Plane Algebraic Curves

Andreas Gathmann

Class Notes RPTU Kaiserslautern 2026

– preliminary version –

Contents

0. Introduction

These notes are meant as a gentle introduction to *algebraic geometry*, a combination of *linear algebra* and *algebra*:

(a) In linear algebra (as e. g. in the "Foundations of Mathematics" class [G2]), we study systems of linear equations in several variables over a fixed ground field K.

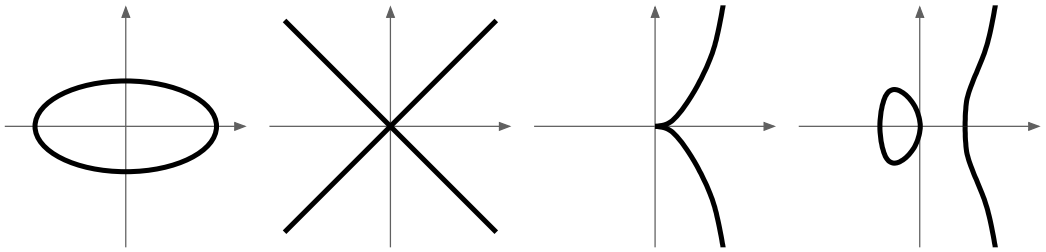
(b) In algebra (as e. g. in the "Algebraic Structures" or "Introduction to Algebra" classes [G1, G3]), a central topic are polynomials in one variable over K.

Algebraic geometry combines this by studying systems of polynomial equations in several variables over K. Of course, such polynomials in several variables occur in many places both in pure mathematics and in applications. Consequently, algebraic geometry has become a very large and active field of mathematics with deep connections to many other areas, such as commutative algebra, computer algebra, number theory, cryptography, topology, and complex analysis, just to name a few.

On the one hand, all these connections make algebraic geometry into a very interesting field to study – but on the other hand they may also make it hard for the beginner to get started. So to keep everything digestible, we will restrict ourselves here to the first case that is covered by neither (a) nor (b) above: *one polynomial equation in two variables*. Its set of solutions in K^2 can then be thought of as a curve in the plane, we can draw it (at least in the case $K = \mathbb{R}$), ask geometric questions about it, and try to answer them with algebraic methods. This restriction will significantly reduce the required theoretical background, but still leads to many interesting results that we will discuss in these notes.

To get a feeling for the kind of problems that one may ask about plane curves, we will now mention a few of them in this introductory chapter. Their flavor differs quite a bit depending on the chosen ground field K.

Example 0.1 (Curves over $\mathbb{R}$)**.** The following picture shows some real plane curves. Note that they can have many different "shapes": The curve (a) lies in a bounded region of the plane, whereas the others do not. The curve (b) consists of two components in the sense that it can be decomposed into two subsets (given by $x+y=0$ and $x-y=0$) that are given by polynomial equations themselves. The curve (c) has a so-called singularity at the origin, i. e. a point where it does not locally look like a smoothly deformed real line (in fact, (b) has a singularity at the origin as well). Finally, the image in (d) consists of two disconnected parts, but these parts are *not* given by separate polynomial equations themselves, as we will see in Exercise 1.8.



$\frac{x^2}{4}+y^2-1=0$ (a) $\quad x^2-y^2=0$ (b) $\quad y^2-x^3=0$ (c) $\quad y^2+x-x^3=0$ (d)

It is a main goal of algebraic geometry to prove such properties of curves just from looking at the polynomials, i. e. without drawing and referring to a picture (which would not be an exact proof anyway). Other related questions we might ask are: In how many points can two curves intersect? How many singularities can a curve have?

Example 0.2 (Curves over $\mathbb{C}$)**.** Over the complex numbers, pictures of curves will look different since a 1-dimensional complex object is real 2-dimensional, i. e. a surface. Note that we cannot draw such a surface as a subset of $K^2 = \mathbb{C}^2 = \mathbb{R}^4$ since we would need four dimensions for that. But we can still get a correct topological picture of the curve itself if we disregard this embedding. Let us show informally how to do this for the curve with the equation $y^2 + x - x^3 = 0$ as in Example 0.1 (d) above; for more details see **??**.

Note that in this case it is actually possible to write down all the points of the curve explicitly, because the given equation

$$y^2 = x^3 - x = x(x-1)(x+1)$$

is (almost) solved for y already: We can pick x to be any complex number, and then get two values for y, namely the two square roots of $x(x-1)(x+1)$ – unless $x \in \{-1,0,1\}$, in which case there is only one value for y (namely 0).

So one might think that the curve looks like two copies of the complex plane, glued together at the three points $-1,0,1$: The complex plane parametrizes the values for x, and the two copies of it correspond to the two possible values for y, i. e. to the two roots of the number $x(x-1)(x+1)$.

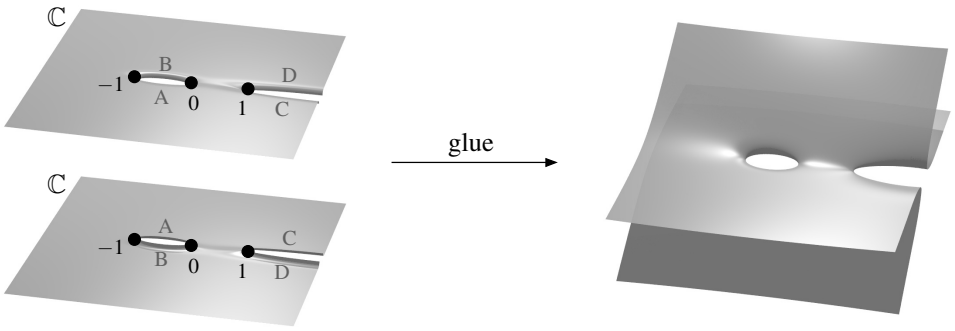
This is not the correct topological picture however, because a non-zero complex number does not have a distinguished first and second root that could correspond to the first and second copy of the complex plane. Rather, the two roots of a complex number get exchanged if we run around the origin once: If we consider a closed path

$$z = r\mathrm{e}^{\mathrm{i}\varphi} \qquad \text{for } 0 \leq \varphi \leq 2\pi \text{ and fixed } r > 0$$

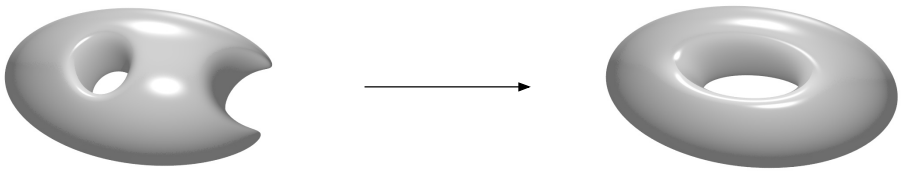
around the complex origin, the square root of this number would have to be defined by

$$\sqrt{z} = \sqrt{r}\mathrm{e}^{\frac{\mathrm{i}\varphi}{2}},$$

which gives opposite values at $\varphi = 0$ and $\varphi = 2\pi$. In other words, if x runs around one of the points $-1,0,1$ (i. e. around a point at which y is the square root of 0), we go from one copy of the plane to the other. One way to draw this topologically is to cut the two planes along the real intervals $(-1,0)$ and $(1,\infty)$, and to glue the two planes along these edges as in the following picture on the left, where edges with the same letter are meant to be identified. The gluing itself is then visualized best by first turning one of the planes upside down; this is shown in the picture on the right.

