exercise* **6.3.13.** Let A and B be quasi-affine or quasi-projective algebraic sets, and let $\varphi : A \to B$ be a map. Show that φ is a morphism iff the following two conditions hold:

1. φ is continous.
2. For any open subset $U \subset B$ and any regular function f on U, the composition $f \circ \varphi$ is a regular function on the open subset $\varphi^{-1}(U) \subset A$. □

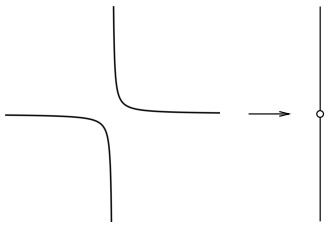
Clearly, the composition of two morphisms is a morphism. As usual, we have the notions of **isomorphism** and **isomorphic**. A morphism $\varphi : A \to B$ is said to be a **closed embedding** if $\varphi(A) \subset B$ is closed, and φ is an isomorphism of A onto $\varphi(A)$.

Example 6.3.14. 1. The canonical projection $\pi : \mathbb{A}^{n+1} \setminus \{o\} \to \mathbb{P}^n$ is a morphism.

2. The coordinate maps $\varphi_i : U_i \to \mathbb{A}^n$ are isomorphisms.

3. The Segre embedding $\sigma_{m,n}$ is a closed embedding.

4. Projecting onto the y-component, we get an isomorphism of the hyperbola $\mathrm{V}(xy-1) \subset \mathbb{A}^2$ with the punctured line $\mathbb{A}^1 \setminus \{0\}$.



Whereas the hyperbola is an affine algebraic set in the sense considered so far, the punctured line is not.

5. More generally, if $f \in \mathbb{K}[y_1, \ldots, y_m]$ is any polynomial, then $\mathrm{V}(xf-1) \subset \mathbb{A}^{m+1}$ and $\mathrm{D}(f) \subset \mathbb{A}^m$ are isomorphic. □

To make the notion of affine and quasi-affine algebraic sets invariant under isomorphisms, we alter our definitions. For this, note that if $A \subset \mathbb{A}^n$ is a quasi-affine algebraic set, then $\varphi_0^{-1}(A) \subset U_0 \subset \mathbb{P}^n$ is quasi-projective, and φ_0 restricts to an isomorphism $\varphi_0^{-1}(A) \to A$. We may, thus, regard A as a quasi-projective algebraic set.

Definition 6.3.15. An **affine algebraic set** is a quasi-projective algebraic set which is isomorphic to an algebraic subset of some affine space. A **quasi-affine algebraic set** is defined similarly. □

A quasi-projective algebraic set $A \subset \mathbb{P}^n$ which is isomorphic to an algebraic subset of some $\mathbb{P}^m$ is necessarily a closed subset of $\mathbb{P}^n$ and, thus, a projective algebraic set in the sense of Definition 5.1.3 (see Theorem 6.3.26 below).

Exercise 6.3.16. Show that $A = \mathbb{A}^2 \setminus \{(0,0)\}$ is a quasi-projective algebraic set which is neither projective nor affine.
Hint. To exclude that A is affine, compute the ring $\mathcal{O}(A)$. □

The definition of a morphism says what conditions we require, but not how to create meaningful examples. Here is one possibility for the latter:

Remark 6.3.17. Let $A \subset \mathbb{P}^n$ be a quasi-projective algebraic set. Suppose that $f_0, \ldots, f_m \in \mathbb{K}[x_0, \ldots, x_n]$ are forms of the same degree, and such that $A \cap \mathrm{V}(f_0, \ldots, f_m) = \emptyset$. Then we have a well-defined map

$$A \to \mathbb{P}^m,\ p \mapsto [f_0(p) : \cdots : f_m(p)],$$

where $[f_0(p) : \cdots : f_m(p)]$ is obtained by substituting the homogeneous coordinates of p for the x_i in the f_j. This map is a morphism: the open subsets $A \setminus \mathrm{V}(f_j)$ cover A, and on $A \setminus \mathrm{V}(f_j)$, the map is given by the tuple of regular functions $f_0/f_j, \ldots, f_m/f_j$. □

Projection from a point gives an example. More generally, we have:

Example 6.3.18. Let $y_0, \ldots, y_m \in \mathbb{K}[x_0, \ldots, x_n]$ be linearly independent linear forms, and let $L = \mathrm{V}(y_0, \ldots, y_m) \cong \mathbb{P}^{n-m-1}$ be the corresponding linear subspace of $\mathbb{P}^n$. Then the y_j define a morphism

$$\mathbb{P}^n \setminus L \to \mathbb{P}^m$$

which is called **projection from L to $\mathbb{P}^m$**. □

Example 6.3.19. Let $n, d \geq 1$, let $N = \binom{d+n}{n} - 1$, and let $m_0, \ldots, m_N$ be the monomials of degree d in $x_0, \ldots, x_n$ (listed in some order). Then the m_j define a morphism

$$\rho_{n,d} : \mathbb{P}^n \to \mathbb{P}^N$$

which is called the ***d*-uple embedding** (or **Veronese embedding**) of $\mathbb{P}^n$ into $\mathbb{P}^N$. □

If $n = 1$ and d is arbitrary, we get the map

$$\rho_{1,d} : \mathbb{P}^1 \to \mathbb{P}^d,\ [s : t] \mapsto [s^d : s^{d-1}t : \cdots : t^d],$$

whose image is the rational normal curve in $\mathbb{P}^d$ (see Exercise 6.2.5). Another special case is treated in the following example:

Example 6.3.20. If $n = d = 2$, we get the map

$$\rho_{2,2} : \mathbb{P}^2 \to \mathbb{P}^5,\ [a : b : c] \mapsto [a^2 : ab : b^2 : ac : bc : c^2].$$

Let V be the image of $\rho_{2,2}$, and let $w_0, \ldots, w_5$ be the homogeneous coordinates on $\mathbb{P}^5$. Consider the symmetric matrix

$$\Delta = \begin{pmatrix} w_0 & w_1 & w_3 \\ w_1 & w_2 & w_4 \\ w_3 & w_4 & w_5 \end{pmatrix}.$$

Clearly, the 2×2 minors of Δ vanish on V. That is, if $I \subset \mathbb{K}[w_0, \ldots, w_5]$ is the ideal generated by the minors, then $V \subset \mathrm{V}(I)$. We show that $V = \mathrm{V}(I)$, and that $\rho_{2,2}$ maps $\mathbb{P}^2$ isomorphically onto V. For this, we define a morphism $\varphi : \mathrm{V}(I) \to \mathbb{P}^2$ which, as the reader may easily check, is inverse to $\rho_{2,2}$. We consider a covering of $\mathrm{V}(I)$ by coordinate charts: $\mathrm{V}(I) \subset U_0 \cup U_2 \cup U_5$. On $\mathrm{V}(I) \cap U_0$, let φ be the map $p \mapsto [w_0(p) : w_1(p) : w_3(p)]$. On $\mathrm{V}(I) \cap U_2$ and $\mathrm{V}(I) \cap U_5$, define φ similarly by considering the second and third column of the matrix Δ. Since Δ has rank 1 one $\mathrm{V}(I)$, the respective local maps agree on the respective overlaps $U_i \cap U_j \cap \mathrm{V}(I)$, so that φ is well-defined. Note that φ is not a morphism of the type described in Example 6.3.17.

It turns out that I is in fact the vanishing ideal of V. To see this, we proceed as in the case of the Segre embedding, using a counting argument to show that I is prime ideal. This time, according to how we defined $\rho_{2,2}$, we consider the ring homomorphism

$$\phi : \mathbb{K}[w_0, \ldots, w_5] \to \mathbb{K}[x, y, z],\ w_0 \mapsto x^2, w_1 \mapsto xy, \ldots, w_5 \mapsto z^2,$$

whose kernel contains I. To show that $I = \ker \phi$, choose the degree reverse lexicographic order on $\mathbb{K}[w_0, \ldots, w_5]$, where the variables are ordered such that $w_1, w_3, w_4 > w_0, w_2, w_5$. Then the leading monomials of the minors are

$$w_1^2, w_1 w_3, w_3^2, w_1 w_4, w_3 w_4, w_4^2.$$

It follows that for each $d \geq 2$, there are precisely $3\binom{d+1}{2} + \binom{d+2}{2} = \binom{2d+2}{2}$ standard monomials of degree d. Hence, since the map

$$\mathbb{K}[w_0, \ldots, w_5]_d / I_d \to \mathbb{K}[x, y, z]_{2d}$$

induced by ϕ is surjective, it must be an isomorphism. Thus, as in the case of the Segre embedding, a polynomial $f \in \mathbb{K}[w_0, \ldots, w_5]$ is contained in $\ker \phi$ iff the remainder on division by the minors is zero. We conclude that the minors form a Gröbner basis for $\ker \phi$, and the result follows. □

The variety $V \subset \mathbb{P}^5$ in the example is known as the **Veronese surface**.

Exercise 6.3.21. Show that $\rho_{n,d}$ is a closed embedding for every n and d. Moreover, show that the vanishing ideal of the image is generated by quadrics which are binomials. How many quadrics do you get? □

In contrast to the affine case, the homogeneous coordinate ring of a projective algebraic set is not invariant under isomorphism:

Exercise 6.3.22. Let $A = \mathbb{P}^1$, and let $B \subset \mathbb{P}^2$ be the image of A under the 2-uple embedding. Then show that $S(A) \ncong S(B)$. □

Proposition 6.3.23. *Every quasi-projective algebraic set $A \subset \mathbb{P}^n$ has a finite open covering of affine algebraic sets.*

Proof. If $A = A_1 \setminus A_2$, where A_1 and $A_2 \subset A_1$ are closed subsets of $\mathbb{P}^n$, let $f_1, \ldots, f_r \in \mathbb{K}[x_0, \ldots, x_n]$ be forms such that $A_2 = \mathrm{V}(f_1, \ldots, f_r)$ (if $A_2 = \emptyset$, take the linear forms $x_0, \ldots, x_n$). Then $A = \bigcup_{i=1}^{r} \big(A_1 \setminus \mathrm{V}(f_i)\big)$. Hence, since $A_1 \setminus \mathrm{V}(f_i)$ is closed in $\mathbb{P}^n \setminus \mathrm{V}(f_i)$, it is enough to show that $\mathbb{P}^n \setminus \mathrm{V}(f)$ is an affine algebraic set for each form f. For this, we identify $\mathbb{P}^n$ with its image under the d-uple embedding of $\mathbb{P}^n$ into $\mathbb{P}^N$. Then $\mathrm{V}(f)$ is the intersection of $\mathbb{P}^n$ with a hyperplane H of $\mathbb{P}^N$. The result follows since $\mathbb{P}^n \setminus \mathrm{V}(f)$ is closed in $\mathbb{P}^N \setminus H \cong \mathbb{A}^N$. □

Remark 6.3.24. Let $A \subset \mathbb{P}^n$ be a quasi-projective algebraic set, and let

$$\phi = (f_{ij})$$

be a matrix of forms $f_{ij} \in \mathbb{K}[x_0 \ldots, x_n]$, $1 \leq i \leq \ell$, $0 \leq j \leq m$. For all i, suppose that $\deg f_{ij}$ depends only on i. In addition, suppose:

1. $A \cap \mathrm{V}(f_{ij} \mid 1 \leq i \leq \ell,\ 0 \leq j \leq m) = \emptyset$;
2. All 2×2 minors of ϕ vanish on A.

Given a point $p \in A$, choose an index i such that $p \notin \mathrm{V}(f_{i0}, \ldots, f_{im})$, and set $\varphi(p) = [f_{i0}(p) : \ldots : f_{im}(p)]$. Then

$$\varphi : A \to \mathbb{P}^m,\ p \mapsto \varphi(p),$$

is a well-defined morphism. □

Exercise 6.3.25. If $A \subset \mathbb{P}^n$ is a quasi-projective algebraic set, show that every morphism $A \to \mathbb{P}^m$ is given by a matrix as in Remark 6.3.24 above. □

Morphisms between affine algebraic sets are easier to describe, but morphisms between projective algebraic sets are better behaved. For instance, as we already know, the image of an affine algebraic set under a morphism needs not be closed. In fact, the image may not even be a quasi-projective algebraic set: As an example, consider the map $\varphi : \mathbb{A}^2 \to \mathbb{A}^2$ corresponding to the substitution homomorphism

$$\mathbb{K}[x, y] \to \mathbb{K}[u, v],\ x \mapsto u,\ y \mapsto uv,$$

whose image is

$$(\mathbb{A}^2 \setminus \mathrm{V}(x)) \cup \{(0, 0)\}.$$

For the image of a projective algebraic set, however, we have:

Theorem 6.3.26. *Let A be a projective algebraic set, and let $\varphi : A \to B$ be a morphism of quasi-projective algebraic sets. Then $\varphi(A) \subset B$ is closed.*

Proof. The theorem follows from Lemma 6.3.27 and Theorem 6.3.28 below. □

Lemma 6.3.27. *If $\varphi : A \to B$ is a morphism of quasi-projective algebraic sets, then the graph of φ is a closed subset of $A \times B$.*

Proof. Closedness is a local property. Hence, by Corollary 6.3.23, we may replace B by an open affine subset U of B, and A by an open affine subset of $\varphi^{-1}(U) \subset A$. That is, we may suppose that A respectively B are algebraic subsets of some $\mathbb{A}^n$ respectively $\mathbb{A}^m$. Then φ is a polynomial map $(\overline{f}_1, \ldots, \overline{f}_m)$, and its graph is defined by the ideal $\langle \overline{f}_1 - \overline{y}_1, \ldots, \overline{f}_m - \overline{y}_m \rangle \subset \mathbb{K}[A \times B]$. □

Theorem 6.3.28 (Fundamental Theorem of Elimination Theory). *Let A be a projective algebraic set, and let B be any quasi-projective algebraic set. Then the projection $A \times B \to B$ is a closed map.*

Proof. As in the previous proof, we may suppose that B is an algebraic subset of some $\mathbb{A}^m$. Hence, if $\mathbb{P}^n$ is the ambient space of A, then $A \times B \subset \mathbb{P}^n \times \mathbb{A}^m$ is a closed subset, and it suffices to consider the case where $A \times B = \mathbb{P}^n \times \mathbb{A}^m$.

So let $X \subset \mathbb{P}^n \times \mathbb{A}^m$ be any closed subset. Then X is the common vanishing locus of polynomials $f_1, \ldots, f_r \in \mathbb{K}[x_0, \ldots, x_n, y_1, \ldots, y_m]$, where each f_i is homogeneous in $x_0, \ldots, x_n$ of some degree d_i. By the projective Nullstellensatz, a point $q \in \mathbb{A}^m$ is in the image Y of X iff the ideal

$$I(q) := \langle f_1(\boldsymbol{x}, q), \ldots, f_r(\boldsymbol{x}, q) \rangle \subset \mathbb{K}[\boldsymbol{x}]$$

does not contain any of the ideals $\langle \boldsymbol{x} \rangle^d$, $d \geq 1$. Writing

$$Y_d = \{ q \in \mathbb{A}^m \mid I(q) \supsetneq \langle \boldsymbol{x} \rangle^d \},$$

we have $Y = \bigcap_d Y_d$, and it suffices to show that Y_d is closed for any given d.

To obtain equations for Y_d, multiply each f_i with any monomial in $\boldsymbol{x}$ of degree $d - d_i$, and write T_d for the resulting set of polynomials. Then $q \in Y_d$ iff each monomial in $\mathbb{K}[\boldsymbol{x}]_d$ is a $\mathbb{K}$-linear combination of the polynomials $f(\boldsymbol{x}, q)$, $f \in T_d$. That is, the $f(\boldsymbol{x}, q)$, $f \in T_d$, span $\mathbb{K}[\boldsymbol{x}]_d$. Arranging the coefficients of the monomials $m \in \mathbb{K}[\boldsymbol{x}]_d$ appearing in the polynomials $f \in T_d$ as a $\binom{d+n}{n} \times \sum_i \binom{d-d_i+n}{n}$ matrix ϕ_d with entries in $\mathbb{K}[\boldsymbol{y}]$, the condition is that $\operatorname{rank} \phi_d(q) < \binom{d+n}{n}$. That is, the $\binom{d+n}{n} \times \binom{d+n}{n}$ minors of ϕ_d define Y_d. □

Remark 6.3.29. Theorem 6.3.26 is reminiscent of the fact that the image of a compact topological space under a continous map to an Hausdorff space is compact. Note that such a map is proper (that is, it is closed, and each fiber is compact). In complex analysis, Remmert's proper mapping theorem states that the image of a proper holomorphic map $f : X \to Y$ of complex analytic spaces is an analytic subset of Y (see **?**).

In algebraic geometry, the usual notion of properness is not suitable since the Zariski topology is not Hausdorff. There is, however, a corresponding notion of properness: A morphism $A \to B$ of quasi-projective algebraic sets is called **proper** if it can be factored as the composite of a closed embedding

$A \to \mathbb{P}^n \times B$ with the projection $\mathbb{P}^n \times B \to B$ (if A is projective, this condition is automatically fulfilled). It is clear from the proof of the fundamental theorem of elimination theory that Theorem 6.3.26 can be generalized to the following statement: If $\varphi : A \to B$ is a proper morphism of quasi-projective algebraic sets, then $\varphi(A) \subset B$ is closed. Moreover, it is easy to show that over the complex numbers, a morphism is proper in the sense of algebraic geometry iff it is proper in the usual sense with respect to the Euclidean topology. □

Corollary 6.3.30. *Let A be a projective variety. Then every regular function on A is constant. More generally, every morphism from A to an affine algebraic set is constant.*

Proof. Let $f \in \mathcal{O}(A)$. Then f defines a morphism $A \to \mathbb{A}^1 \subset \mathbb{P}^1$. The image is a closed, proper subset of $\mathbb{P}^1$ and consists, thus, of finitely many points. Being irreducible, it consists of a single point. This proves the first statement of the corollary. Composing with coordinate functions, we get the second one. □

Remark 6.3.31. For $\mathbb{K} = \mathbb{C}$, the corollary can also be deduced from the maximum modulus principle. Indeed, a regular function f on A is holomorphic. Since A is compact in the Euclidian topology, the modulus $|f|$ achieves its maximum on A. Hence, f is constant on every connected component of A (with respect to the Euclidean topology). The corollary follows since A is path connected by Theorem 6.7.13 in Section 6.6 below. □

Corollary 6.3.32. *Let $\pi : \mathbb{P}^n \setminus \{p\} \to \mathbb{P}^{n-1}$ be projection from the point $p = [1 : 0 : \cdots : 0]$. Let $A \subset \mathbb{P}^n$ be a projective algebraic subset such that $p \notin A$. Then $A' := \pi(A) \subset \mathbb{P}^{n-1}$ is an algebraic subset of $\mathbb{P}^{n-1}$. Moreover, the inclusion of homogeneous coordinate rings*

$$\mathbb{K}[A'] = \mathbb{K}[x_1, \ldots, x_n]/\mathrm{I}(A') \longrightarrow \mathbb{K}[A] = \mathbb{K}[x_0, \ldots, x_n]/\mathrm{I}(A)$$

is an integral ring extension, and $\dim A = \dim A'$.

Proof. The first statement is clear. For the second statement, we note that $\mathbb{K}[A] = \mathbb{K}[A'][\overline{x}_0]$ is finite over $\mathbb{K}[A']$. Indeed, since $p \notin A$, the vanishing ideal $\mathrm{I}(A)$ contains a form f of some degree $d \geq 1$ which is monic in x_0:

$$f = x_0^d + c_1(x_1, \ldots, x_n)x_0^{d-1} + \ldots + c_d(x_1, \ldots, x_n).$$

This shows that $\mathbb{K}[A'] \subset \mathbb{K}[A]$ is integral. For the last statement, write V_i and U_i for the coordinate charts on $\mathbb{P}^{n-1}$ and $\mathbb{P}^n$, respectively. Then, for $i = 1, \ldots, n$, the inclusions of affine coordinate rings $\mathbb{K}[A' \cap V_i] \longrightarrow \mathbb{K}[A \cap U_i]$ are also finite: A polynomial in $\mathrm{I}(A \cap U_i)$ which is monic in x_0 is obtained by dehomogenizing f with respect to x_i. We conclude that $\dim A = \dim A'$. □

Corollary 6.3.33 (Projective Noether Normalization). *Let $A \subset \mathbb{P}^n$ be a projective algebraic set.*

1. *The dimension* $\dim A$ *is the least number* r *such that there is a linear subspace* $L \subset \mathbb{P}^n$ *of dimension* $n - r - 1$ *with* $A \cap L = \emptyset$.
2. *Let* $r = \dim A$*, and let* L *be any linear subspace as above. Then projection from* L *defines a morphism*

$$\pi : A \to \mathbb{P}^r$$

which is surjective and has finite fibers. Moreover, the map of homogeneous coordinate rings

$$\mathbb{K}[y_0, \ldots, y_r] \longrightarrow \mathbb{K}[A]$$

is a Noether normalization. In particular,

$$\dim A = \dim \mathbb{K}[A] - 1.$$

Proof. If $r = n$, then $A = \mathbb{P}^n$, and we are done. If $r < n$, there is a point $p \in \mathbb{P}^n \setminus A$. After a change of coordinates, we may suppose that $p = [1 : 0 : \cdots : 0]$. So the result follows from the preceeding Corollary by induction on $n - r$. □

Remark 6.3.34. A morphism $\varphi : A \to B$ of projective algebraic sets is called a **finite morphism** if for every point $q \in B$ there is an open affine neighborhood V of q in B such that $U := \varphi^{-1}(V)$ is affine, and the induced morphism $U \to V$ is finite in the sense of Chapter 3. We conclude from the proofs of the last two corollaries that the morphism $\pi : A \to \mathbb{P}^r$ above is finite. In the projective case, a morphism is finite iff it has finite fibers (see Harris (1992), Lemma 14.8). The example of the inclusion $\mathbb{A}^1 \setminus \{o\} \to \mathbb{A}^1$ shows that this is wrong in the affine case. □

Exercise 6.3.35. Show: The points corresponding to reducible polynomials $f = gh$ form an algebraic subset of $\mathbb{P}(\mathbb{K}[x_0, \ldots, x_n]_d)$. □

We finish this section by briefly treating Grassmanians. These are natural generalizations of projective spaces and provide important examples of projective varieties.

Definition 6.3.36. Given an n-dimensional vector space W over the field $\mathbb{K}$, the **Grassmannian** $\mathbb{G}(k, W)$ is the set

$$\mathbb{G}(k, W) = \big\{k\text{-dimensional linear subspaces of } W\big\}.$$

If $W = \mathbb{K}^n$, we write $\mathbb{G}(k, n)$ for $\mathbb{G}(k, W)$. □

Remark 6.3.37. Note that $\mathbb{G}(k, W)$ can also be thought of as the set of $(k-1)$-dimensional linear subspaces of the projective space $\mathbb{P}(W)$. □

To show that $\mathbb{G}(k, W)$ carries the structure of a projective variety, let $V \subset W$ be a k-dimensional linear subspace, and let $v_1, \ldots, v_k$ be a basis for V. Then $v_1 \wedge \cdots \wedge v_k$ is a nonzero vector of the exterior product $\bigwedge^k W$. This vector is determined by V up to scalar (choosing a different basis means to multiply

the vector by the determinant of the change of basis matrix). We, thus, obtain a well-defined map

$$\mathbb{G}(k, W) \to \mathbb{P}(\bigwedge^k W) \tag{6.2}$$

whose image is the set of points corresponding to the totally decomposable vectors of $\bigwedge^k W$. This map is injective: if $v_1 \wedge \cdots \wedge v_k \in \bigwedge^k W$ represents a point p in the image, the kernel of the linear map

$$W \to \bigwedge^{k+1} W,\ w \mapsto w \wedge v_1 \wedge \ldots \wedge v_k,$$

is the unique linear subspace of W sent to p.

Definition 6.3.38. The map (6.2) is called the **Plücker embedding** of $\mathbb{G}(k, W)$ into $\mathbb{P}(\bigwedge^k W)$. The homogeneous coordinates on $\mathbb{P}(\bigwedge^k W)$ are called the **Plücker coordinates** on $\mathbb{P}(\bigwedge^k W)$. □

Note that if $p \in \mathbb{P}(\bigwedge^k W)$ corresponds to the linear subspace $V = \langle v_1, \ldots, v_k \rangle$ of W under the Plücker embedding, then the Plücker coordinates of p are the $k \times k$ minors of the $n \times k$ matrix with columns v_j.

Exercise* 6.3.39. With notation as above, show:

1. The Plücker embedding is a closed embedding.
2. Each coordinate chart of $\mathbb{P}(\bigwedge^k W)$ intersects $\mathbb{G}(k, W)$ in an affine space of dimension $k(n-k)$. □

We give $\mathbb{G}(k, W)$ the **structure of a projective variety** by identifying it with its image under the Plücker embedding.

6.4 Hilbert Functions and Hilbert Polynomials

Numerical invariants of a projective algebraic set such as the dimension are useful in that they allow us to partition a given classification problem into handy pieces. In this section, we will rediscover the dimension as the degree of the Hilbert polynomial, and we will use this polynomial to obtain other important invariants. Theorem 6.4.5, which shows the existence of the polynomial, is the fourth major result of Hilbert treated in this book. Hilbert's goal when proving the result was to encode the infinitely many values of what is nowadays called the Hilbert function in finite terms. The general context for the Hilbert function is that of graded modules.

Definition 6.4.1. Let $S = \bigoplus_{d \geq 0} S_d$ be a graded ring. A **graded module** over S is an S-module with a decomposition $M = \bigoplus_{d \in \mathbb{Z}} M_d$ as Abelian groups such that $S_d M_e \subset M_{d+e}$ for all d, e. An element of M_d is, then, called a **homogeneous element** of M of **degree** d. A **graded submodule** of M is a submodule generated by homogeneous elements. If $N = \bigoplus N_d$ is another graded S-module, a **graded homomorphism** from M to N is an S-module homomorphism $\phi : M \to N$ such that $\phi(M_d) \subset N_d$ for any d. □

If we consider S as a graded module over itself, its graded submodules are precisely its homogeneous ideals. The characterization of homogeneous ideals in Proposition 6.1.2 extends from the ideal to the submodule case:

Aushuehren

Furthermore and if $N = \bigoplus N_d$ is a graded submodule of $M = \bigoplus M_d$, then the quotient $M/N = \bigoplus M_d/N_d$ is graded as well. The direct sum of a collection of graded S-modules is naturally graded, and so are the kernel and the image of a graded homomorphism.

Example 6.4.2. Let S be a graded ring. Given a graded S-module $M = \bigoplus M_d$ and $\ell \in \mathbb{Z}$, the **ℓth twist of M**, written $M(\ell)$, is the graded S-module

$$M(\ell) = \bigoplus_{d \in \mathbb{Z}} M_{d+\ell}.$$

That is, $M(\ell)$ is isomorphic to M as an S-module, but its grading is shifted in degrees by ℓ. In particular, for each ℓ, we have the graded S-module $S(\ell)$ in which the free generator 1 of S has degree $-\ell$. Since each homomorphism of S is multiplication by an element of S, each graded homomorphism $S(k) \to S(\ell)$ is multiplication by a homogeneous element of S of degree $k - l$.

By specifying a basis together with a degree for each basis vector, a free S-module F becomes a **graded free S-module** (with a basis of homogeneous elements). That is, as a graded S-module, F is isomorphic to a direct sum of graded modules of type $S(\ell)$, for various ℓ. □

Each graded piece of a graded S-module M is an S_0-module and, thus, a $\Bbbk$-vector space if S is a graded $\Bbbk$-algebra. These vector spaces are *of finite dimension* if, in addition, S is *Noetherian*, and M is *finitely generated*. Indeed, in this case, M is Noetherian by Exercise 1.10.9. On the other hand, if M_e would not be of finite dimension for some e, the truncation $M_{\geq e} = \bigoplus_{d \geq e} M_d$ would be a submodule of M which is not finitely generated.

Definition 6.4.3. Let S be a Noetherian graded $\Bbbk$-algebra, and let $M = \bigoplus_{d \in \mathbb{Z}} M_d$ be a finitely generated graded S-module. The function

$$H(M, \_) : \mathbb{Z} \longrightarrow \mathbb{Z}, \quad d \longmapsto H(M, d) := \dim_{\Bbbk} M_d,$$

is called the **Hilbert function** of M. □

Example 6.4.4. Let S be the polynomial ring $\Bbbk[x_0, \ldots, x_n]$. Then

$$H(S, d) = \binom{d+n}{n}$$

for all $d \geq 0$. In fact, the formula holds for all $d \in \mathbb{Z}$ if we set $S_d = 0$ for $d < 0$. Thus, $H(S, d)$ agrees for $d \geq -n$ with the polynomial expression

$$\frac{(d+n)(d+n-1)\cdots(d+1)}{n!}.$$

We refer to this fact by saying that $H(S, \_)$ is of **polynomial nature**. □

More generally, we have:

Theorem 6.4.5 (Polynomial Nature of Hilbert Functions). *Let S be the polynomial ring $\Bbbk[x_0, \dots, x_n]$, and let M be a finitely generated graded S-module. Then there is a unique polynomial $P_M(t) \in \mathbb{Q}[t]$ such that*

$$H(M, d) = P_M(d) \text{ for all } d \gg 0.$$

Furthermore, $\deg P_M \leq n$. □

Definition 6.4.6. In the situation of the theorem, P_M is called the **Hilbert polynomial** of M. □

Following Hilbert, we will use *graded* free resolutions to reduce Theorem 6.4.5 to the special case considered in Example 6.4.4. Here is the relevant notation:

Definition 6.4.7. Let $S = \bigoplus_{d \geq 0} S_d$ be a graded ring. A **graded complex** of S-modules is a complex of S-modules where all modules and homomorphisms are graded. Similarly, we define the notions **graded free resolution** and **graded homomorphism of graded complexes**. □

In the context of graded free resolutions, we often write homomorphisms "from right to left" since this is consistent with how information on the resolutions is printed by computer algebra systems. Note that a graded homomorphism $F = \bigoplus_{i=1}^{s} S(\ell_i) \longleftarrow G = \bigoplus_{j=1}^{t} S(k_j)$ is given by an $s \times t$-matrix whose ij entry is a homogeneous element of S of degree $k_j - \ell_i$, for each pair i, j.