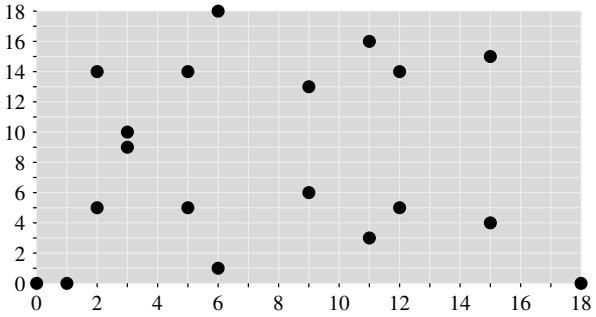


This is now actually a topologically correct picture of the given curve. To make the situation a little nicer, we can compactify it by adding a point at infinity, which corresponds to identifying the two planes at their infinitely far points as well (the precise construction will be described in Chapter 3). This is shown in the picture below, and leads topologically to a torus.



We will show in Proposition **??** how such topological pictures can be obtained immediately from the given equation of the curve.

Example 0.3 (Curves over finite fields)**.** Of course, over a finite field such as $\mathbb{Z}/p\mathbb{Z}$ for a prime number p, a curve just consists of finitely many points, and hence once again looks completely different. The following picture shows again the curve given by the equation $y^2+x-x^3=0$ as in our previous two examples, but this time over the ground field $\mathbb{Z}/19\mathbb{Z}$.



Note that we can still see the symmetry $y \leftrightarrow -y$ in the picture, but apart from that we just have a seemingly random collection of points. In fact, we will see in Example **??** that such curves have important applications in modern cryptography.

Example 0.4 (Curves over $\mathbb{Q}$)**.** The most famous application of algebraic geometry to ground fields other than just the real or complex numbers is probably Fermat's Last Theorem. This is the statement that, for $n \in \mathbb{N}_{\geq 3}$, the curve given by the equation $x^n+y^n-1=0$ *over the rational numbers* has only the trivial solutions where $x=0$ or $y=0$, or equivalently (by setting $x=\frac{a}{c}$ and $y=\frac{b}{c}$ for $a,b,c \in \mathbb{Z}$ with $c \neq 0$), that the equation $a^n+b^n=c^n$ has no non-trivial solutions over $\mathbb{Z}$ at all. Note that this picture is again very different from the cases of the other ground fields considered above. But as one might expect, a large part of the theory of algebraic curves works over arbitrary ground fields, and in fact the proof of Fermat's Last Theorem uses concepts of algebraic geometry in many places. So, in some sense, we can view (algebraic) number theory as a part of algebraic geometry.

Example 0.5 (Relations to complex analysis)**.** We have just seen in the examples above that algebraic geometry has deep relations to e. g. topology and number theory, and it should not come as a surprise that there are many relations to algebraic fields of mathematics such as commutative algebra and computer algebra as well. Although it is not within the scope of these notes, let us finish this introductory chapter by showing interesting relations to complex analysis as well.

Consider a (sufficiently nice) compactified complex curve, such as a torus as in Example 0.2. Of course, in algebraic geometry one does not only study curves for themselves but also maps between them; and hence we will have to consider "nice" functions on such curves (where "nice" will translate into "locally a quotient of polynomials"). What do such functions f look like if they are defined globally on the whole curve? As the curve is compact, note that the image of f must be a compact subset of the complex plane, which means that the absolute value $|f|$ must take a maximum somewhere. But locally the curve just looks like the complex plane, and by the Maximum Modulus Principle [G4, Proposition 6.14] the absolute value of a nice (read: holomorphic) function on the complex plane cannot have a local maximum unless it is constant. So we conclude that f must be a constant function: There are actually no non-trivial nice global functions on a compact curve.

In fact, we will prove this statement in Corollary **??** using only algebraic methods, and hence over arbitrary (algebraically closed) ground fields. In a similar way, many interesting results over the ground field $\mathbb{C}$ can be obtained using both algebraic geometry and complex analysis, with completely different methods, and thus give a close relation between these two branches of mathematics as well.

But let us now start with our study of plane curves. In order to keep these notes as accessible as possible, we will only assume a basic knowledge of groups, rings, and fields as about to the

extent of the "Algebraic Structures" class [G1], but a little more experience in dealing with these structures would certainly be advantageous. Very occasionally we will need to assume results from commutative algebra that go beyond these prerequisites (marked as "Facts" in the notes), but they will always be clearly stated and motivated, and provided with a reference. However, in order not to lose this very interesting part of the subject we will nevertheless quite frequently explore the relations of our results to other fields of mathematics in side remarks and excursions (that will then not be needed afterwards to follow the remaining parts of the notes).

1. Affine Curves

In this first chapter we will introduce plane curves both from an algebraic and a geometric point of view. As explained in the introduction, they will be given as solutions of polynomial equations. So let us start by fixing the corresponding notations.

Rings are always assumed to be commutative with a multiplicative neutral element 1. The multiplicative group of units of a ring R will be denoted by R^*.

Notation 1.1 (Polynomials)**.** Throughout these notes, K will always denote a fixed ground field. By $K[x_1,\dots,x_n]$ we will denote the *polynomial ring* in n variables $x_1,\dots,x_n$ over K, i. e. the ring of finite formal sums

$$f = \sum_{i_1,\dots,i_n\in\mathbb{N}} a_{i_1,\dots,i_n}\, x_1^{i_1}\cdot\dots\cdot x_n^{i_n}$$

with all $a_{i_1,\dots,i_n}\in K$ (see e. g. [G1, Chapter 9] how this concept of "formal sums" can be defined in a mathematically rigorous way). Note that we can regard it as an iterated univariate polynomial ring since $K[x_1,\dots,x_n] = K[x_1,\dots,x_{n-1}][x_n]$. Of course, for a polynomial f as above and a point $P=(c_1,\dots,c_n)\in K^n$, the *value* of f at P is defined as

$$f(P) := \sum_{i_1,\dots,i_n\in\mathbb{N}} a_{i_1,\dots,i_n}\, c_1^{i_1}\cdot\dots\cdot c_n^{i_n} \quad \in K.$$

Unless stated otherwise, the *degree* of a term $a_{i_1,\dots,i_n}\, x_1^{i_1}\cdot\dots\cdot x_n^{i_n}$ as above is meant to be the total degree $i_1+\dots+i_n$ in all variables together. The maximum degree occurring in a term with non-zero coefficient of a polynomial $f\neq 0$ is called the *degree* $\deg f$ of f. We call F *homogeneous* if all its terms have the same degree.

It is easy to see that $K[x_1,\dots,x_n]$ is an integral domain, and that $\deg(fg)=\deg f+\deg g$ holds for all non-zero polynomials f,g. The units of $K[x_1,\dots,x_n]$ are just the non-zero constant polynomials, which we can identify with $K^*=K\backslash\{0\}$.

Fact 1.2 (Factorial rings)**.** The polynomial ring $K[x_1,\dots,x_n]$ is a *factorial ring* (also called a *unique factorization domain*) [G6, Proposition 8.1 and Remark 8.4]. This means that prime and irreducible elements agree, and that every non-zero non-unit has a decomposition as a product of irreducible polynomials in a unique way (up to permutations, and up to multiplication with units). In the following, we will usually use this unique factorization property without mentioning. Note however that, as it is already the case for the integers $\mathbb{Z}$, performing such factorizations in $K[x_1,\dots,x_n]$ explicitly or even determining if a given polynomial is irreducible is usually hard.

Definition 1.3 (Affine varieties)**.**

(a) For $n\in\mathbb{N}$ we call $\mathbb{A}^n := \mathbb{A}^n_K := K^n$ the **affine n-space** over K.

It is customary to use the different notation $\mathbb{A}^n$ for K^n here since K^n is also a K-vector space and a ring. We will usually write $\mathbb{A}^n_K$ if we want to ignore these additional structures: For example, addition and scalar multiplication are defined on K^n, but not on $\mathbb{A}^n_K$. The affine space $\mathbb{A}^n_K$ will be the ambient space for our zero loci of polynomials below.