Example 6.4.8. If $S = \Bbbk[w, x, y, z]$, the matrix

$$\phi = \begin{pmatrix} x + y + z & w^2 - x^2 & z^3 \\ 1 & x & xy + z^2 \end{pmatrix}$$

defines a graded homomorphism

$$S \oplus S(-1) \xleftarrow{\phi} S(-1) \oplus S(-2) \oplus S(-3).$$

□

In the graded case, the recipe from Section 2.8 for constructing free resolutions yields a *graded* free resolution if we choose *homogeneous* generators at each stage. In the special case where S is the polynomial ring $\Bbbk[x_0, \dots, x_n]$, we get a **graded version of the syzygy theorem**: Each finitely generated graded S-module M has a graded free resolution of length $\leq n + 1$, with finitely generated graded free S-modules. Indeed, this follows from our constructive proof of the syzygy theorem in Chapter 2 and Remark 6.1.10 on the behaviour of Buchberger's algorithm in the graded case.

Example 6.4.9. Consider the ideal $I = \langle f_1, f_2, f_3 \rangle \subset S = \Bbbk[w, x, y, z]$, where $f_1 = x^2 - wy$, $f_2 = xy - wz$, and $f_3 = y^2 - xz$. Then I defines the twisted cubic curve in $\mathbb{P}^3$, and

$$0 \longleftarrow S/I \longleftarrow S \xleftarrow{(f_1,f_2,f_3)} S(-2)^3 \xleftarrow{\begin{pmatrix} x & w \\ -y & -x \\ z & y \end{pmatrix}} S(-3)^2 \longleftarrow 0$$

is a graded free resolution of S/I. Note that f_1, f_2, f_3 are precisely the 2×2 minors of the 3×2 matrix in the resolution (with appropriate signs). This is no accident. It is, in fact, a consequence of the theorem of Hilbert-Burch, proved by Hilbert in his 1890 paper to give examples of free resolutions (see Eisenbud (1995), Theorem 20.15). □

Given a graded free resolution

$$0 \longleftarrow M \longleftarrow F_0 \xleftarrow{\phi_1} F_1 \longleftarrow \cdots \longleftarrow F_{i-1} \xleftarrow{\phi_i} F_i \xleftarrow{\phi_{i+1}} F_{i+1} \longleftarrow \cdots ,$$

where all free modules are finitely generated, we usually collect all copies of S involving the same twist when writing F_i:

$$F_i = \bigoplus_j S(-j)^{\beta_{ij}}. \tag{6.3}$$

The β_{ij} are known as the **graded Betti numbers** of the resolution. A convenient way of visualizing these numbers is to write a **Betti diagram** as in the following example:

```
            0     1     2     3
------------------------------
    0:      1     -     -     -
    1:      -     2     1     -
    2:      -     2     3     1
------------------------------
total:      1     4     4     1
```

A number `i` in the top row of the diagram refers to the ith free module F_i of the resolution. More precisely, the column with first entry `i` lists the number of free generators of F_i in different degrees and, in the bottom row, the total number of free generators (that is, the rank of F_i). If `k:` is the first entry of a row containing a number β in the column corresponding to F_i, then F_i has β generators in degree $k + i$. That is, in (6.3), β is the number β_{ij} with $j = k+i$. The diagram above indicates, for instance, that F_2 has one generator in degree 3 and three generators in degree 4. In total, the diagram corresponds to a graded free resolution of type

$$S(-2)^2 \oplus S(-3)^2 \leftarrow S(-3) \oplus S(-4)^3 \leftarrow S(-5) \leftarrow 0\,.$$

Example 6.4.10. Resolving the homogeneous coordinate ring of the twisted cubic curve as in Example 6.4.9, we get the Betti diagram below:

```
           0     1     2
------------------------
    0:     1     -     -
    1:     -     3     2
------------------------
total:     1     3     2
```

□

In general, the β_{ij} cannot be called invariants of M since they depend on the choices made when constructing the resolution. Over a Noetherian graded $\Bbbk$-algebra S, the concept of minimal free resolutions takes care of this problem. To show the uniqueness of such a resolution, we need a graded version of Nakayama's lemma. In comparison with the local version, we replace the uniquely determined maximal ideal $\mathfrak{m}$ by the ideal S_+, which is the uniquely determined homogeneous maximal ideal if S is a graded $\Bbbk$-algebra.

Theorem 6.4.11 (Lemma of Nakayama, Graded Version). *Let S be any graded ring, let M be a finitely generated graded S-module, and let $N \subset M$ be a graded submodule. Then*

$$N + S_+M = M \text{ iff } N = M.$$

Proof. Reducing to the case $N = 0$ as in the proof of the local version, it suffices to show that $S_+M = M$ implies $M = 0$. Since M is finitely generated, $M_d = 0$ for $d \ll 0$. Suppose that $M \neq 0$, let d be the least d such that $M_d \neq 0$, and let $m \in M_d$ be a nonzero element. If $S_+M = M$, then m can be written as a sum $m = \sum_i s_i m_i$, with elements $s_i \in S_+$ and $m_i \in M$, and where we may assume that all s_i and m_i are nonzero and homogeneous. Then all $d_i = \deg s_i$ are strictly positive, so that $d - d_i < d$ for each i. This contradicts the fact that the M_{d-d_i} are zero by the choice of d. □

If S is a graded $\Bbbk$-algebra, and M is a graded S-module, then the quotient $\overline{M} = M/S_+M$ is a $\Bbbk$-vector space, and each graded homomorphism $\phi : M \to N$ induces a $\Bbbk$-vector space homomorphism $\overline{\phi} : \overline{M} \to \overline{N}$. As in the local case, Nakayama's lemma gives:

Corollary 6.4.12. *Let S be a graded $\Bbbk$-algebra, and let M be a finitely generated graded S-module. Then $m_1, \ldots, m_r \in M$ generate M as an S-module iff the residue classes $\overline{m}_i = m_i + S_+M$ generate $\overline{M} = M/S_+M$ as a $\Bbbk$-vector space. In particular, any minimal set of generators for M corresponds to a $\Bbbk$-basis for $\overline{M}$, and any two such sets have the same number of elements.* □

Let, now, S be a *Noetherian* graded $\Bbbk$-algebra, and let M be a finitely generated graded S-module. A **minimal free resolution** of M is obtained by choosing a minimal set of homogeneous generators at each stage of constructing a graded free resolution of M. Given any graded free resolution

$$0 \longleftarrow M \xleftarrow{\phi_0} F_0 \xleftarrow{\phi_1} F_1 \longleftarrow \ldots \longleftarrow F_{i-1} \xleftarrow{\phi_i} F_i \xleftarrow{\phi_{i+1}} F_{i+1} \longleftarrow \ldots$$

with finitely generated free modules, the images of the basis vectors of F_i under ϕ_i form a minimal set of generators for $\operatorname{im}\phi_i$ iff $\operatorname{im}\phi_{i+1} \subset S_+F_i$. That is, if we regard ϕ_{i+1} as a matrix, then ϕ_{i+1} does not have a nonzero scalar entry. In fact, the jth row of ϕ_{i+1} has an entry in $\Bbbk \setminus \{0\}$ iff the image of the jth basis vector of F_i under ϕ_i is an S-linear combination of the images of the other basis vectors.

Example 6.4.13. The resolution of the homogeneous coordinate ring of the twisted cubic curve in Example 6.4.9 is minimal. □

Minimal free resolutions are uniquely determined up to graded isomorphisms of complexes. This is a consequence of the following more general result:

Proposition 6.4.14. *Let S be a Noetherian graded $\Bbbk$-algebra, let M be a finitely generated graded S-module, and let*

$$0 \longleftarrow M \xleftarrow{\phi_0} F_0 \xleftarrow{\phi_1} F_1 \xleftarrow{\phi_2} F_2 \longleftarrow \cdots$$

and

$$0 \longleftarrow M \xleftarrow{\psi_0} G_0 \xleftarrow{\psi_1} G_1 \xleftarrow{\psi_2} G_2 \longleftarrow \cdots$$

be graded free resolutions with finitely generated graded S-modules. Suppose that the first resolution is minimal. Then there is a graded homomorphism of complexes

$$\begin{array}{ccccccccccc}
0 & \longleftarrow & M & \xleftarrow{\phi_0} & F_0 & \xleftarrow{\phi_1} & F_1 & \xleftarrow{\phi_2} & F_2 & \longleftarrow & \cdots \\
 & & \downarrow{\scriptstyle \mathrm{id}_M} & & \downarrow{\scriptstyle \alpha_0} & & \downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_2} & & \\
0 & \longleftarrow & M & \xleftarrow{\psi_0} & G_0 & \xleftarrow{\psi_1} & G_1 & \xleftarrow{\psi_2} & G_2 & \longleftarrow & \cdots
\end{array}$$

such that each α_i is injective and identifies F_i with a direct summand of G_i:

$$G_i \cong F_i \oplus G_i', \quad \text{for some graded free } S\text{-module } G_i'.$$

Proof. Following the recipe from Exercise 2.8.17, starting from homogeneous free generators for F_0, we find a graded homomorphism α_0 such that the diagram

$$\begin{array}{ccc}
M & \xleftarrow{\phi_0} & F_0 \\
{\scriptstyle \mathrm{id}_M}\downarrow & & \downarrow{\scriptstyle \alpha_0} \\
M & \xleftarrow{\psi_0} & G_0
\end{array}$$

commutes. If we regard α_0 as a matrix with entries in S, all entries and, in fact, all minors are homogenous. On the other hand, by Corollary 6.4.12, the induced maps on vector spaces $\overline{\phi_0}$ and, thus, also $\overline{\alpha_0}$ are injective. Hence, there is a $\operatorname{rank} F_0 \times \operatorname{rank} F_0$ minor of α_0 which is nonzero modulo S_+. Since the minor is homogeneous, it must be a nonzero scalar, so that the corresponding $\operatorname{rank} F_0 \times \operatorname{rank} F_0$ matrix is invertible over S. This shows that α_0 has the desired properties. The result follows by induction. □

Exercise 6.4.15. With S and M as in the proposition, design an algorithm which computes a minimal free resolution starting from any given graded free resolution (of finite length, with finitely generated free modules).
Hint. Use nonzero scalar entries of the given matrices as pivot elements as for Gaussian elimination. □

The proposition shows that the graded Betti numbers β_{ij} of a minimal free resolution depend on the finitely generated S-module M only. We, therefore, call these numbers the **graded Betti numbers of M**, written $\beta_{ij}(M) = \beta_{ij}$.

Remark 6.4.16. Due to the local version of Nakayama's lemma, the concept of minimal free resolutions makes also sense over a *local* Noetherian ring R. If a finitely generated R-module M is given, its ***i*th Betti number** is the rank of the ith free module in the minimal free resolution of M. □

Proof of Theorem 6.4.5 (Hilbert). The uniqueness of P_M is clear. For the existence, consider any graded free resolution of M of length $\leq n+1$, with finitely generated free modules $F_i = \bigoplus_j S(-j)^{\beta_{ij}}$, where $S = \Bbbk[x_0, \ldots, x_n]$:

$$0 \longleftarrow M \longleftarrow F_0 \longleftarrow F_1 \longleftarrow F_2 \longleftarrow \cdots \longleftarrow F_{n+1} \longleftarrow 0$$

Then, for each d, the graded pieces of degree d fit into an induced exact sequence of finite dimensional $\Bbbk$-vector spaces. Computing the alternating sum of the dimensions as in Exercise 2.8.4, we get

$$\begin{aligned} H(M,d) &= \sum_{i=0}^{n+1} (-1)^i \sum_j \beta_{ij} H(S(-j),d) \\ &= \sum_{i=0}^{n+1} (-1)^i \sum_j \beta_{ij} \binom{n-j+d}{n} \end{aligned}$$

(see Example 6.4.4). For each $d \geq j-n$, the value $H(S(-j),d)$ agrees with the polynomial expression

$$\frac{(d-j+n)(d-j+n-1)\cdots(d-j+1)}{n!}.$$

Hence, if P_M is the polynomial

$$P_M(t) = \sum_{i=0}^{n+1} (-1)^i \sum_j \beta_{ij} \binom{t-j+n}{n} \in \mathbb{Q}[t],$$

then $H(M,d) = P_M(d)$ for each $d \geq \max\{j-n \mid \beta_{ij} \neq 0 \text{ for some } i\}$. □

In algebraic geometry, the module M in Hilbert's theorem is the homogenous ccordinate ring of a projective algebraic set.

Definition 6.4.17. If $A \subset \mathbb{P}^n$ is an algebraic set, the **Hilbert polynomial** of A, written $P_A(t)$, is defined to be the Hilbert polynomial of the homogeneous coordinate ring $\mathbb{K}[A]$. □

Theorem 6.4.18. *If $A \subset \mathbb{P}^n$ is a projective algebraic set of dimension r, then its Hilbert polynomial is of type*

$$P_A(t) = d\,\frac{t^r}{r!} \;+\; \textit{terms of degree} < r,$$

where d is a strictly positive integer.

Proof. By Remark 3.3.2, there is a Noether normalization

$$\mathbb{K}[y_0, \ldots, y_m] \subset \mathbb{K}[A] = \mathbb{K}[x_0, \ldots, x_n]/\mathrm{I}(A)$$

such that the y_j are linear forms in the x_i. Then $A \cap \mathrm{V}(y_0, \ldots, y_m) = \emptyset$ since, otherwise, the y_j would not be algebraically independent over $\mathbb{K}$. Hence, by Exercise **??**, projection from $\mathrm{V}(y_0, \ldots, y_m)$ defines finite morphisms $A \cap \pi^{-1}(U_j) \to \pi(A) \cap U_j$, where the U_j are the coordinate charts of $\mathbb{P}^m$. In particular, $r = \dim A = m$. Furthermore, by the second defining condition of a Noether normalization, $\mathbb{K}[A]$ is a *finitely generated* graded $\mathbb{K}[y_0, \ldots, y_r]$-module. Considering graded free resolutions over $\mathbb{K}[y_0, \ldots, y_r]$, we see that the Hilbert function of $\mathbb{K}[A]$ is of type

$$H(\mathbb{K}[A], d) = \sum_{i=0}^{r+1} (-1)^i \sum_j \alpha_{ij} \binom{r-j+d}{r}.$$

It follows that $P_A(t) \in \mathbb{Q}[t]$ is a polynomial of degree $\leq r$, and that $r!\, P_A(t) \in \mathbb{Z}[t]$. On the other hand, since $\Bbbk[y_0, \ldots, y_r]$ is a graded subring of $\mathbb{K}[A]$, we have

$$H(\mathbb{K}[A], d) \geq \binom{r+d}{r} \;\text{ for all }\; d.$$

We conclude that P_A has exactly degree r, and that its leading coefficient is strictly positive. □

Here are two corollaries of the proof:

Corollary 6.4.19. *Let $A \subset \mathbb{P}^n$ be a projective algebraic set, and let $C(A) \subset \mathbb{A}^{n+1}$ be the affine cone over A. Then*

$$\dim \mathbb{K}[A] = \dim C(A) = \dim A + 1.$$

Proof. We have $\dim \mathbb{K}[A] = \dim C(A)$, and this number is obtained via a Noether normalization as in the proof of the theorem. □

Corollary 6.4.20. *Let $A \subset \mathbb{P}^n$ be a projective algebraic set. Then* $\dim A$ *is the least number r such that there is a linear subspace $L \subset \mathbb{P}^n$ of dimension $n - r - 1$ with $A \cap L = \emptyset$.*

Proof. The projection from a linear subspace $\mathbb{P}^{n-r-1} \subset \mathbb{P}^n$ with $X \cap \mathbb{P}^{n-r-1} = \emptyset$ induces a morphism $X \to \mathbb{P}^r$, which is finite onto its image. If r is minimal, then the map is onto $\mathbb{P}^r$ and corresponds to a Noether normalization of the coordinate ring. □

Definition 6.4.21. *In the situation of Theorem 6.4.18, we write* $\deg A = d$, *and call this number the* **degree** *of* A. □

Though our definition is of purely algebraic nature, the degree has a geometric meaning: We will show in Proposition 6.6.11 that $\deg A$ is the number of points in which a *general* linear subspace of $\mathbb{P}^n$ of complementary dimension $n - \dim A$ intersects A.

Example 6.4.22. Let $A \subset \mathbb{P}^n$ be a hypersurface, let $f \in S = \mathbb{K}[x_0, \ldots, x_n]$ be a square-free form defining A, and let $d = \deg f$. Then

$$0 \longleftarrow \mathbb{K}[A] \longleftarrow S \xleftarrow{f} S(-d) \longleftarrow 0$$

is a graded free resolution of $\mathbb{K}[A]$, so that

$$\begin{aligned} P_A(t) &= \binom{n+t}{n} - \binom{n+t-d}{n} \\ &= d\,\frac{t^{n-1}}{(n-1)!} \;+\; \text{terms of degree} < n-1. \end{aligned}$$

Hence, $\deg A = d = \deg f$, and we conclude that our general definition of degree is consistent with that for hypersurfaces given earlier. □

Definition 6.4.23. Let $A \subset \mathbb{P}^n$ be a projective algebraic set of dimension r, with Hilbert polynomial P_A. The **arithmetic genus** of A is defined to be

$$p_a(A) = (-1)^r (P_A(0) - 1).$$

Let $C \subset \mathbb{P}^n$ be a curve. Then the Hilbert function can be written in the form

$$p_C(t) = dt + 1 - p_a.$$

p_a is called the **arithmetic genus** of C. □

Example 6.4.24. A plane curve $C \subset \mathbb{P}^2$ of degree d has Hilbert polynomial

$$p_C(t) = \binom{t+2}{2} - \binom{t-d+2}{2} = dt + 1 - \binom{d-1}{2}.$$

So C has arithmetic genus $p_a = \binom{d-1}{2}$. □

Remark 6.4.25. The funny way to write the constant term of the Hilbert polynomial comes from the Riemann-Roch Theorem 8.3.2.

We already mentioned that the degree d has a geometric interpretation. The arithmetic genus p_a has an even more fundamental interpretation. For a smooth irreducible curve over the complex numbers the arithmetic genus p_a determines the Euclidean topology of the underlying 2-dimensional manifold. By Corollary 8.4.7 and 8.2.6, the Euler number of the underlying 2-dimensional real manifold is $2 - 2p_a$. We will return to the arithmetic genus in Chapter 7, where we prove Riemann's inequality 7.4.12, and in Chapter 8. □

Exercise 6.4.26. Let $A \subset \mathbb{P}^4$ be the projective closure of the surface considered in Example 4.7.20. Compute equations for A as well as $\deg A$. □

Computing the Hilbert polynomial of a homogeneous coordinate ring S/I via syzygies may be costly since this means to compute Gröbner bases for I as well as for every kernel needed to construct a graded free resolution. The ideas of Macaulay only require the computation of a Gröbner basis for I:

Theorem 6.4.27 (Macaulay). *Let $S = \Bbbk[x_0, \ldots, x_n]$, let F be a graded free S-module, and let $M \subset F$ be a graded submodule. For any global monomial order $>$ on F, we have*

$$H(F/M, \_) = H(F/\mathbf{L}_>M, \_).$$

Proof. By Macaulay's Theorem 2.3.5, the standard monomials of degree d represent $\Bbbk$-vector space bases for both $(F/M)_d$ and $(F/\mathbf{L}_>(M))_d$. □

Computing the intitial ideal of a homogeneous ideal J and then the Hilbert polynomial of $p_{S/\mathbf{L}(J)}$ is one of the fastest ways to obtain information about $\mathrm{V}(J)$.

Exercise 6.4.28. Let $A \subset \mathbb{P}^n$ be a projective algebraic set, and let B be its image under the d-uple embedding of $\mathbb{P}^n$ into $\mathbb{P}^N$, with $N = \binom{n+e}{d}$. Show that P_A and P_B have the same constant term:

$$P_A(0) = P_B(0).$$

□

Exercise 6.4.29. Let $C \subset \mathbb{P}^1 \times \mathbb{P}^1$ be a hypersurface of bidegree (a, b). Show that C has degree $\deg C = a + b$ and arithmetic genus $p_a(C) = (a-1)(b-1)$. □

Exercise 6.4.30. Describe an algorithm which computes the minimal resolution from an arbitrary finite free resolution. Give a simplified algorithm which computes only the graded Betti numbers of the minimal resolution. □

Let $X \subset \mathbb{P}^n$ be a projective variety of dimension r, and let $H = \mathrm{V}(h) \subset \mathbb{P}^n$ be a hypersurface which does not contain X. By the Principal Ideal Theorem **??**, every component Z of $X \cap H$ has dimension $r - 1$.

Definition 6.4.31. *The* **intersection multiplicity** *of X and H along Z is the length of the Artinian ring $\mathcal{O}_{Z,\mathbb{P}^n}/(I_X^a + \langle h^a \rangle)\mathcal{O}_{Z,\mathbb{P}^n}$, where I_X^a and $\langle h^a \rangle$ denote the corresponding ideals in an affine chart $U_i \cong \mathbb{A}^n$ intersecting Z:*

$$i(X, H; Z) = \operatorname{length} \mathcal{O}_{Z,\mathbb{P}^n}/(I_X^a + \langle h^a \rangle)\mathcal{O}_{Z,\mathbb{P}^n}.$$

Example 6.4.32. The two hypersurfaces of Exercise 4.1.16 intersect along their common intersection curve with multiplicity two.

Theorem 6.4.33 (Bézout's Theorem, second version). *Let $X \subset \mathbb{P}^n$ be a projective variety and let $H \subset \mathbb{P}^n$ be a hypersurface which does not contain X. Let $Z_1, \ldots, Z_s$ be the irreducible components of $X \cap H$. Then*

$$\deg X \cdot \deg H = \sum_{j=1}^{s} i(X, H; Z_j) \deg Z_j.$$

For the proof we need some preparations.

Definition 6.4.34. *Let M be a module over a ring R and $m \in M$. Then*

$$\operatorname{Ann}(m) = \{r \in R \mid rm = 0\}$$

is called the **annihilator** *of m.*

$$\operatorname{Ann}(M) = \{r \in R \mid rm = 0 \, \forall m \in M\}$$

is the annihilator of M. An **associated prime** $\mathfrak{p}$ *of M is a prime ideal which occurs as annihilator of an element.*

$$\mathfrak{p} = \operatorname{Ann}(m)$$

for some $m \in M \setminus 0$.

$$\operatorname{Ass} M = \{\mathfrak{p} \text{ prime } \mid \mathfrak{p} = \operatorname{Ann}(m) \text{ for some } m \in M\}$$

denotes the set of associated primes.

Thus with this notation the associated primes of an ideal I in the sense of Chapter 1 are the associated primes of the quotient R/I as R-module, and not the associated primes of the R-module I. This inconsistency in notation is unfortunate, but has a long tradition. In practise it rarely leads to confusion. The associated primes of R/I are of much more interest than the associated primes of the module I.

Remark 6.4.35. Note, that in case of an module over an affine coordinate ring

$$\mathrm{V}(\operatorname{Ann}(M)) = \bigcup_{\mathfrak{p} \in \operatorname{Ass} M} \mathrm{V}(\mathfrak{p})$$

is the **support** of M. The **minimal primes** in $\operatorname{Ass}(M)$ correspond to the irreducible components of the support of M. Non-minimal primes are called **embedded primes**, because their zero loci is strictly contained in a component.

Exercise 6.4.36. Let M be an R-module, and let $\mathfrak{q}$ be a prime ideal of R. Prove $M_{\mathfrak{q}} = 0$ iff $\mathfrak{q} \supset \mathfrak{p}$ for an associated prime $\mathfrak{p} \in \mathrm{Ass}(M)$ □

The set of associated primes is never empty for a module $M \neq 0$ over a Noetherian ring.

Lemma 6.4.37. *Every maximal element in the set* $\{\mathrm{Ann}(m) \mid m \in M \setminus 0\}$ *is a prime ideal.*

Proof. Let $\mathfrak{p} = \mathrm{Ann}(m)$ be maximal among the annihilators. Suppose $x, y \in \mathfrak{p}$ and $x \notin \mathfrak{p}$. Then $xm \neq 0$ and $\mathrm{Ann}(m) \subset \mathrm{Ann}(xm)$ and $y \in \mathrm{Ann}(xm) = \mathrm{Ann}(m) = \mathfrak{p}$ by the maximality. So $\mathfrak{p}$ is prime. □

Thus, by the Noetherian property there exist an associated prime.

Exercise 6.4.38. Every associated prime of a graded module is homogeneous. □

Exercise 6.4.39. Let

$$0 \to M' \to M \to M'' \to 0$$

be a short exact sequence. Prove:

$$\mathrm{Ass}(M') \subset \mathrm{Ass}(M) \subset \mathrm{Ass}(M') \cup \mathrm{Ass}(M'')$$

□

Proposition 6.4.40. *Let M be a finitely generated graded S-module. M has a filtration*

$$0 = M^0 \subset M^1 \subset \ldots \subset M^r = M$$

by graded submodules such that the quotients $M^i/M^{i-1} \cong (S/\mathfrak{p}_i)(a_i)$ for a homogeneous prime ideal $\mathfrak{p}_i$ and a twist a_i.

Proof. If $m \in M$ is a homogeneous element of degree a with $\mathfrak{p} = \mathrm{Ann}(m)$ an associated prime, then

$$(S/\mathfrak{p})(-a) \hookrightarrow M\,,\ r + \mathfrak{p} \mapsto rm$$

is an embedding.

Consider the set of graded submodules $N \subset M$, which have a filtration as in the proposition. This set is nonempty, because M has an associated prime. Let $M' \subset M$ be maximal in this set. We have to show $M' = M$. Suppose $M' \subsetneq M$. Consider an associated prime $\mathfrak{p}$ of M/M' and the inclusion $(S/\mathfrak{p})(a) \hookrightarrow M/M'$. Let M^+ be the preimage of $(S/\mathfrak{p})(a)$ in M. Then $M' \subsetneq M^+$ has a one step longer filtration. This contradicts the maximality of M'. □

Exercise 6.4.41. Let $\mathfrak{p}$ be a minimal prime of M. Then $\mathfrak{p}$ occurs precisely length $M_{(\mathfrak{p})}$-times in any filtration of M. □

Proof of Bézout's Theorem 6.4.33. We compute the Hilbert polynomial of $M = S/(I_X + I_H) = R_X/hR_X$ in two ways. The short exact sequence

$$0 \longrightarrow R_X(-\deg h) \xrightarrow{h} R_X \longrightarrow M \longrightarrow 0$$

gives us

$$\begin{aligned} p_M(t) &= \deg X(t^r/r! - (t - \deg H)^r/r!) + \text{ lower terms} \\ &= \deg X \cdot \deg H\ t^{r-1}/(r-1)! + \text{ lower terms}\ . \end{aligned}$$

On the other hand, the filtration of M gives

$$\begin{aligned} p_M(t) &= \sum_j p_{S/\mathfrak{p}_j}(t + a_j) \\ &= \sum_{\dim \mathrm{V}(\mathfrak{p}_j) = r-1} \deg \mathrm{V}(\mathfrak{p}_j)\, t^{r-1}/(r-1)! + \text{ lower terms} \\ &= \Big(\sum_{j=1}^{s} i(X, H; Z_j) \deg Z_j\Big)\, t^{r-1}/(r-1)! + \text{ lower terms}\ , \end{aligned}$$

because the number, in which $\mathrm{I}(Z_j)$ occurs in the filtration, coincides with $i(X, H; Z_j)$. Comparing the leading coefficients gives

$$\deg X \cdot \deg H = \sum_{j=1}^{s} i(X, H; Z_j) \deg Z_j$$

as desired. □

Exercise 6.4.42. Let M be a graded S-module. Prove that the Hilbert polynomial of M has degree

$$\deg p_M(t) = \dim \operatorname{supp} M = \max\{\dim \mathrm{V}(\mathfrak{p}) | \mathfrak{p} \in \operatorname{Ass}(M)\},$$

and that the leading coefficient is

$$\sum_{\dim \mathrm{V}(\mathfrak{p}) = \dim \operatorname{supp} M} \text{length}\, M_{(\mathfrak{p})} \frac{\deg \mathrm{V}(\mathfrak{p})}{r!}.$$

□

Apriori knowledge of the Hilbert function or Hilbert polynomial can ease Gröbner basis computation tremendously. We illustrate this in an example.