(b) For a subset $S\subset K[x_1,\dots,x_n]$ of polynomials we call

$$V(S) := \{P\in\mathbb{A}^n : f(P)=0 \text{ for all } f\in S\} \quad \subset \mathbb{A}^n$$

the (affine) **zero locus** of S. Subsets of $\mathbb{A}^n$ of this form are called **(affine) varieties**. If $S=\{f_1,\dots,f_k\}$ is a finite set, we will write $V(S)=V(\{f_1,\dots,f_k\})$ also as $V(f_1,\dots,f_k)$.

In these notes we will mostly restrict ourselves to zero loci of a single polynomial in two variables. We will then usually call these variables x and y instead of x_1 and x_2.

Remark 1.4. Obviously, for two polynomials $f, g \in K[x,y]$ we have ...

(a) $V(f) \cup V(g) = V(fg)$, as $fg(P) = 0$ for a point $P \in \mathbb{A}^2$ if and only if $f(P) = 0$ or $g(P) = 0$;

(b) $V(f) \cap V(g) = V(f,g)$ by definition.

One would probably expect now that a plane curve is just the zero locus of a polynomial in two variables. However, for our purposes it turns out to be more convenient to define a (plane) curve as such a polynomial itself rather than as its zero locus – this will simplify many statements and proofs later on when we want to study curves algebraically, i. e. in terms of their polynomials. Often, we will denote polynomials by capital instead of small letters if we want to think of them in this way. However, as it is obvious that two polynomials F and G with $F = \lambda G$ for some $\lambda \in K^*$ have the same zero locus (and thus determine the same geometric object), we incorporate this already in the definition of a curve:

Definition 1.5 (Affine curves)**.**

(a) An **(affine plane algebraic) curve** (over K) is a non-constant polynomial $F \in K[x,y]$ modulo units, i. e. modulo the equivalence relation $F \sim G$ if $F = \lambda G$ for some $\lambda \in K^*$. We will write it just as F, not indicating this equivalence class in the notation – this will not lead to any confusion.

We call $V(F) = \{P \in \mathbb{A}^2 : F(P) = 0\}$ the **set of points** of F.

(b) The **degree** of a curve is its degree as a polynomial. Curves of degree $1, 2, 3, \dots$ are usually referred to as **lines**, **quadrics/conics**, **cubics**, and so on.

(c) A curve F is called **irreducible** if it is as a polynomial, and **reducible** otherwise. Similarly, if $F = {F_1}^{a_1} \cdot \dots \cdot {F_k}^{a_k}$ is the irreducible decomposition of F as a polynomial (see Fact 1.2), we will also call this the **irreducible decomposition** of the curve F. The curves $F_1, \dots, F_k$ are then called the **(irreducible) components** of F and $a_1, \dots, a_k$ their **multiplicities**.

A curve F is called **reduced** if all its irreducible components have multiplicity 1.

Remark 1.6.

(a) Obviously, the notions of Definition 1.5 are well-defined, i. e. they do not change when multiplying a polynomial with a unit in K^*. All our future constructions with curves will also have this property, and it will be equally obvious in all these cases as well. In the following, we will therefore not mention this fact any more.

(b) In the literature, a curve often refers to the set of points $V(F)$ as in Definition 1.5 (a), i. e. to the geometric object in $\mathbb{A}^2$ rather than to the polynomial F.

Example 1.7. Especially in the case of the ground field $K = \mathbb{R}$, we will usually visualize a curve F by drawing its set of points $V(F)$ in the plane – although this does not contain the full information on the curve, as we will see below.

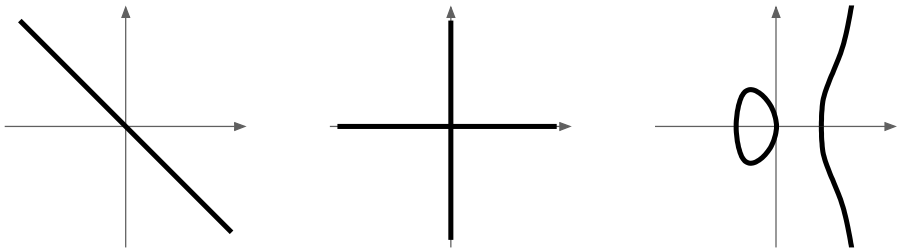
(a) The curve $x + y$ is a line, and hence irreducible (as a polynomial of degree 1 cannot be a product of two non-constant polynomials). Its square $(x+y)^2$ has the same set of points as $x + y$, but it is a quadric. It is neither irreducible nor reduced.

More generally, it is obvious that curves with the same irreducible components, just with different multiplicities, have the same set of points.

(b) The quadric xy is reducible as well, but it is reduced since it has two irreducible components x and y of multiplicity 1.

(c) In contrast to its appearance (see the picture below), the cubic $F = y^2 + x - x^3$ is irreducible: If we had $F = GH$ for some non-constant G and H, and thus $V(F) = V(G) \cup V(H)$ by Remark 1.4 (a), then one of these factors would have to be a line and the other one a quadric. But F does not contain a line as we can see from the picture.

(d) The set of points of the real curve $F = x^2 + y^2 + 1$ is empty, but by our definition F is nevertheless a curve – and also different from the curve $x^2 + y^2 + 2$, whose set of points is also empty. If we consider F over the complex numbers however, it has a non-empty set of points, but it is hard to visualize as it lies in $\mathbb{A}^2_{\mathbb{C}} = \mathbb{A}^4_{\mathbb{R}}$.



(a) (b) (c)

Exercise 1.8. Prove algebraically that the curve $y^2 + x - x^3$ of Example 1.7 (c) is irreducible.

Even if we defined a curve to be a polynomial (modulo scalars), we would of course rather like to think of it as a geometric object in $\mathbb{A}^2$ as in the pictures in Examples 0.1 or 1.7. For the rest of this chapter we will therefore study to what extent the set of points $V(F)$ determines back F, i. e. whether we can "draw $V(F)$ in the plane to specify F". We have already seen two reasons why this does not work in general:

- If a curve F is non-reduced as in Example 1.7 (a), we cannot determine the multiplicities on its components from $V(F)$.
- If (as in the case $K = \mathbb{R}$) there are non-constant polynomials without zeros, the set of points $V(F)$ might be empty as in Example 1.7 (d), and thus does not determine back F.

We now want to see that these are essentially the only two problems that can arise, and simultaneously prove that the intersection of two curves without a common component is finite. For this, we need two algebraic prerequisites.

Remark 1.9 (Algebraically closed fields)**.** A field K is called *algebraically closed* if every non-constant polynomial $F \in K[x]$ in one variable has a zero. The most prominent example is clearly $K = \mathbb{C}$ [G4, Proposition 6.20] – but it can be shown that every field is contained in an algebraically closed one, so that considering only curves over algebraically closed fields would not be a serious restriction. In fact, many textbooks on algebraic geometry restrict to this case altogether. In these notes however we will at least develop the general theory for arbitrary ground fields up to Chapter **??** in order not to exclude e. g. the geometrically most intuitive case of real curves from the very beginning.

Note that any algebraically closed field is necessarily infinite: If $K = \{c_1, \ldots, c_n\}$ was finite, the polynomial $F = \prod_{i=1}^{n}(x - c_i) + 1$ would have no zero.

Construction 1.10 (Quotient fields)**.** For any integral domain R, there is an associated *quotient field*

$$\operatorname{Quot} R = \left\{ \frac{a}{b} : a, b \in R \text{ with } b \neq 0 \right\},$$

where the "fraction" $\frac{a}{b}$ denotes the equivalence class of the pair (a, b) under the relation

$$(a, b) \sim (a', b') \;\Leftrightarrow\; ab' = a'b.$$

It is in fact a field with the standard addition and multiplication rules for fractions. The ring R is then a subring of $\operatorname{Quot} R$ by identifying $a \in R$ with $\frac{a}{1} \in \operatorname{Quot} R$ [G6, Example 6.5 (b)].