Example 6.4.43. Consider the morphism

$$\mathbb{P}^1 \to \mathbb{P}^3, \quad [x_0 : x_1] \mapsto [x_0^4, x_0^3x_1, x_0x_1^3, x_1^4].$$

We want to compute the equations of the image curve. One way to do this is to compute a Gröbner basis of

$$\langle y_0 - x_0^4, y_1 - x_0^3x_1, y_2 - x_0x_1^3, y_3 - x_1^4\rangle$$

with respect to a product order. Another way is to guess the equations and then argue. Clearly,

$$J = \langle y_1y_2 - y_0y_3, y_1^3 - y_0^2y_2, y_1^2y_3 - y_0y_2^2, y_1y_3^2 - y_2^3\rangle$$

is contained in the kernel $I = \ker\varphi$ of

$$\varphi : S = \Bbbk[y_0, \ldots, y_3] \to R = \Bbbk[x_0, x_1].$$

To prove, that this is the Gröbner basis of the kernel, we compare various Hilbert functions. The image is $\operatorname{im}\varphi = \Bbbk[x_0^4, x_0^3x_1, x_0x_1^3, x_1^4] \subset R$. Hence, $S/I \cong \operatorname{im}\varphi$ has Hilbert function

$$h_{S/I}(t) = h_R(4t) = 4t + 1 \text{ for } t \geq 2.$$

On the other hand the lead terms of the generators of J with respect to the reversed lexicographic order and variables sorted $y_1 > y_2 > y_3 > y_0$ generate the ideal $J' = \langle y_1y_2, y_1^3, y_1^2y_3, y_2^3\rangle$. A $\Bbbk$-basis of S/J' is represented by the monomials in

$$\Bbbk[y_3, y_0] \oplus \Bbbk[y_3, y_0]y_1 \oplus \Bbbk[y_3, y_1]y_2 \oplus \Bbbk[y_3, y_0]y_2^2 \oplus \Bbbk[y_0]y_1^2.$$

Thus, $h_{S/J'}(t) = t + 1 + 2t + t - 1 + 1 = 4t + 1$ for $t \geq 2$. On the other hand,

$$h_{S/J'}(t) \geq h_{S/J}(t) \geq h_{S/I}(t).$$

Thus, equality holds, $I = J$, $\mathbf{L}(I) = J'$ and our 4 generators form a Gröbner basis. This completes our goal.

Finally, we can now easily compute the shape of the free resolution of S/I.

$$\begin{array}{lll} M_2 = \langle y_1y_2\rangle & : y_1^3 & = \langle y_2\rangle, \\ M_3 = \langle y_1y_2, y_1^3\rangle & : y_1^2y_3 & = \langle y_1, y_2\rangle, \\ M_4 = \langle y_1y_2, y_1^3, y_1^2y_3\rangle & : y_2^3 & = \langle y_1\rangle \end{array}$$

Thus, the shape of the free resolution computed as in 2.8.11 is

$$0 \leftarrow S/I \leftarrow S \leftarrow S(-2) \oplus S(-3)^3 \leftarrow S(-4)^4 \leftarrow S(-5) \leftarrow 0,$$

and this gives the minimal free resolution, since no constant term is contained in syzygy matrices for degree reasons. Computing the Hilbert polynomial from the free resolution, we get

$$p_{S/I}(t) = \binom{t+3}{3} - \binom{t+1}{3} - 3\binom{t}{3} + 4\binom{t-1}{3} - \binom{t-2}{3} = 4t + 1,$$

which agrees already for $t \geq 2$ with the Hilbert function.

For practical computations, the idea of using the Hilbert function in Gröbner basis computations leads to the following spead up of the elimination algorithm. The key point is, that a Gröbner basis with respect to a weighted reversed lexicographic order is much sheaper to compute than a Gröbner basis with respect to an elimination order.

Algorithm 6.4.44 (Hilbert function driven elimination). Input*: A homogeneous ideal $I \subset \Bbbk[x_0, \ldots, x_n, y_0, \ldots, y_m]$ with weighted variables of possibly different degrees.* **Output***: $I \cap \Bbbk[y_0, \ldots, y_m]$*
1. Compute a Gröbner basis with respect to the weighted reverse lexicographic order.
2. Compute the Hilbert function of $\Bbbk[x, y]/I$.
3. Compute a Gröbner basis with respect to an elimination order, but skip all Buchberger tests in a given degree, when there are already enough leading terms to account for the Hilbert function.

Example 6.4.45. Here is an example, where the Hilbert function driven Buchberger allows to compute the elimination ideal, while without this the computation takes much too long. Camera positioning.

Another way to present the Hilbert function is as follows:

Definition 6.4.46. *Let M be a graded module with $\dim M_d < \infty$ for all d. Then*

$$H_M(s) = \sum_{d \in \mathbb{Z}} \dim M_d s^d \in \mathbb{Z}[[s, s^{-1}]]$$

is called the **Hilbert series** *of M.*

Lemma 6.4.47. *Let M be a finitely generated graded module over the polynomial ring $\Bbbk[x_0, \ldots, x_n]$. Then H_M is the rational function*

$$H_M(s) = \frac{\sum_{ij} (-1)^i \beta_{ij} s^j}{(1-s)^{n+1}},$$

where the β_{ij} are the graded Betti numbers of M. If $r = \dim \operatorname{supp} M$ then the rational function $H_M(s)$ has a pole of order precisely $r+1$ at $s = 1$.

Proof. The Hilbert series of $\Bbbk[x_1, \ldots, x_n]$ is

$$\frac{1}{(1-s)^{n+1}} = \sum_{t=0}^{\infty} \binom{n+t}{n} s^t.$$

Thus, expanding the rational function

$$\frac{\sum_{ij} (-1)^i \beta_{ij} s^j}{(1-s)^{n+1}}$$

at $s = 0$ yields a series whose coefficients satisfy the same formula as the Hilbert function $h_M(t) = \dim M_t$:

$$h_M(t) = \sum_{i=0}^{n+1} (-1)^i \sum_j \beta_{ij} \binom{n-j+t}{n}.$$

If we consider syzygies over a linear Noether normalization

$$\operatorname{supp} M \to \mathbb{P}^r$$

of $\operatorname{supp} M$, then we see that $H_M(s)$ has a pole of order at most $r+1$ at $s = 1$. It cannot have a pole of smaller order, because otherwise the coefficients of $H_M(s)$ would not grow fast enough. □

Remark 6.4.48. A similar formula holds for graded modules over a polynomial ring with generators x_i of different degrees. If $\deg x_i = d_i$ then the denominator takes the form $(1 - s^{d_0}) \cdot \ldots \cdot (1 - s^{d_n})$.

Example 6.4.49. Let $d_0, \ldots, d_n \in \mathbb{Z}_{>}0$ be a set of integers with no common divisor. We consider the group action of $\Bbbk^*$ on $\Bbbk^{n+1} \setminus 0$ defined by

$$\Bbbk^* \times \Bbbk^{n+1} \to \Bbbk^{n+1},\ (\lambda, (a_0, \ldots, a_n)) \mapsto (\lambda^{d_0} a_0, \ldots, \lambda^{d_n} a_n).$$

The **weighted projective space**

$$\mathbb{P}(d_0, \ldots, d_n) = (\Bbbk^{n+1} \setminus 0)/\Bbbk^*$$

is defined as the orbit space under this action. In case $d_0 = d_1 = \ldots = d_n = 1$ this is the ordinary projective space $\mathbb{P}^n$. We give $\mathbb{P}(d_0, \ldots, d_n)$ the structure of a projective variety as follows. Consider the polynomial ring $S = \Bbbk[x_0, \ldots, x_n]$ with grading induced by $\deg x_i = d_i$. Let $\ell = \operatorname{lcm}(d_0, \ldots, d_n)$ and let $m_0, \ldots, m_N \in S_\ell$ be a basis formed by monomials. Then

$$\mathbb{P}(d_0, \ldots, d_n) \to \mathbb{P}^N$$

induced by

$$a = (a_0, \ldots, a_n) \mapsto [m_0(a) : \ldots : m_N(a)]$$

is a well-defined embedding. However $\mathbb{P}(d_0, \ldots, d_n)$ is in general not smooth. The standard charts might carry some quotient singularities:

$$U_i = \{[a] \mid a_i = 1\} \cong \Bbbk^n/\mu_{d_i},$$

where μ_d denotes the group of d-th roots of unity.

Exercise 6.4.50. Prove that

$$\mathbb{P}(1, 1, 2) \cong V(x_0 x_2 - x_1^2) \subset \mathbb{P}^3.$$

□

Exercise 6.4.51. Consider $S = \Bbbk[x_0, \ldots, x_n]$ the polynomial ring with the grading induced by $\deg x_i = d_i$ and the corresponding weighted projective space. Let $I \subset S$ be a homogenous ideal with respect to this grading.

1. Prove that

$$V(I) = \{[a] \in \mathbb{P}(d_0, \ldots, d_n) \mid f(a) = 0 \text{ for all homogeneous } f \in I\}$$

is an algebraic subset of $\mathbb{P}(d_0, \ldots, d_n)$, and that every algebraic subset arises in this way.
2. Let

$$H_{S/I}(s) = \frac{\sum_{ij}(-1)^i \beta_{ij} s^j}{(1 - s^{d_0}) \cdot \ldots \cdot (1 - s^{d_n})}$$

be the Hilbert series of S/I according to Remark 6.4.48. Prove that $V(I) \subset \mathbb{P}(d_0, \ldots, d_n)$ has dimension r iff $H_{S/I}(s)$ has a pole of order $r + 1$ at $s = 1$.

□

Exercise 6.4.52. Complete the proof of Theorem 3.3.8.

Hint: Consider the projective closure in a suitable weighted projective space $\mathbb{P}(1, d_1, \ldots, d_n)$, where $w = (d_1, \ldots, d_n) \in \mathbb{Z}^n_{>0}$ is a weight vector, such that the Gröbner basis for the given monomial order $>$ and the weight order $>_w$ coincides. □

Exercise 6.4.53. Let $I \subset \Bbbk[x_0, \ldots, x_n] = \Bbbk[x]$ be a homogeneous ideal, and let

$$\varphi : \Bbbk[y_0, \ldots, y_m] \to \Bbbk[x]/I, y_i \mapsto f_i + I$$

be the substitution homomorphism induced by homogeneous forms $f_i \in \Bbbk[x_0, \ldots, x_n]$ of degree $\deg f_i = d_i$. Let

$$J = I\Bbbk[x, y] + \langle y_0 - f_0, \ldots, y_m - f_m \rangle$$

be the ideal of the graph in $\mathbb{P}(\deg x_0, \ldots, \deg x_n, d_0, \ldots d_m)$ of the corresponding rational map

$$\mathrm{V}(I) \dashrightarrow \mathbb{P}(d_0, \ldots, d_m).$$

Prove

$$H_{\Bbbk[x]/I}(s) = H_{\Bbbk[x,y]/J}(s).$$

□

6.5 Dimension Formulas

Theorem 6.5.1 (on the dimension of intersections). *Let $X, Y \subset \mathbb{P}^n$ be two subvarieties. Then every component Z of $X \cap Y$ has dimension*

$$\dim Z \geq \dim X + \dim Y - n.$$

If the right hand side is non-negative then the intersection $X \cap Y$ is non-empty.

Proof. Consider the **join** $J(X,Y) \subset \mathbb{P}^{2n+1}$ defined by the ideal $I(X)+I(Y) \subset \Bbbk[x_0,\ldots,x_n,y_0,\ldots,y_n]$. $J(X,Y)$ is the union of all lines joining a point of $X \subset \mathbb{P}^n \subset \mathbb{P}^{2n+1}$ with a point of $Y \subset \mathbb{P}^n \subset \mathbb{P}^{2n+1}$ contained in two complementary linear subspaces $\mathbb{P}^n \subset \mathbb{P}^{2n+1}$. With $\mathbb{P}^n \cong \Delta = \mathrm{V}(x_0-y_0,\ldots,x_n-y_n) \subset \mathbb{P}^{2n+1}$ the "diagonal" we have

$$X \cap Y = \Delta \cap J(X,Y).$$

A Gröbner basis of $J(X,Y)$ is the union of the Gröbner basis for X and for Y. So $\dim J(X,Y) = \dim X + \dim Y + 1$. On the other hand Δ is defined by $n+1$ equations. Thus the generalized Principle Ideal Theorem 4.6.19 gives the desired inequality for the dimension of each component of $X \cap Y$.

For the second statement we consider the affine cones $C(X), C(Y) \subset \mathbb{A}^{n+1}$. The origin $0 \in \mathbb{A}^{n+1}$ lies in the intersection of the cones. Since every component of the intersection $C(X) \cap C(Y)$ has dimension at least $\dim X + 1 + \dim Y + 1 - n - 1 \geq 1$, there is at least one component containing the origin properly. This component is a cone again. Hence, we obtain $X \cap Y \neq \emptyset$. □

Remark 6.5.2. The reader might ask, why we did not prove Bézout's Theorem in a more general version for intersections $X \cap Y \subset \mathbb{P}^n$, say in case all components Z of $X \cap Y$ have expected $\dim Z = \dim X + \dim Y - n$. The reason is that $\operatorname{length} \mathcal{O}_{Z,\mathbb{P}^n}/(I_X + I_Y)\mathcal{O}_{Z,\mathbb{P}^n}$ no longer gives the correct intersection multiplicity for the Theorem.

Exercise 6.5.3. Consider the surface $X \subset \mathbb{P}^4$ from Example 4.7.20 and Exercise 6.4.26 and let $Y = \mathrm{V}(x_1 - x_3, x_3 - x_4) \subset \mathbb{P}^4$ be a plane passing through the improper node $p = [0:0:0:0:1]$. Prove that

$$\operatorname{length} \mathcal{O}_p/(I_X + I_Y)\mathcal{O}_p = 3,$$

although there are 3 intersection points away from the node. Thus, adding the various length gives at least 3+1+1+1=6, which is larger than $\deg X \deg Y = 5 \cdot 1$

The reason why the numbers do not match is, that the module $S/(I_X+I_H)$ for the intersection of X with a hyperplane H containing Y has already $\mathfrak{m}_p$ as an associated prime. Thus, the full intersection ring gets too large. □

The general correct definition of the intersection multiplicity was a topic of Gröbner's research [1951]. In case of an intersection of two varieties of "expected" dimension $\dim X + \dim Y - \dim \mathbb{P}^n$, the correct definition was finally given by Serre [1957]:

$$i(X,Y;Z) = \sum_{i \geq 0} (-1)^i \operatorname{length} \operatorname{Tor}^i_{\mathcal{O}_{\mathbb{P}^n,Z}}(\mathcal{O}_{\mathbb{P}^n,Z}/I_X\mathcal{O}_{\mathbb{P}^n,Z}, \mathcal{O}_{\mathbb{P}^n,Z}/I_Y\mathcal{O}_{\mathbb{P}^n,Z}).$$

A disadvantage of this formula is that $i(X,Y;Z) > 0$ is no longer obvious. Fortunately, this is still true . In case we have a component Z of excess dimension, that is of dimension $\dim Z > \dim X + \dim Y - \dim \mathbb{P}^n$, one can apply

the intersection theory of Fulton [1998] and/or Flenner, O'Carrel and Vogel [1999].