The easiest example is $R = \mathbb{Z}$, in which case we just have $\operatorname{Quot} R = \mathbb{Q}$. For our purposes the most important example is the polynomial ring $R = K[x_1, \ldots, x_n]$, for which $\operatorname{Quot} R$ is denoted $K(x_1, \ldots, x_n)$ and called the *field of rational functions* over K. Note that, despite its name, its elements are not defined as functions, but rather as formal quotients of polynomials as e. g. $\frac{x_1 + x_2}{x_1 - x_2} \in K(x_1, x_2)$. They do, however, define functions on the subset of $\mathbb{A}^n$ where the denominator is non-zero.

Lemma 1.11. *Let F be an affine curve.*

(a) *If K is algebraically closed then $V(F)$ is infinite.*

(b) *If K is infinite then $\mathbb{A}^2_K \setminus V(F)$ is infinite.*

Proof. As F is not a constant polynomial, it has positive degree in at least one of the variables x and y. By symmetry we may assume that this is x, so that $F = a_n x^n + \cdots + a_0$ for some $a_0, \ldots, a_n \in K[y]$ with $n > 0$ and $a_n \neq 0$.

Being non-zero, the polynomial $a_n \in K[y]$ has only finitely many zeros. But K is in any case infinite by Remark 1.9, hence there are infinitely many $y \in K$ with $a_n(y) \neq 0$. For each such y, the polynomial $F(x,y)$ is non-constant in x, so in case (a) there is an $x \in K$ with $F(x,y) = 0$, and in case (b) there is an $x \in K$ with $F(x,y) \neq 0$ (as $F(\cdot, y)$ has only finitely many zeros). □

01

Proposition 1.12 (Finiteness of the intersection of curves)**.** *Let F and G be two curves without a common component.*

(a) *The ideal $\langle F, G \rangle$ in $K[x,y]$ contains a non-zero polynomial that depends only on x (and hence by symmetry also a non-zero polynomial that depends only on y).*

(b) *The intersection $V(F,G)$ of the two curves is finite.*

Proof.

(a) By assumption, F and G are coprime in $K[x,y]$. We claim that they are then also coprime in $K(x)[y]$. In fact, if they had a common factor in $K(x)[y]$ then after clearing denominators we would have $aF = HF'$ and $aG = HG'$ for some $H, F', G' \in K[x,y]$ and non-zero $a \in K[x]$, where H has a positive y-degree. But then every irreducible factor of a must divide H or both F' and G' in $K[x,y]$. So by replacing H or both F' and G' by these quotients we arrive at a new decomposition $F = HF'$ and $G = HG'$ with $H, F', G' \in K[x,y]$ and H of positive y-degree, in contradiction to F and G being coprime in $K[x,y]$.

Now the ring $K(x)[y]$ as a univariate polynomial ring over a field $K(x)$ is a principal ideal domain [G1, Example 10.23]. So as $F, G \in K(x)[y]$ are coprime we can write 1 as a linear combination of F and G with coefficients in $K(x)[y]$ [G1, Proposition 10.13 (b)], which means after clearing denominators again that $c = DF + EG$ for some $D, E \in K[x,y]$ and a non-zero $c \in K[x]$. Hence, $c \in \langle F, G \rangle$ is a non-zero polynomial that depends only on x.

(b) Continuing the above notation, if $P \in V(F,G)$ we have $c(P) = D(P)F(P) + E(P)G(P) = 0$. This restricts the x-coordinate of all points $P \in V(F,G)$ to the finitely many zeros of c. By symmetry, we then also have only finitely many choices for the y-coordinate, i. e. $V(F,G)$ is finite. □

Corollary 1.13. *Let F be a curve over an algebraically closed field. Then for any irreducible curve G we have*

$$G \mid F \;\Leftrightarrow\; V(G) \subset V(F).$$

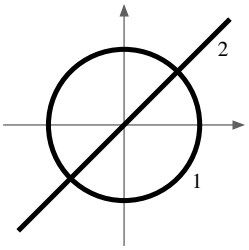
In particular, the irreducible components of F (but not their multiplicities, see Example 1.7 (a)) can be recovered from $V(F)$.

Proof.

"⇒" Assume that $F = GH$ for some curve H. If $P \in V(G)$, i. e. $G(P) = 0$, then we also have $F(P) = G(P)H(P) = 0$, and hence $P \in V(F)$.

"⇐" Now assume that $V(G) \subset V(F)$. Then $V(F,G) = V(G)$ is infinite by Lemma 1.11 (a). By Proposition 1.12 (b) this means that F and G must have a common component. As G is irreducible, this is only possible if $G \mid F$. □

Remark 1.14 (Specifying a curve by its set of points)**.** By Corollary 1.13, over an algebraically closed field we can specify a curve by giving its set of points together with a multiplicity on each irreducible component. For example, the picture on the right (where the circle has radius 1 and the numbers at the components are their multiplicities) represents the curve $(x^2+y^2-1)(x-y)^2$. (Note however that this is a real picture, but Corollary 1.13 would only hold over $\mathbb{C}$.)



If we do not specify multiplicities in a picture, we usually mean the corresponding reduced curve, i. e. where all multiplicities are 1.

Notation 1.15. Due to the above correspondence between a curve F and its set of points $V(F)$, we will sometimes write:

(a) $P \in F$ instead of $P \in V(F)$, i. e. $F(P) = 0$ ("P lies on the curve F");

(b) $F \cap G$ instead of $V(F,G)$ for the points that lie on both F and G;

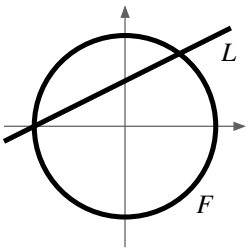
(c) $F \cup G$ for the curve FG (see Remark 1.4 (a));

(d) $G \subset F$ instead of $G \mid F$.

Exercise 1.16 (Pythagorean triples in algebraic geometry)**.** Let $F = x^2+y^2-1 \in K[x,y]$ be the "unit circle" over K. Assume that the characteristic of K is not 2, i. e. that $1+1 \neq 0$ in K.

(a) Considering the intersection points of an arbitrary line L (with slope t) through $(-1,0)$ with F, show that the set of points of F is

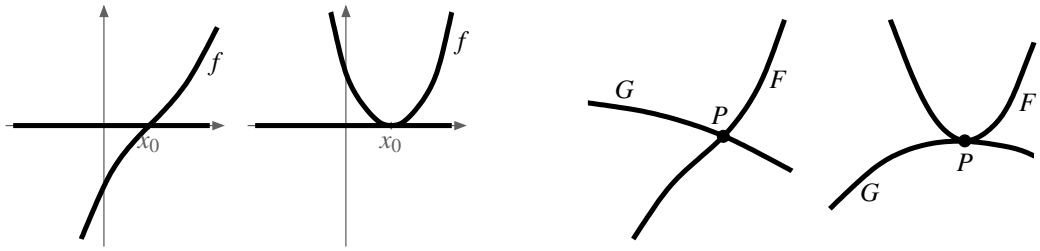
$$V(F) = \{(-1,0)\} \cup \left\{ \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right) : t \in K \text{ with } 1+t^2 \neq 0 \right\}.$$



(b) Using (a), prove that the integer solutions (a,b,c) of the equation $a^2+b^2=c^2$ (the so-called Pythagorean triples) are, up to a permutation of a and b, exactly the triples of the form $\lambda(u^2-v^2, 2uv, u^2+v^2)$ with $\lambda, u, v \in \mathbb{Z}$.

2. Intersection Multiplicities

Let us start our study of curves by introducing the concept of intersection multiplicity, which will be central throughout these notes. It generalizes the well-known notion of multiplicity of a zero of a univariate polynomial: If $f \in K[x]$ is a polynomial and $x_0 \in K$ such that $f = (x-x_0)^m g$ for a polynomial $g \in K[x]$ with $g(x_0) \neq 0$, then f is said to have multiplicity m at x_0. As in the following two pictures on the left, a zero of multiplicity 1 means that the graph of f intersects the x-axis transversely, whereas in the case of multiplicity (at least) 2 it is tangent to it. Roughly speaking, higher multiplicities would correspond to graphs for which the x-axis is an even better approximation around x_0.



multiplicity 1 at x_0 $f = (x-x_0)\,g$ | multiplicity 2 at x_0 $f = (x-x_0)^2\,g$ | multiplicity 1 at P | multiplicity 2 at P

In this geometric interpretation, we have considered how the graph of f intersects the horizontal axis locally at the given point, i. e. how the two curves $F = y - f$ and $G = y$ intersect. As in the picture above on the right, this concept should thus also make sense for arbitrary curves F and G at an intersection point P: If they intersect transversely, i. e. with different tangent directions, we want to say that they have an intersection multiplicity of 1 at P, whereas equal tangents correspond to higher multiplicities. But of course, the curves F and G might also have "singularities" as e. g. the origin in Example 0.1 (b) and (c), in which case it is not clear a priori how their intersection multiplicity can be interpreted or even defined.

So our first task must be to actually construct the intersection multiplicity for arbitrary curves. For this we need the following algebraic object that allows us to capture the local geometry of the plane around a point.

Definition 2.1 (Local rings of $\mathbb{A}^2$)**.** Let $P \in \mathbb{A}^2$ be a point.

(a) The **local ring** of $\mathbb{A}^2$ at P is defined as

$$\mathscr{O}_P := \mathscr{O}_{\mathbb{A}^2,P} := \left\{ \frac{f}{g} : f,g \in K[x,y] \text{ with } g(P) \neq 0 \right\} \quad \subset K(x,y).$$

(b) It admits a well-defined ring homomorphism

$$\mathscr{O}_P \to K,\ \frac{f}{g} \mapsto \frac{f(P)}{g(P)}$$

which we will call the **evaluation map**. Its kernel will be denoted by

$$I_P := I_{\mathbb{A}^2,P} := \left\{ \frac{f}{g} : f,g \in K[x,y] \text{ with } f(P) = 0 \text{ and } g(P) \neq 0 \right\} \quad \subset \mathscr{O}_P.$$

Remark 2.2 (Geometric and algebraic interpretation of local rings)**.** Intuitively, $\mathscr{O}_P$ describes "nice" (i. e. rational) functions that have a well-defined value at P (determined by the evaluation map), and thus also in a neighborhood of P. Note however that $\mathscr{O}_P$ does not admit similar evaluation maps

at other points $Q \neq P$ since the denominator of the fractions might vanish there. This explains the name "local ring" from a geometric point of view. The ideal I_P in $\mathcal{O}_P$ describes exactly those local functions that have the value 0 at P.

Algebraically, $\mathcal{O}_P$ is a subring of $K(x,y)$ that contains $K[x,y]$. As a subring of a field it is an integral domain, and its units are precisely the fractions $\frac{f}{g}$ for which both f and g are non-zero at P. Moreover, just like $K[x,y]$ it is a factorial ring, with the irreducible elements being the irreducible polynomials that vanish at P (since the others have become units).

For those who know some commutative algebra we should mention that $\mathcal{O}_P$ is also a local ring in the algebraic sense, i. e. that it contains exactly one maximal ideal, namely I_P [G6, Definition 6.9]: If I is any ideal in $\mathcal{O}_P$ that is not a subset of I_P then it must contain an element $\frac{f}{g}$ with $f(P) \neq 0$ and $g(P) \neq 0$. But this is then a unit since $\frac{g}{f} \in \mathcal{O}_P$ as well, and hence we have $I = \mathcal{O}_P$.

In fact, in the algebraic sense $\mathcal{O}_P$ is just the localization of the polynomial ring $K[x,y]$ at the maximal ideal $\langle x - x_0, y - y_0 \rangle$ associated to the point $P = (x_0, y_0)$ – which also shows that it is a local ring [G6, Corollary 6.10].

Definition 2.3 (Intersection multiplicities)**.** For a point $P \in \mathbb{A}^2$ and two curves (or polynomials) F and G we define the **intersection multiplicity** of F and G at P to be

$$\mu_P(F,G) := \dim \mathcal{O}_P/\langle F,G\rangle \quad \in \mathbb{N} \cup \{\infty\},$$

where dim denotes the dimension as a vector space over K.

As this definition is rather abstract, we should of course figure out how to compute this number, what its properties are, and why it captures the geometric idea given above. In fact, it is not even clear whether $\mu_P(F,G)$ is finite. But let us start with a few simple statements and examples.

Remark 2.4.

(a) It is clear from the definitions that an invertible *affine coordinate transformation* from (x,y) to

$$(x',y') = (ax+by+c, dx+ey+f) \quad \text{for } a,b,c,d,e,f \in K \text{ with } ae-bd \neq 0$$

gives us an isomorphism between the local rings $\mathcal{O}_P$ and $\mathcal{O}_{P'}$, where P' is the image point of P; and between $\mathcal{O}_P/\langle F,G\rangle$ and $\mathcal{O}_{P'}/\langle F',G'\rangle$, where F' and G' are F and G expressed in the new coordinates x' and y'. We will often use this invariance to simplify our calculations by picking suitable coordinates, e. g. such that $P = 0$ is the origin.

(b) The intersection multiplicity is symmetric: We have $\mu_P(F,G) = \mu_P(G,F)$ for all F and G.

(c) For all F,G,H we have $\langle F, G+FH\rangle = \langle F,G\rangle$, and thus $\mu_P(F,G+FH) = \mu_P(F,G)$.

In Definition 2.3, we have not required a priori that P actually lies on both curves F and G. However, the intersection multiplicity is at least 1 if and only if it does:

Lemma 2.5. *Let $P \in \mathbb{A}^2$, and let F and G be two curves (or polynomials). We have:*

(a) $\mu_P(F,G) \geq 1$ *if and only if* $P \in F \cap G$*;*

(b) $\mu_P(F,G) = 1$ *if and only if* $\langle F,G\rangle = I_P$ *in* $\mathcal{O}_P$*.*

Proof. Assume first that $F(P) \neq 0$. Then F is a unit in $\mathcal{O}_P$, and thus $\langle F,G\rangle = \mathcal{O}_P$, i. e. $\mu_P(F,G) = 0$. Moreover, we then have $P \notin F$ and $F \notin I_P$, proving both (a) and (b) in this case. Of course, the case $G(P) \neq 0$ is analogous.

So we may now assume that $F(P) = G(P) = 0$, i. e. $P \in F \cap G$. Then the evaluation map at P induces a well-defined and surjective map $\mathcal{O}_P/\langle F,G\rangle \to K$. It follows that $\mu_P(F,G) \geq 1$, proving (a) in this case. Moreover, we have $\mu_P(F,G) = 1$ if and only if this map is an isomorphism, i. e. if and only if $\langle F,G\rangle$ is exactly the kernel I_P of the evaluation map. □

Example 2.6 (Intersection multiplicity of coordinate axes)**.** The kernel I_0 of the evaluation map at 0 consists exactly of the fractions $\frac{f}{g}$ such that f does not have a constant term, which is just the ideal $\langle x,y\rangle$ in $\mathscr{O}_0$. By Lemma 2.5 (b) this means that $\mu_0(x,y) = 1$, i. e. (as expected) that the two coordinate lines have intersection multiplicity 1 at the origin.