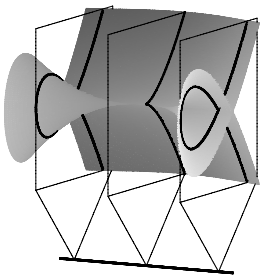
Let $\varphi : X \to Y$ be a morphism. For $q \in Y$ we call $X_q = \varphi^{-1}(q)$ the **fiber** of φ over q. On the right is the illustration of an affine piece of the surface

$$X = \mathrm{V}(y^2z - x^2(t^2z - x)) \subset \mathbb{P}^2 \times \mathbb{A}^1$$

$$\varphi \downarrow$$

$$Y = \mathbb{A}^1$$

and three fibers of the projection to the t-axis.



Theorem 6.5.4 (on the fiber dimension). *Let $\varphi : X \to Y$ be a projective morphism.*

1. *The function*
$$q \mapsto \dim X_q$$
is upper semi-continous on Y.
2. *If φ is a surjective map between varieties then there exists a non-empty open subset of $U \subset Y$, such that*
$$\dim X_q = \dim X - \dim Y$$
for all $q \in U$.

In particular, for a surjective projective morphism,

$$\dim X_q \geq \dim X - \dim Y$$

holds for every $q \in Y$.

Proof. 1.) We may assume that $X \subset Y \times \mathbb{P}^n$ is a closed subset. Let $q \in Y$ be a point and $\dim X_q = r$. Choose a linear subspace $\mathbb{P}^{n-r-1} \subset \mathbb{P}^n$ which does not intersect $X_q \subset \mathbb{P}^n$. Then $A = X \cap (Y \times \mathbb{P}^{n-r-1}) \subset Y \times \mathbb{P}^n$ is an algebraic set, whose image $pr_1(A) \subset Y$ contains all points q', where the fiber $X_{q'}$ has dimension $> r$ by Theorem 6.5.1 and perhaps some other points. Since the image is algebraic by 6.3.26 and $q \notin pr_1(A)$ the open set $V = Y \setminus pr_1(A)$ is an open neighborhood of q with $\dim X_{q'} \leq r$ for all $q' \in V$.

2.) We may assume that Y is affine and that $X \subset Y \times \mathbb{P}^n$. Consider the function fields $\Bbbk(Y) \subset \Bbbk(X)$.

$$\mathrm{trdeg}_{\Bbbk(Y)} \Bbbk(X) = \mathrm{trdeg}_{\Bbbk} \Bbbk(X) - \mathrm{trdeg}_{\Bbbk} \Bbbk(Y).$$

Let $I \subset \Bbbk[Y][x_0, \ldots, x_n]$ be the ideal of $X \subset Y \times \mathbb{P}^n$. We compute a Gröbner basis for $I \subset \Bbbk(Y)[x_0, \ldots, x_n]$ over the function field $\Bbbk(Y)$. The resulting Gröbner basis corresponds to a variety of dimension $\operatorname{trdeg}_{\Bbbk(Y)} \Bbbk(X)$ defined over $\Bbbk(Y)$. In such a computation of a Gröbner basis we have to invert finitely many leading coefficients in $\Bbbk[Y]$. Let f be the product of all these leading coefficients. Then for a point $q \in U = Y \setminus \mathrm{V}(f)$ the Gröbner basis of the ideal $I_q = \langle f(x, q) \mid f \in I \rangle$ defining X_q is obtained by substituting q into the coefficients of the Gröbner basis for $I \subset \Bbbk(Y)[x_0, \ldots, x_n]$. Thus, $\dim X_q = \operatorname{trdeg}_{\Bbbk(Y)} \Bbbk(X) = \dim X - \dim Y$ for all $q \in U$. We have proved more: the Hilbert function of $\Bbbk[x_0, \ldots, x_n]/I_q$ is the same for all $q \in U$.

The last statement follows from combining 1.) and 2.). □

Remark 6.5.5. 1. Assertion 6.5.4.1 does not hold without the hypothesis of projectivity. An example where the assertion does not hold is Example **??**.2.
2. An example of a projective morphism between varieties, where the fiber dimension is not constant, is the blow-up 7.2.1 below.

The following result has a very similar proof.

Theorem 6.5.6 (Reduction mod p). *Let $I = \langle f_1, \ldots, f_r \rangle \subset \mathbb{Q}[x_0, \ldots, x_n]$ be a homogeneous ideal defined by polynomials f_i with integer coefficients. For a prime number p we denote by $I_p \subset \mathbb{F}_p[x_0, \ldots, x_n]$ the ideal generated by the reduction of the f_i mod p. For all but finitely many primes the Hilbert function of $\mathbb{Q}[x_0, \ldots, x_n]/I$ and $\mathbb{F}_p[x_0, \ldots, x_n]/I_p$ coincide.*

Proof. We compute a normalized Gröbner basis of $I \subset \mathbb{Q}[x_0, \ldots, x_n]$. In this process we divide by finitely many leading terms. Let B be the set of primes, which devides a numerator of some of these leading terms. For p a prime outside B the computation of the Gröbner basis of I_p has exactly the same steps. In particular, $\mathbf{L}(I)$ and $\mathbf{L}(I_p)$ are generated by the same monomials. The result follows with Corollary 6.4.27. □

Remark 6.5.7. 1. Within Grothendieck's theory of schemes (eg. Hartshorne [1977], Chapter II and III), Theorem 6.5.6 and Theorem 6.5.4 have indeed a common generalization.
2. For practical purposes, Theorem 6.5.6 on the reduction mod p is of great importants. As long as we are only interested in the qualitative behavior of a system of equations, say in the dimension or degree, we can use a Gröbner basis computation mod p, which is much faster than the computations over $\mathbb{Q}$, because the bit length of the coefficients do not grow over $\mathbb{F}_p$. In doing so, we have to choose p outside B, which we usually do not know in advance. However, when choosing moderate size p, the chances for $p \in B$ are really low. The authors never had the bad luck to choose $p \in B$.

Exercise 6.5.8. Let $X \subset \mathbb{P}^n$ be a variety defined over $\mathbb{Q}$, and let $\mathrm{I}(X) = \langle f_1, \ldots, f_r \rangle$ be generators with integral coefficients. Let $I_p = \langle f_1, \ldots, f_r \rangle \subset$

$\mathbb{F}_p[x_0,\dots,x_n]$ be generated by their reductions mod p. Prove: If X is non-singular, then $X_p = \mathrm{V}(I_p)$ is non-singular for all but finitely many primes p. □

Exercise 6.5.9. Let $f_1,\dots,f_r \in \mathbb{Z}[x_0,\dots,x_n]$ be homogeneous polynomials, and let $I \subset \mathbb{Q}[x_0,\dots,x_n]$ and $I_p \subset \mathbb{F}_p[x_0,\dots,x_n]$ denote the ideals generated by them over $\mathbb{Q}$ and $\mathbb{F}_p$, respectively. Prove

$$h_{\mathbb{F}_p[x_0,\dots,x_n]/I_p}(t) \geq h_{\mathbb{Q}[x_0,\dots,x_n]/I}(t) \text{ for all } t \in \mathbb{Z}.$$

□

6.6 Bertini's Theorem and other Applications

The dimension formulas have many applications. One of the most important is Bertini's theorem.

For a given projective space $\mathbb{P}^n = \mathbb{P}(V)$ the space of hyperplanes is natural the projective space of the dual vector space

$$\check{\mathbb{P}}^n = \mathbb{P}^n(V^*).$$

Theorem 6.6.1 (Bertini). *Let $X \subset \mathbb{P}^n$ be a smooth projective variety of dimension r. There exists a non-empty open subset $U \subset \check{\mathbb{P}}^n$, such that $X \cap H$ is smooth of dimension $r-1$ for every $H \in U$.*

Remark 6.6.2. It is true that for $\dim X \geq 2$ and $H \in U$ the intersection $X \cap H$ is also connected, hence irreducible. Frequently, this is considered to be part of Bertini's Theorem. The connectedness statement follows easily from cohomology theory of coherent sheaves, in particular Serre duality, which we do not treat in this book. See Hartshorne [1977] III.7.9. We will sketch a proof for fields $\Bbbk$ of characteristic zero in the appendix to this section.

Proof. We may assume that X is **non-degenerate**, i.e. that X spans $\mathbb{P}^n$. Then $X \cap H$ is singular at p iff $T_pX \subset H$. Since $T_pX \cong \mathbb{P}^r$ there exists an $\mathbb{P}^{n-r-1} \subset \check{\mathbb{P}}^n$ of hyperplanes H with $H \supset T_pX$. Consider the diagram

$$\begin{array}{ccc} N = \{(p,H) \in X \times \check{\mathbb{P}}^n \mid T_pX \subset H\} & \to & \check{\mathbb{P}}^n \\ \downarrow & & \\ X & & \end{array}$$

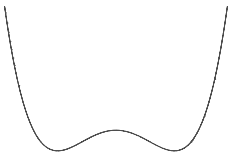
The fibers of $N \to X$ are $(n-r-1)$-dimensional. Hence, $\dim N = n-1$ and the image $\check{X}$ of N in $\check{\mathbb{P}}^n$ is at most a hypersurface. The open set $U = \check{\mathbb{P}}^n \setminus \check{X}$ has the desired property. □

Definition 6.6.3. *$\check{X} \subset \check{\mathbb{P}}^n$ is called the dual variety of $X \subset \mathbb{P}^n$. More generally, for possibly singular varieties $X \subset \mathbb{P}^n$ the dual variety is defined as the closure of the image of*

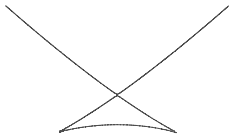
$$N^0 = \{(p, H) \in X^0 \times \check{\mathbb{P}}^n \mid T_p X \subset H\} \to \check{\mathbb{P}}^n$$

where $X^0 = X \setminus X_{sing}$ *denotes the set of smooth points of* X.

Example 6.6.4. For a plane curve $C \subset \mathbb{P}^2$ the dual variety is again a plane curve $\check{C} \subset \check{\mathbb{P}}^2$.



The curve defined by $y = x^4 - x^2$.



The dual curve in the chart $b = 1$.

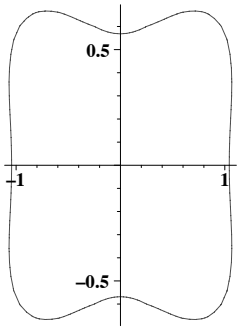
In this example the dual curve has equation

$$27a^4 - 4a^2b^2 + 144a^2bc - 16b^3c + 128b^2c^2 - 256bc^3 = 0$$

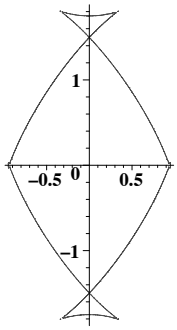
in coordinates a, b, c dual to x, y, z.

Exercise 6.6.5. Prove: An ordinary double point of $\check{C}$ corresponds to a bitangent of C. A cusp of $\check{C}$ corresponds to a flex of C. □

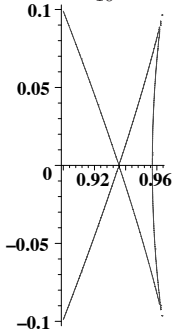
Exercise 6.6.6. Consider the curve $\mathrm{V}(x^4 + 4y^4 - x^2z^2 - y^2z^2 - \frac{1}{10}z^4) \subset \mathbb{P}^2$.



The curve with equation $x^4 + 4y^4 - x^2 - y^2 - \frac{1}{10}$



The dual curve.



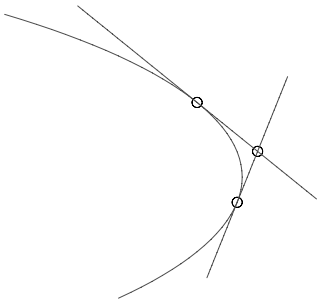
A detail of the dual curve.

Verify that the dual curve is defined by the equation

$$\begin{aligned}
&a^{12} + \frac{20}{13}a^{10}b^2 + \frac{1297}{676}a^8b^4 + \frac{205}{169}a^6b^6 + \frac{239}{338}a^4b^8 + \frac{35}{169}a^2b^{10} + \frac{49}{676}b^{12} \\
&+\frac{290}{13}a^{10}c^2 - \frac{1210}{169}a^8b^2c^2 - \frac{3335}{338}a^6b^4c^2 + \frac{385}{338}a^4b^6c^2 - \frac{1355}{338}a^2b^8c^2 + \frac{385}{338}b^{10}c^2 \\
&+\frac{23430}{169}a^8c^4 - \frac{34000}{169}a^6b^2c^4 + \frac{34595}{338}a^4b^4c^4 - \frac{9250}{169}a^2b^6c^4 + \frac{30}{169}b^8c^4 \\
&+\frac{9600}{169}a^6c^6 + \frac{61800}{169}a^4b^2c^6 + \frac{37800}{169}a^2b^4c^6 - \frac{5400}{169}b^6c^6 - \frac{164800}{169}a^4c^8 \\
&-\frac{80000}{169}a^2b^2c^8 + \frac{800}{169}b^4c^8 + \frac{192000}{169}a^2c^{10} + \frac{48000}{169}b^2c^{10} - \frac{64000}{169}c^{12} = 0
\end{aligned}$$

Here a, b, c are dual coordinates to x, y, z. □

Exercise 6.6.7. Suppose $\operatorname{char}\Bbbk = 0$. Prove for an irreducible plane projective curve, that the double dual curce is the original curve, i.e. $\check{\check{C}} = C$.



□

Remark 6.6.8. In case of $\operatorname{char}\Bbbk = p > 0$, the double dual curve is not necessarily the original curve. For example, each tangent of the curve $\mathrm{V}(x^p + yz^{p-1})$ passes through the point $[1:0:0]$, so the dual curve is the line $L \subset \check{\mathbb{P}}^2$ dual to this point. A curve different from a line with the property that every tangent line passes through a fixed point is called **strange**. Strange curves exist only in $\operatorname{char}\Bbbk = p > 0$, by the exercise above. One can prove that strange curves are not smooth.