Regarding the finiteness of the intersection multiplicity, the following two exercises show that $\mu_P(F,G)$ is finite if and only if F and G do not have a common component through P. This should not come as a surprise since an infinite intersection multiplicity should mean that the two curves "touch at P to infinite order", i. e. that they agree locally around P in the irreducible case, resp. share a common component in the general case. By Remark 2.4 (a) it suffices to consider the case when $P = 0$ is the origin.

Exercise 2.7 (Finiteness of the intersection multiplicity)**.** Let F and G be two curves without a common component that passes through the origin. Show:

(a) There is a number $n \in \mathbb{N}$ such that $x^n = y^n = 0$ in $\mathscr{O}_0/\langle F,G\rangle$.

(b) Every element of $\mathscr{O}_0/\langle F,G\rangle$ has a polynomial representative.

(c) $\mu_0(F,G) < \infty$.

Exercise 2.8 (Infinite intersection multiplicities)**.** Let F and G be two curves that pass through the origin. Show:

(a) If F and G have no common component then the family $(F^n)_{n\in\mathbb{N}}$ is linearly independent in $\mathscr{O}_0/\langle G\rangle$.

(b) If F and G have a common component that passes through the origin then $\mu_0(F,G) = \infty$.

For the last important basic property of intersection multiplicities we first need another easy algebraic tool.

Construction 2.9 (Short exact sequences)**.** We say that a sequence

$$0 \longrightarrow U \xrightarrow{\varphi} V \xrightarrow{\psi} W \longrightarrow 0$$

of linear maps between vector spaces (where 0 denotes the zero vector space) is **exact** if the image of each map equals the kernel of the next, i. e. if

(a) $\ker\varphi = 0$ (i. e. φ is injective);

(b) $\operatorname{im}\varphi = \ker\psi$; and

(c) $\operatorname{im}\psi = W$ (i. e. ψ is surjective).

In this case, we get a dimension formula

$$\begin{aligned}\dim U + \dim W &\overset{\text{(a),(c)}}{=} \dim\operatorname{im}\varphi + \dim\operatorname{im}\psi = \dim\operatorname{im}\varphi + \dim V/\ker\psi \overset{\text{(b)}}{=} \dim\operatorname{im}\varphi + \dim V/\operatorname{im}\varphi\\ &= \dim V.\end{aligned}$$

Proposition 2.10 (Additivity of intersection multiplicities)**.** *Let $P \in \mathbb{A}^2$, and let F,G,H be any three curves (or polynomials).*

(a) *If F and G have no common component through P there is an exact sequence*

$$0 \longrightarrow \mathscr{O}_P/\langle F,H\rangle \xrightarrow{\cdot G} \mathscr{O}_P/\langle F,GH\rangle \xrightarrow{\pi} \mathscr{O}_P/\langle F,G\rangle \longrightarrow 0,$$

where π is the natural quotient map.

(b) *We have $\mu_P(F,GH) = \mu_P(F,G) + \mu_P(F,H)$.*

Proof.

(a) We may assume that F and G have no common component at all, since components that do not pass through P are units in $\mathscr{O}_P$ and can therefore be dropped in the ideals.

It is checked immediately that both non-trivial maps in this sequence are well-defined, and that conditions (b) and (c) of Construction 2.9 hold. Hence we just have to show that the first multiplication map is injective: Assume that $\frac{f}{g}$ is in the kernel of this map, i. e. that

$$\frac{f}{g} \cdot G = \frac{f'}{g'} \cdot F + \frac{f''}{g''} \cdot GH$$

for certain $f', f'', g', g'' \in K[x,y]$ with $g'(P)$ and $g''(P)$ non-zero. We may assume without loss of generality that all three fractions have the same denominator, and multiply by it to obtain the equation $fG = f'F + f''GH$ in $K[x,y]$. Now G clearly divides fG and $f''GH$, hence also $f'F$, and consequently f' as F and G have no common component. So we have $f' = aG$ for some $a \in K[x,y]$, and we see that $fG = aFG + f''GH$. Dividing by G, it follows that $f = aF + f''H$, so that f and hence also $\frac{f}{g}$ are zero in $\mathcal{O}_P/\langle F,H \rangle$. This shows the injectivity of the first map.

(b) If F and G have no common component through P the statement follows immediately from (a) by taking dimensions as in Construction 2.9. Otherwise the equation is true as $\infty = \infty$ by Exercise 2.8 (b). □

02

Touching the mathematical field of computer algebra, we are now ready to explicitly compute the intersection multiplicity $\mu_P(F,G)$ of two arbitrary curves F and G at a point P where they do not have a common component. By Remark 2.4 (a) it suffices to do this at the origin $P = 0$. Let us start with the simple case when one of the curves is the horizontal axis; this will be needed in the general algorithm afterwards.

Example 2.11 (Intersection multiplicity with the horizontal axis)**.** Let F be an affine curve that does not contain the horizontal axis y. We want to compute the intersection multiplicity $\mu_0(y,F)$ with this axis at the origin.

By Remark 2.4 (c) we may remove all multiples of y from F, i. e. replace F by the polynomial $F(x,0) \in K[x]$, which is not the zero polynomial since y is not a component of F. We can write $F(x,0) = x^m g$ where $g \in K[x]$ is non-zero at the origin, so that m is the multiplicity of 0 in $F(x,0)$. Hence we obtain

$$\begin{aligned}
\mu_0(y,F) &= \mu_0(y,F(x,0)) && \text{(Remark 2.4 (c))} \\
&= \mu_0(y,x^m g) && \\
&= m\,\mu_0(y,x) + \mu_0(y,g) && \text{(Proposition 2.10 (b))} \\
&= m && \text{(Example 2.6 and Lemma 2.5 (a)).}
\end{aligned}$$

Note that this coincides with the expectation from the beginning of this chapter: If $f \in K[x]$ is a univariate polynomial with a zero x_0 of multiplicity m (which is just $x_0 = 0$ in our current case) then the intersection multiplicity of its graph $y - f$ with the x-axis at the point $(x_0, 0)$ is m.

Algorithm 2.12 (Computation of the intersection multiplicity $\mu_0(F,G)$)**.** Let F and G be two curves (or polynomials) without common component through the origin. We then repeat the following procedure recursively to compute the intersection multiplicity $\mu_0(F,G)$:

(a) If $F(0) \neq 0$ or $G(0) \neq 0$, i. e. if one of the curves does not pass through the origin, we stop with $\mu_0(F,G) = 0$ by Lemma 2.5 (a).

(b) Otherwise, if F and G both contain a monomial independent of y, we write

$$\begin{aligned}
F &= ax^m + (\text{terms involving } y \text{ or with a lower power of } x), \\
G &= bx^n + (\text{terms involving } y \text{ or with a lower power of } x)
\end{aligned}$$

for some $a, b \in K^*$ and $m, n \in \mathbb{N}_{>0}$, where we may assume (by possibly swapping F and G) that $m \geq n$. Similarly to a standard polynomial long division we then set

$$F' := F - \frac{a}{b} x^{m-n} G,$$

hence canceling the x^m-term in F. By Remark 2.4 (c) we then have $\mu_0(F,G) = \mu_0(F',G)$, so we can replace F by F' (which also passes through the origin) and repeat this step (b). As this procedure makes the number $m+n$ strictly smaller in each step, we will eventually arrive at a situation with one of the polynomials not having a monomial independent of y, leading to the final case:

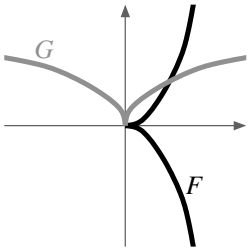
(c) If one of the polynomials F and G, say F, does not contain a monomial independent of y, we can factor $F = yF'$ and obtain by Proposition 2.10 (b)

$$\mu_0(F,G) = \mu_0(y,G) + \mu_0(F',G).$$

In this expression, the multiplicity $\mu_0(y,G)$ can be computed directly by Example 2.11: It is the lowest power of x in a term of G independent of y. Note that this number is non-zero as $G(0) = 0$. Hence we have $\mu_0(F',G) < \mu_0(F,G)$; so if we now repeat the algorithm recursively to compute $\mu_0(F',G)$ it will terminate in finitely many steps.

Example 2.13. Let us compute the intersection multiplicity $\mu_0(F,G)$ at the origin of the two curves $F = y^2 - x^3$ and $G = x^2 - y^3$ as in the picture below on the right. We follow Algorithm 2.12 and indicate which step we performed each time:

$$\begin{aligned}
\mu_0(y^2-x^3, x^2-y^3) &\overset{\text{(b)}}{=} \mu_0(y^2 - x^3 + x(x^2-y^3), x^2-y^3) \\
&= \mu_0(y^2 - xy^3, x^2-y^3) \\
&\overset{\text{(c)}}{=} \underbrace{\mu_0(y, x^2-y^3)}_{=2 \text{ by } 2.11} + \mu_0(y - xy^2, x^2-y^3) \\
&\overset{\text{(c)}}{=} 2 + \underbrace{\mu_0(y, x^2-y^3)}_{=2 \text{ by } 2.11} + \underbrace{\mu_0(1-xy, x^2-y^3)}_{=0 \text{ by (a)}} \\
&= 4.
\end{aligned}$$



Remark 2.14 (Curves with common components)**.** If F and G have a common component through 0, Algorithm 2.12 still performs correct computations, but it might not terminate. For example, for the curves $F = x^2$ and $G = xy - x$ with common component x it yields

$$\begin{aligned}
\mu_0(x^2, xy-x) &\overset{\text{(b)}}{=} \mu_0(x^2 + x(xy-x), xy-x) \\
&= \mu_0(x^2 y, xy-x) \\
&\overset{\text{(c)}}{=} \underbrace{\mu_0(y, xy-x)}_{=1 \text{ by } 2.11} + \mu_0(x^2, xy-x),
\end{aligned}$$

leading to an infinite loop. However, if for arbitrary given F and G it does terminate with a finite answer, then by Exercise 2.8 (b) we have proven simultaneously with this computation that F and G have no common component through the origin. In contrast, if the algorithm does not seem to terminate we will find in Remark **?? ??** a rigorous way to decide whether F and G have a common component through 0.

Exercise 2.15. Draw the real curves $F = x^2 + y^2 + 2y$ and $G = y^3x^6 - y^6x^2$, determine their irreducible decompositions, their intersection points, and their intersection multiplicities at these points.

Following our algorithm, we can now also give an easy and important criterion for when the intersection multiplicity is 1.

Notation 2.16 (Homogeneous parts of polynomials)**.** For a polynomial $F \in K[x,y]$ of degree d and $i = 0,\dots,d$, we define the *degree-i part* of F to be the sum of all terms of F of degree i. Hence all F_i are homogeneous, and we have $F = F_0 + \cdots + F_d$. We call F_0 the *constant part*, F_1 the *linear part*, and F_d the *leading part* of F.

Proposition 2.17 (Intersection multiplicity 1)**.** *Let F and G be two curves (or polynomials) through the origin. Then $\mu_0(F,G) = 1$ if and only if the linear parts F_1 and G_1 are linearly independent.*

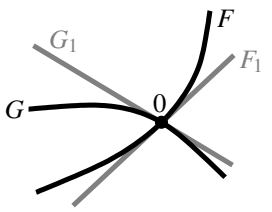
Proof. We prove the statement following Algorithm 2.12, using the notation from there.

By assumption F and G pass through the origin, so we are not in case (a) of the algorithm. In case (b), note that F_1' and G_1 are linearly independent if and only if F_1 and G_1 are, as either $F_1' = F_1$ (if $m > n$) or $F_1' = F_1 - \frac{a}{b}G_1$ (if $m = n$). Hence we can consider the first time we reach case (c). As $\mu_0(y, G) > 0$ we then have

$$\begin{aligned}
\mu_0(F,G) = 1 &\Leftrightarrow \mu_0(y,G) = 1 \text{ and } \mu(F',G) = 0 \\
&\Leftrightarrow G \text{ contains a monomial } x^1y^0 \text{ and } F' \text{ contains a constant term} \\
&\qquad \text{(by Example 2.11 and Lemma 2.5 (a))} \\
&\Leftrightarrow G_1 = ax + by \text{ for some } a \in K^*, b \in K, \text{ and } F_1 = cy \text{ for some } c \in K^* \\
&\Leftrightarrow F_1 \text{ and } G_1 \text{ are linearly independent,}
\end{aligned}$$

where the last implication "$\Leftarrow$" follows since $F = yF'$ clearly does not contain a monomial x^1y^0. □

In fact, Proposition 2.17 has an easy geometric interpretation in the spirit of the beginning of this chapter: F_1 and G_1 can be thought of as the linear approximations of F and G around the origin. If these approximations are non-zero, hence lines, they can be thought of as the tangents to the curves as in the picture on the right, and the proposition states that the intersection multiplicity is 1 if and only if these tangent directions are not the same.



In general, it is the lowest non-zero terms of a curve F that can be considered as the best local approximation of F around 0. We can use this idea to define tangents to arbitrary curves (i. e. even if the linear approximation F_1 vanishes) as follows.

Definition 2.18 (Tangents and multiplicities of points)**.** Let F be a curve.

(a) The smallest $m \in \mathbb{N}$ for which the homogeneous part F_m is non-zero is called the **multiplicity** $m_0(F)$ of F at the origin. Any linear factor of F_m (considered as a curve) is called a **tangent** to F at the origin.

(b) For a general point $P = (x_0, y_0) \in \mathbb{A}^2$, tangents at P and the multiplicity $m_P(F)$ are defined by first shifting coordinates to $x' = x - x_0$ and $y' = y - y_0$, and then applying (a) to the origin $(x', y') = (0, 0)$.

Exercise 2.19. Given a linear coordinate transformation that maps the origin to itself and a curve F to F', show that $m_0(F) = m_0(F')$, and that the transformation maps any tangent of F to a tangent of F'. In particular, despite its appearance, Definition 2.18 is independent of the choice of coordinates on $\mathbb{A}^2$.

By definition, we clearly have $m_P(F) > 0$ if and only if $P \in F$. The most important case of Definition 2.18 is then $m_P(F) = 1$, i. e. if there is a non-zero local linear approximation for F around P. There is a special terminology for this case.

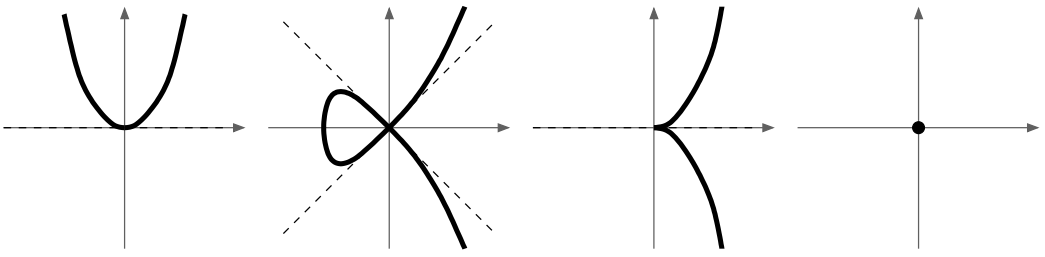
Definition 2.20 (Smooth and singular points)**.** Let F be a curve.