Exercise 6.6.9. ($\operatorname{char}\Bbbk = 0$). Prove $\check{\check{X}} = X$ for arbitrary varieties. □

Corollary 6.6.10. *Let $X \subset \mathbb{P}^n$ be a variety. There exists a open set $U \subset \check{\mathbb{P}}^n$ such that $(X \cap H)_{sing} = X_{sing} \cap H$ for all $H \in U$.*

Proof. $U = \check{\mathbb{P}}^n \setminus \check{X}$ has this property. □

Corollary 6.6.11. *Let $X \subset \mathbb{P}^n$ be a variety of dimension r and degree d. A general linear subspace $\mathbb{P}^{n-r} \subset \mathbb{P}^n$ intersects X in d distinct points.*

Proof. Combine Bertini's Theorem with Bézout's Theorem 6.4.33. □

Exercise 6.6.12. Let $X \subset \mathbb{P}^n$ an absolutely irreducible non-degenerate variety of dimension r. Prove

$$\deg X \geq n - r + 1.$$

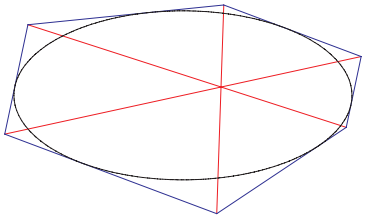
□

Exercise 6.6.13. Consider the d-th Veronese embedding

$$\mathbb{P}^n \hookrightarrow \mathbb{P}^N$$

with $N = \binom{n+d}{d}$. The dual variety $\check{X}$ of the image X can be identified with the set of singular hypersurfaces of degree d in $\mathbb{P}^n$. What is the degree of X? See Ge'lfand, Kapranov and Zelevinsky [1994] for a beautiful treatise on dual varieties. □

Exercise 6.6.14. Deduce Brianchon's Theorem from Pascal's Theorem 5.5.4 and projective duality: A hexagon in $\mathbb{P}^2$ is circumscribed to a smooth conic, if and only if the lines joining opposite vertices intersect in a point.



□

The dimension formulas and Bertini's theorem give another proof that every variety is birational to a hypersurface:

Theorem 6.6.15. *Let the ground field $\Bbbk$ be infinite. A variety $X \subset \mathbb{P}^n$ of dimension r can be birationally projected onto a hypersurface $X' \subset \mathbb{P}^{r+1}$*

Proof. We will project X from a center $\mathbb{P}^{n-r-2} \subset \mathbb{P}^n$ to $\mathbb{P}^{r+1}$. The induced map $X \to X' \subset \mathbb{P}^{r+1}$ is everywhere defined and finite if the center does not intersect X, which is the case for a general choice of the projection center. The problem is to prove that $X \to X'$ is birational. The preimage of a line $L \subset \mathbb{P}^{r+1}$ is a $\mathbb{P}^{n-r}$ containig the center of projection. For general choices this linear space will intersect X in $d = \deg X$ many distinct points by Bertini's Theorem. $X \to X'$ is birational in a neighborhood of one of these points iff none of the $d-1$ secant lines of X through the point intersect the center $\mathbb{P}^{n-r-2}$. We can acchieve this if we choose the primage $\mathbb{P}^{n-r}$ of the line first and then the center of projection $\mathbb{P}^{n-r-2} \subset \mathbb{P}^{n-r}$ such that it intersects none of the $\binom{d}{2}$ secant lines. □

Exercise 6.6.16. With the notation as in the proof of 6.6.15 and the additional assumption that $X \subset \mathbb{P}^n$ is smooth, prove that X' is either smooth and $X \to X'$ an isomorphismen, or X'_{sing} is of pure dimension $r-1$. □

The proof of the following theorem is of a simular flavour.

Theorem 6.6.17. *Every smooth projective curve can be embedded into $\mathbb{P}^3$.*

Proof. Suppose $C \subset \mathbb{P}^n$. If $n \leq 3$ there is nothing to prove. If $n \geq 4$ then we consider the secant variety. Consider the variety $\{(p_1, p_2, q) \in C \times C \times \mathbb{P}^r \mid p_1 \neq p_2 \text{ and } q \in \overline{p_1 p_2}\}$. The secant variety $Sec(C) \subset \mathbb{P}^n$ is the image of the closure of this set. Note that all tangent lines of C are contained in $Sec(C)$. By the dimension formula $\dim Sec(C) \leq 3$. Thus for $n \geq 4$ we can find a point $q \in \mathbb{P}^n \setminus Sec(C)$. The projection from p induces an isomorphism from C onto its image in $\mathbb{P}^{n-1}$. □

Exercise 6.6.18. Why is Theorem 6.6.17 not true for singular curves? □

Exercise 6.6.19. Prove that every smooth projective variety of dimension d can be embedded into $\mathbb{P}^{2d+1}$. □

Remark 6.6.20. Surfaces which can be embedded into $\mathbb{P}^4$ satisfy an identity between their numerical invariants, (see eg. Hartshorne [1977], Appendix A. Example 4.1.3). A famous result of Severi says that a non-degenerate smooth surface $X \subset \mathbb{P}^5$ can be isomorphically projected into $\mathbb{P}^4$ iff X is projectively equivalent to the Veronese surface, i.e. the image $\mathbb{P}^2 \hookrightarrow \mathbb{P}^5$ under the 2-uple embedding.

Exercise 6.6.21. a) Prove with Computer algebra the easy part of Severi's theorem: $\mathbb{P}^2 \hookrightarrow \mathbb{P}^5$ can be projected isomorphically. b) Describe the set of points in $\mathbb{P}^5$ from which one can project the Veronese surface isomorphically, and give a proof of the easy part without Computer algebra. (c) Prove the hard part of Severi's Theorem, i.e. no other surface in $\mathbb{P}^5$ can be projected isomorphically. □

6.7 Appendix: Monodromy Arguments

In this appendix we will prove the irreducibility of a general hyperplane $X \cap H$ section of a variety $X \subset \mathbb{P}^n$ of dimension $\dim X \geq 2$. We start by investigating general hyperplane sections of curves. Our first step is to establish the path connectedness of irreducible curves.

Theorem 6.7.1. *Let $f \in \mathbb{C}[x,y]$ be an irreducible polynomial and $C = \mathrm{V}(f) \subset \mathbb{A}^2(\mathbb{C})$ the corresponding plane algebraic curve. Then C equipped with the Euclidean topology is path connected.*

The proof of this result is interesting in its own. However, it requires some basic knowledge in Galois theory and analytic continuation of algebraic functions of one complex variable.

Proof. Let

$$f(x,y) = g_d(x)y^d + \ldots + g_0(x)$$

with coefficients $g_j(x) \in \mathbb{C}[x]$. If our coordinates are choosen general, then $d = \deg f$, a_d is a non-zero constant and $\deg g_j \leq d - j$. In that case we have counted with multiplicities precisely d solutions $(a,b) \in C$ for any given value $a \in \mathbb{C}$, and these solutions are distinct, iff the resultant $R(x) = Res(f, f_y)$ does not vanish at a. Moreover, the solutions depend continously on a. In particular, f has no isolated zeroes. In what follows we will not assume general coordinates. Then $g_d(x)$ might be a non-constant polynomial and some of the roots of $f(a,y)$ might approach infinity, if a approaches a zero of $g_d(x)$ in $\mathbb{A}^1(\mathbb{C}) = \mathbb{C}$. Let $B = \mathrm{V}(g_d(x)R(x)) \subset \mathbb{C}$. The projection onto the x-coordinate induces an unramified d sheeted covering

$$pr_1 : C \setminus pr_1^{-1}(B) \to \mathbb{C} \setminus B.$$

Since C has no isolated points, it suffices to prove that $C \setminus B$ is path connected. We will prove this with monodromy and Galois theory.

Let $p \in \mathbb{C} \setminus B$ be a base point. For each closed path

$$\gamma : [0,1] \to \mathbb{C} \setminus B \text{ with } \gamma(0) = \gamma(1) = p$$

and each preimage point $p_i \in \Gamma = pr_1^{-1}(p)$ path lifting defines a path $\gamma_i : [0,1] \to C \setminus pr_1^{-1}(B)$ which starts in $\gamma_i(0) = p_i$ and ends in a possibly different point $p_j = \gamma(1) \in \Gamma$. Thus, path lifting of γ induces a permutation

$$\mu(\gamma) : \Gamma \to \Gamma, \quad p_i \mapsto \gamma_i(1)$$

of Γ. We call the subgroup G, generated all permutations $\mu(\gamma)$ the **monodromy group** of the covering $pr_1 : C \setminus pr_1^{-1}(B) \to \mathbb{C} \setminus B$.

Path connectedness follows, if we can prove that G acts transitively on Γ. The key point is to identify G with a Galois group.

Consider the field extension $\mathbb{C}(x) \subset \mathbb{C}(x)[y]/\langle f \rangle$. Since f is irreducible, $\mathbb{C}[x,y]/\langle f \rangle$ is a domain, and $\mathbb{C}(x)[y]/\langle f \rangle$ is simply its quotient field. Let $K \supset \mathbb{C}(x)[y]/\langle f \rangle$ a splitting field of $f \in \mathbb{C}(x)[y]$. The splitting field K can be constructed explicitely as follows. Suppose that $p = 0 \in \mathbb{C}$ for notational convenience. We denote by $\mathbb{C}\{x\}$ the ring of convergent power series and by $\mathbb{C}\{x\}[x^{-1}] = Q(\mathbb{C}\{x\})$ the quotient field of meromorphic power series. We construct the splitting field of f over $\mathbb{C}(x)$ as a subfield of $\mathbb{C}\{x\}[x^{-1}]$. Let $p_i = (0, b_i) \in \Gamma$ be a point. By the Theorem on implicit functions , there exists an holomorphic power series $y_i(x) \in \mathbb{C}\{x\}$ with constant term $y_i(0) = b_i$, such that C near b_i equals the graph of y_i.

More precisely, there are $\epsilon, \delta > 0$, such that for

$$U_\epsilon(b_i) = \{y \in \mathbb{C} \mid |y - b_i| < \epsilon\} \text{ and } U_\delta(0) = \{x \in \mathbb{C} \mid |x| < \delta\},$$

we have

$$C \cap (U_\epsilon(b_i) \times U_\delta(0)) = \{(x, y_i(x)) \mid x \in U_\delta(0)\}.$$

Then

$$K \cong \mathbb{C}(x)[y_1(x), \ldots, y_d(x)] \subset \mathbb{C}\{x\}[x^{-1}],$$

indeed

$$f(x,y) = g_d(x)(y - y_1(x)) \cdot \ldots \cdot (y - y_d(x)).$$

We now consider the analytic continuation of our functions $y_i(x)$ along one of the closed path $\Gamma : [0,1] \to \mathbb{C} \setminus B$. This is possible, since for each point $\gamma(t)$ the implicit function theorem guarantees the existence of power serieses $y_{i,t}(x - \gamma(t)) \in \mathbb{C}\{x - \gamma(t)\}$, whose graphs parametrize C locally above $\gamma(t)$. For any t' in domain of convergence of the powerseries $y_{i,t}$, the function $y_{i,t}(x - \gamma(t))$ coincides with some $y_{i,t'}(x - \gamma(t'))$ in their common domain of definition, because both parametrize the same piece of C. At the end of

the path the analytic continuation ends up with the same set of power series $y_1(x), \ldots, y_d(x)$, however, possibly permuted. The permutation coincides with $\mu(\gamma)$.

We now claim, that each of these permutation induces an automorphism of the field K over $\mathbb{C}(x)$. Consider

$$\varphi : \mathbb{C}(x)[Y_1, \ldots, Y_d] \to K \subset \mathbb{C}\{x\}[x^{-1}], \quad Y_i \mapsto y_i(x).$$

To prove that $\sigma = \mu(\gamma)$ gives an automorhism of K, we have to show that for any $F \in \ker \varphi$ the function $F(y_{\sigma(1)}(x), \ldots, y_{\sigma(d)}(x)) = 0 \in K$. This follows from analytic continuation. The function $F(y_{1,t}(x - \gamma(t)), \ldots, y_{d,t}(x - \gamma(t)))$ stays identically zero by the identity theorem for functions in one complex variable . Thus G is a subset of the Galois group $\mathrm{Gal}(f)$ of f.

The Theorem follows, if we can prove that $G = \mathrm{Gal}(f)$, because the Galois group of an irreducible polynomial acts transitively on the roots. So the following theorem completes the proof. □

Theorem 6.7.2. *With notation as above, the monodromy group G coincides with the Galois group of f over $\mathbb{C}(x)$.*

Proof. Let $h \in K^G$ an invariant function. Then by the definition of G, the invarinat function h has a well-defined meromorphic continuation to $\mathbb{C} \setminus B$. Moreover, also in B and infinity, the continuation of h cannot have an essential singularity, because it is a polynomial function in the local roots $y_{i,t}(x - \gamma(t))$ with coefficients in $\mathbb{C}(x)$. Thus, h extend to a meromorphic function on $\mathbb{P}^1(\mathbb{C})$. So h is rational. This proves $K^G = \mathbb{C}(x)$, and hence $G = \mathrm{Gal}(K/\mathbb{C}(x)) = \mathrm{Gal}(f)$ by the main theorem of Galois theory.

□

Remark 6.7.3. The image of a closed path γ in G depends only on the homotopy class of γ. What we really have is an group homomorphism

$$\pi_1(\mathbb{C} \setminus B, p) \to \mathrm{Aut}(\Gamma).$$

Here we use the notation $\pi_1(X, p)$ for Poincaré's **fundamental group** of homotopy classes of closed loops in a topological space X with base point p, and $\mathrm{Aut}(\Gamma)$ denotes group of permutation group of the set Γ.

Thus to determine the image G, it suffices to apply path lifting to generators of $\pi_1(\mathbb{C} \setminus B, p)$. As it is well known , generators of $\pi_1(\mathbb{C} \setminus B)$ are small loops around each point of $b \in B$ connected via a path forwards and backwards to p.

This gives a numerical method to detect irreducibility of plane curves.

Corollary 6.7.4. *Any irreducible quasi-projective curve C over $\mathbb{C}$ is path connected with respect to the Euclidean topology.*

Proof. Consider a birational projection of C onto a plane curve C'. By the proof of the theorem, any non-empty Zariski open part of C' is path connected. Since we have an isomorphism of Zariski open parts of C' and C, and since C has no isolated points, C is path connected as well. □

Our next goal is to establishing the uniform position of a general hyperplane section of an irreducible curve. This may be considered as an appropriate version of our desired irreduciblity result in case of curves.

Definition 6.7.5. *Let $\Gamma = \{p_1, \ldots, p_d\} \subset \mathbb{P}^n$ be a collection of d distinct points. Γ is in* **linearly uniform position***, if any subset of n points of Γ spans a $\mathbb{P}^{n-1}$. Γ is in (arithmetically)* **uniform position***, if the homogeneous ideals of any two subsets of Γ with the same number of elements have the same Hilbert function. The arithmetically uniform position is the stronger statement.*

Our goal is to prove that the general hyperplane section of an irreducible curve $C \subset \mathbb{P}^{n+1}$ over a field $\Bbbk$ of characteristic 0 is in uniform position. The assertion is not true in positive characteristic.

Exercise 6.7.6. Consider the curve

$$\mathrm{V}(x_0^2 - x_1x_4, x_1^2 - x_2x_4, x_2^2 - x_3x_4) \subset \mathbb{P}^4$$

over a field of characteristic 2. Prove that the points of a general hyperplane section form the vertices of a cube. □

To prove uniform position, we treat the case $\Bbbk = \mathbb{C}$ first. Let $C \subset \mathbb{P}^n(\mathbb{C})$ be an irreducible curve of degree d. Consider the Zariski open set $U = \check{\mathbb{P}}^n \setminus \check{C}$ of transversal hyperplanes. U is path connected in the Euclidean topology. Pick a base point $H_0 \in U$ and consider the monodromy action of the fundamental group $\pi_1(U, H_0)$ on $\Gamma = C \cap H_0 = \{p_1, \ldots, p_d\}$ defined by path lifting: Let

$$\gamma : [0, 1] \to U,\ t \mapsto H_t$$

be a continuous path with $\gamma(0) = H_0$. Then by the continuity of roots of algebraic systems of equations there exist d continues paths

$$\gamma_i : [0, 1] \to C \text{ with } \gamma_i(0) = p_i,$$

such that $C \cap H_t = \{\gamma_1(t), \ldots, \gamma_d(t)\}$ for all t. Since all H_t intersect transversally, a loop in U starting and ending in H_0 induces a permutation of Γ:

$$\Gamma \to \Gamma,\ p_i = \gamma_i(0) \mapsto \gamma_i(1),$$

which in fact depends only on the homotopy class of the closed loop. Thus, if $\pi_1(U, H_0)$ denotes Poincaré fundamental group consisting of homotopy classes of closed loops starting and ending at H_0, we obtain a homomorphism

$$\mu : \pi_1(U, H_0) \to \mathrm{Aut}(\Gamma)$$

to the symmetric group of permutations of Γ.

Theorem 6.7.7 (Harris' Monodromy Theorem). *Let $C \subset \mathbb{P}^n(\mathbb{C})$ be an irreducible curve of degree d. The monodromy action of $\pi_1(U, H_0)$ on $\Gamma = C \cap H_0$ gives the full symmetric group.*

Proof. We assume that C is not a line. We have to prove that ρ is surjective. For this, it is enough to prove that $\pi_1(U, H_0)$ acts double transitive and that the image contains a simple transposition. Applying if necessary a birational projection we may assume $n = 2$. Since the double dual $\check{\check{C}} \cong C$ by 6.6.7, there are only finitely many tangents lines passing through any point $q \in \mathbb{P}^2$, and all but finitely many tangent lines are simple tangents, i.e. tangent in precisely one smooth point of C, which is not a flex.

Consider $C' = C \setminus C_{sing}$ and the fibers X_p of the incidence variety

$$X = \{(p, H) \in C' \times U | p \in C \cap H\} \to C'.$$

C' is path connected by Corollary 6.7.4 and all X_p are path connected, since they are Zariski open subset of a $\mathbb{P}^1$. So X is path connected, which implies that $\pi_1(U, H_0)$ acts transitively. To see double transitivity, we choose a smooth point $p \in C'$ and choose the base point H_0 in the fiber X_p. The image of $\pi(X_p, H_0)$ lies in the stabilizer of p. Since

$$C'' = \bigcup_{H \in X_p} (C \cap H \setminus \{p\})$$

is still path connected by Corollary 6.7.4, we obtaion double transitivity. To exhibit a simple transposition, we look at a general point $H_1 \in \check{C}$. Then $H_1 \cap C$ is tangent at precisely one point with multiplicity 2. A small loop in U near H_1 around $\check{C}$ will interchanges the two nearby intersection points and leaves the other $d - 2$ points unchanged. □

We denote with C^k the product $C \times C \times \ldots \times C$ and with $\Delta = \bigcup \Delta_{i,j}$ the union of the various diagonals.

Corollary 6.7.8. *The closure of $X_k = \{((p_1, \ldots, p_k), H) \in (C^k \setminus \Delta) \times U \mid \{p_1, \ldots, p_k\} \subset H \cap C\}$ in $C^k \times \check{\mathbb{P}}^n$ is irreducible for every k.*

Proof. X_k is non empty only for $k \leq d = \deg C$. It is path connected and irreducible, since we can connect any two points in the fiber of X_k over H_0 by a closed path in the smooth part of X_k according to Harris' Monodromy Theorem 6.7.7. □

Corollary 6.7.9. *The general hyperplane section $\Gamma \cap H$ of an irreducble curve lies in uniform position.*

Proof. Suppose that two subsets of Γ of the same cardinality k have different Hilbert functions. Since the values of the Hilbert function of a collection of points varies semicontineously with the points and H is general, this would give a decomposition of X_k into at least two components, a contradiction to Corollary 6.7.8. □

Remark 6.7.10. Much more general statements than Corollary 6.7.9 can be deduced. For example, the graded Betti numbers of the the image of any subset Γ_1 under the projection from the span of Γ_2 for disjoint subsets $\Gamma_1 \cup \Gamma_2 \subset \Gamma$ depend only on $\deg \Gamma_1$ and $\deg \Gamma_2$.

We now turn to arbitrary fields $\Bbbk$ of characteristic zero. First, if $X \subset \mathbb{P}^n$ is a quasi-projective algebraic set, then only finitely many coefficients occur in any finite set of defining equations of $\overline{X}$ and the complement $\overline{X} \setminus X$. The subfield $\Bbbk_0 \subset \Bbbk$ generated by these coefficients is a field of definition of X. Since $\Bbbk_0$ is a finitely generated field extension of $\mathbb{Q}$ and because $\mathbb{C}$ is algebraically closed with uncountable transcendence degree over $\mathbb{Q}$, there exists an embedding $\Bbbk \hookrightarrow \mathbb{C}$. Pick one and consider $X(\mathbb{C}) \subset \mathbb{P}^n(\mathbb{C})$. Then we apply

Lemma 6.7.11 (Lefschetz principle). *Let $\mathcal{P}$ be a property of algebraic sets which can be formulated by the solvability of a system of algebraic equations and inequalities with coefficients in the field of definition of X. If $X(\mathbb{C})$ satisfies $\mathcal{P}$ then $X(\overline{\Bbbk})$ satisfies $\mathcal{P}$, where $\overline{\Bbbk}$ denotes an algebraic closure of a field of definition of X.*

Proof. Clear, since we can embed $\Bbbk \hookrightarrow \mathbb{C}$. □

Let $C \subset \mathbb{P}^n$ be an absolutely irreducible curve over a field of characteristic zero. Let $U = \check{\mathbb{P}}^n \setminus \check{C}$ be the quasi-projective variety of transversal hyperplanes. For each k, the algebraic set $X_k = \{((p_1, \ldots, p_k), H) \in (C^k \setminus \Delta) \times U \mid \{p_1, \ldots, p_k\} \subset H \cap C\}$ in $C^k \times \check{\mathbb{P}}^n$ is absolutely irreducible, because it is irreducible over $\mathbb{C}$ by Corollary 6.7.8.

Corollary 6.7.12. *There exists a hyperplane $H \in U$ defined over the field of definition of C such that $\Gamma = C \cap H$ lies in uniform position in H.*

Proof. For each fixed t, the space of hyperplane H such that there exist two subsets Γ_1, Γ_2 of $C \cap H$ with the same number of points, but different values $h_{\Gamma_1}(t) \neq h_{\Gamma_2}(t)$, is a proper algebraic subset $B_t \subset U$ by Corollary 6.7.8 and the Lefschetz principle.

Since the Hilbert function $h_{\Gamma_1}(t)$ of a finite set of points takes value $\deg \Gamma_1$ for $t \geq \deg \Gamma_1$, there are only finitely many values t which we have to consider. Hence $B = \bigcup_{t \leq \deg \Gamma} B_t \subset U$ is an proper algebraic subset as well. (Without the bound for t, we would just conclude, that B is a countable union of proper algebraic subsets.) Therefore and because the field of definition $\Bbbk_0$ is infinite, the set of $\Bbbk_0$-rational points in $U \setminus B \subset \check{\mathbb{P}}^n$ is Zariski dense. □

To prove the irreducibilty of a general hyperplane section of a variety $X \subset \mathbb{P}^n$ of dimension $r \geq 2$, we consider the ground field $\mathbb{C}$ first, and start by extending the Mondromy Theorem 6.7.7 to this case.

Theorem 6.7.13. *Let $X \subset \mathbb{P}^n$ be a quasi-projective variety defined over $\mathbb{C}$. Then $X(\mathbb{C})$ is path connected.*

Proof. Adapt the proof of Theorem 6.7.1 and Corollary 6.7.4. □

Consider the Grassmannian

$$\mathbb{G} = \mathbb{G}(n-r+1, \mathbb{C}^{n+1}) = \{\mathbb{P}^{n-r} \subset \mathbb{P}^n\}$$

of complementary dimensional linear subspaces, see Exercise 6.3.39 for a definition of the Grassmannian as a projective variety. Let U be the open subset of transversal subspaces to X:

$$U = \{P \in \mathbb{G} \mid P \text{ intersects in } X \text{ in } d \text{ distinct points}\},$$

where $d = \deg X$. Pick a base point $P_0 \in U$ and consider the monodromy action of $\pi_1(U, P_0)$ on $\Gamma = X \cap P_0$.

Theorem 6.7.14. *Let $X \subset \mathbb{P}^n(\mathbb{C})$ be an irreducible variety of dimension r and degree d. The monodromy action of $\pi_1(U, P_0)$ on $\Gamma = X \cap P_0$ gives the full symmetric group.*

Proof. With minor modifications as before. □

Corollary 6.7.15. *Suppose* $\operatorname{char} \Bbbk = 0$. *A general hyperplane section $X \cap H$ of an irreducible variety $X \subset \mathbb{P}^n$ of dimension $r \geq 2$ is irreducible.*

Proof. We first consider the case $X \subset \mathbb{P}^n(\mathbb{C})$. Consider a flag $P_0 \subset H_0$ of a general complementary linear subspace P_0 and a general hyperplane H_0. By Berini's Theorem 6.6.1 H_0 intersects $X \setminus X_{sing}$ transversally. Suppose $X \cap H_0$ is reducible. Then every general hyperplane section is reducible. Since a loop

$$\gamma : [0,1] \to U, t \mapsto P_t$$

can be lifted to a loop of flags $t \mapsto (P_t, H_t)$ with P_t, H_t transversal to X, the monodromy action would distinguish between pairs of points in $X \subset P_0$, which do, respectively, which do not lie on the same irreducible component of $X \cap H_0$. This contradicts the Monodromy Theorem. Thus, $X \cap H_0$ is irreducible. For arbitrary fields of chararcteristic 0, the statement follows by applying the Lefschetz principle. □

Remark 6.7.16. As we see from the above, path lifting allows to establish an algorithmic test for absolute irreducibility of an algebraic set. Path lifting itself can be computed by numerical methods. An implementation numerical primary deomposition based on these ideas, has been developed by Sommese, Verschelde and Wampler, see Sommese, Wampler [2005].

Remark 6.7.17. A projective algebraic set $A \subset \mathbb{P}^n$ is called **non-degenerate**, if $I(A)$ contains no linear form, equivalently, if A spans $\mathbb{P}^n$. The study of **degenerate** algebraic sets can be reduced to non-degenerate ones by passing to a projective space of smaller dimension. The homogeneous coordinate ring of an non-degenerate algebraic set is generated by $n+1$ linear forms.

A **quasi-projective** variety W is a open subset of a projective variety, open with respect to the subspace topology. So $W = V \setminus A$, where V is a projective variety and $A \subset V$ an algebraic set. Quasi-projective varieties include both affine and projective varieties.

Graded modules over the polynomial are even better behaved then modules over a local ring.

Definition 6.7.18. *A* **graded ring** R *is a ring together with a decomposition*

$$R = \bigoplus_{d \geq 0} R_d,$$

such that the multplication respects the grading $R_d \times R_e \to R_{d+e}$. *A* **graded module** M *over* R *is a module together with a decomposition*

$$M = \bigoplus_{d \in \mathbb{Z}} M_d,$$

such that $R_d \times M_e \to M_{d+e}$. *We require, that homomorphisms of graded modules preseverve the degree.*

Example 6.7.19. $S = \Bbbk[x_0, \ldots, x_n]$ is a graded ring. A homogenous ideal I is a graded module, the quotient ring $R = S/I$ is another example of a graded ring. In particular, for $X \subset \mathbb{P}^n$ we have the homogeneous ideal $I = I_X = \mathrm{I}(X)$ of X and the homogeneous coordinate ring $R_X = S/I_X$ of X.

Lemma 6.7.20 (Lemma of Nakayama in the graded case). *Let* R *be a graded ring, and let* $R_{>0} = \bigoplus_{d>0} R_d$ *be the ideal of elements of positive degree. Let* $N \subset M$ *be finitely generated graded* R*-modules. If* $N + R_{>0}M = M$ *then* $N = M$.

Proof. Since N and M are finitely generated, $N_d = M_d = 0$ for $d \ll 0$. Suppose $N \subsetneq M$. Consider the smallest d such that $N_d \subsetneq M_d$. Suppose $m \in M_d \setminus N_d$. By assumption $m = n + \sum_i r_i m_i$ for $n \in N$, $r_i \in R_{>0}$ and $m_i \in M$. Since we have graded modules, we may assume that this equation is homogeneous, i.e. $n \in N_d$, $r_i \in R_{d_i}$ and $m_i \in M_{d-d_i}$. Since $d_i > 0$ we have $d - d_i < d$. Hence by induction hypothesis $m_i \in N_{d-d_i}$. Hence $m \in N$, a contradiction. □

Corollary 6.7.21. *If* R_0 *is a field and* M *a finitely generated graded* R *module. Then* $\dim_{R_0} M/R_{>0}M$ *is the minimal number of generators of* M. □

With respect to $S = \bigoplus S_d$, we are mainly concerned with the case where the graded piece S_0 is a field $\Bbbk$. Then S is a $\Bbbk$-algebra, which we call a **graded $\Bbbk$-algebra**. We usually assume that S is finitely generated as a $\Bbbk$-algebra. Then every finitely generated S-module M is Noetherian by Exercise 1.10.9, and the graded pieces M_d are *finite dimensional* $\Bbbk$-vector spaces. Their dimensions are important numerical invariants of M.

Our next topic is that of a minimal free resolution which makes equally sense over local rings and in the graded case. In fact, in both cases, we can apply Nakayama's lemma whose graded version is as follows (note that the *homogeneous* maximal ideal plays the role of the maximal ideal considered earlier):

If $S = \bigoplus S_d$ is a graded ring such that $S_0 = \Bbbk$ is a field, then S is a $\Bbbk = S/S_+$-algebra, and the graded pieces S_d are $\Bbbk$-vector spaces. We, then, say that S is a **graded $\Bbbk$-algebra**.