(a) A point $P \in F$ is called **smooth** or **regular** if $m_P(F) = 1$. Note that F has then a unique tangent at P, which we will denote by T_PF. For $P = 0$, it is simply given by the linear part F_1 of F.

If P is not a smooth point, i. e. if $m_P(F) > 1$, we say that P is a **singular** point or a **singularity** of F. As a special case, a singularity with $m_P(F) = 2$ such that F has (exactly) two different tangents there is called a **node**.

(b) The curve F is said to be **smooth** or **regular** if all its points are smooth. Otherwise, F is called **singular**.

Example 2.21. Let us consider the origin in the real curves in the following picture.



For the case (a), the curve $F = y - x^2$ in (a) has (no constant but) a linear term y. Hence, we have $m_0(F) = 1$, the origin is a smooth point of the curve, and its tangent there is $T_0F = y$.

For the other three curves, the origin is a singular point of multiplicity 2. In (b), this singularity is a node, since the quadratic term is $y^2 - x^2 = (y-x)(y+x)$, and thus we have the two tangents $y-x$ and $y+x$, shown as dashed lines in the picture. The curve in (c) has only one tangent y which is of multiplicity 2. Finally, in (d) there is no tangent at all since x^2+y^2 does not contain a linear factor over $\mathbb{R}$. Note that, in any case, knowing the tangents of F at the origin (which are easy to compute) tells us to some extent what the curve looks like locally around 0.

With these notations we can now reformulate Proposition 2.17.

Corollary 2.22 (Transverse intersections)**.** *Let P be a point in the intersection of two curves F and G. Then $\mu_P(F,G) = 1$ if and only if P is a smooth point of both F and G, and $T_PF \neq T_PG$.*

*We say in this case that F and G intersect **transversely** at P.*

Remark 2.23 (Additivity of point multiplicities)**.** Note that $m_P(FG) = m_P(F) + m_P(G)$. Hence, any point that lies on at least two (not necessarily distinct) irreducible components has multiplicity at least 2, and is thus a singular point. In particular, all points on a component of multiplicity at least 2 (in the sense of Definition 1.5 (c)) are always singular.

To check if a given curve F is smooth, i. e. whether every point $P \in F$ is a smooth point of F, there is a simple criterion that does not require to shift P to the origin first. It uses the (partial) derivatives $\frac{\partial F}{\partial x}$ and $\frac{\partial F}{\partial y}$ of F, which can be defined purely formally over an arbitrary ground field and then satisfy the usual rules of differentiation [G1, Exercise 9.10].

Proposition 2.24 (Affine Jacobi Criterion)**.** *Let $P = (x_0, y_0)$ be a point on an affine curve F.*

(a) *P is a singular point of F if and only if $\frac{\partial F}{\partial x}(P) = \frac{\partial F}{\partial y}(P) = 0$.*

(b) *If P is a smooth point of F the tangent to F at P is given by*

$$T_PF = \frac{\partial F}{\partial x}(P) \cdot (x - x_0) + \frac{\partial F}{\partial y}(P) \cdot (y - y_0).$$

Proof. Substituting $x = x' + x_0$ and $y = y' + y_0$, i. e. $x' = x - x_0$ and $y' = y - y_0$, we can consider F as a polynomial in x' and y'. If we expand

$$F = ax' + by' + (\text{higher order terms in } x' \text{ and } y'),$$

then by definition F is singular at $(x', y') = (0,0)$, i. e. at P, if and only if $a = b = 0$. But by the chain rule of differentiation we have

$$a = \frac{\partial F}{\partial x'}(0) = \frac{\partial F}{\partial x}(P) \quad \text{and} \quad b = \frac{\partial F}{\partial y'}(0) = \frac{\partial F}{\partial y}(P),$$

so that (a) follows. Moreover, if F is smooth at P then its tangent is just the term of F linear in x' and y', i. e.

$$ax' + by' = \frac{\partial F}{\partial x}(P) \cdot (x - x_0) + \frac{\partial F}{\partial y}(P) \cdot (y - y_0),$$

as claimed in (b). □

Example 2.25. Consider again the real curve $F = y^2 - x^2 - x^3$ from Example 2.21 (b). To determine its singular points, we compute the partial derivatives

$$\frac{\partial F}{\partial x} = -2x - 3x^2 \quad \text{and} \quad \frac{\partial F}{\partial y} = 2y.$$

Its common zeros are $(0,0)$ and $(-\frac{2}{3},0)$. But the latter does not lie on the curve, and so we conclude that the origin is the only singular point of F.

Smoothness of a curve F at a point P has another important algebraic consequence: It means that the containment of ideals containing F in $\mathcal{O}_P$ (or in other words of ideals in $\mathcal{O}_P/\langle F \rangle$) can be checked by a simple comparison of intersection multiplicities.

Proposition 2.26 (Comparing ideals using intersection multiplicities)**.** *Let P be a smooth point on a curve F. Then for any two curves G and H that do not have a common component with F through P we have*

$$\langle F,G \rangle \subset \langle F,H \rangle \text{ in } \mathcal{O}_P \quad \Leftrightarrow \quad \mu_P(F,G) \geq \mu_P(F,H).$$

In particular, we have $\langle F,G \rangle = \langle F,H \rangle$ in $\mathcal{O}_P$ if and only if $\mu_P(F,G) = \mu_P(F,H)$.

03

Proof.

"⇒": Clearly, if $\langle F,G \rangle \subset \langle F,H \rangle$ then $\mu_P(F,G) = \dim \mathcal{O}_P/\langle F,G \rangle \geq \dim \mathcal{O}_P/\langle F,H \rangle = \mu_P(F,H)$.

"⇐": Let L be a line through P which is not the tangent T_PF. Then $\mu_P(F,L) = 1$ by Corollary 2.22, and hence $\mu_P(F,L^n) = n$ for all $n \in \mathbb{N}$ by Proposition 2.10.

As for the curves G and H, let us consider only G first and derive an alternative description of the intersection multiplicity $\mu_P(F,G)$: Let $n \in \mathbb{N}$ be the maximal with $\langle F,G \rangle \subset \langle F,L^n \rangle$ in $\mathcal{O}_P$. This maximum exists since $\langle F,G \rangle \subset \mathcal{O}_P = \langle F,L^0 \rangle$, and $\langle F,G \rangle \subset \langle F,L^n \rangle$ requires $n \leq \mu_P(F,G)$ by the direction "⇒" that we have already shown.

We claim that then $\langle F,G \rangle = \langle F,L^n \rangle$ in $\mathcal{O}_P$, i. e. that $L^n \in \langle F,G \rangle$. To see this, note that $\langle F,G \rangle \subset \langle F,L^n \rangle$ implies $G = aF + bL^n$ for some $a,b \in \mathcal{O}_P$. If we had $b(P) = 0$ it would follow that $b \in I_P = \langle F,L \rangle$ by Lemma 2.5 (b), i. e. $b = cF + dL$ for some $c,d \in \mathcal{O}_P$, which means that $G = aF + (cF + dL)L^n \in \langle F,L^{n+1} \rangle$ and thus contradicts the maximality of n. Hence $b(P) \neq 0$, i. e. b is a unit in $\mathcal{O}_P$, and we obtain $L^n = \frac{1}{b}(G - aF) \in \langle F,G \rangle$ as desired.

Of course, now $\langle F,G \rangle = \langle F,L^n \rangle$ implies that $\mu_P(F,G) = \mu_P(F,L^n) = n$, so that we obtain $\langle F,G \rangle = \langle F,L^{\mu_P(F,G)} \rangle$.

But the same holds for H instead of G, and so the inequality $\mu_P(F,G) \geq \mu_P(F,H)$ yields

$$\langle F,G \rangle = \langle F,L^{\mu_P(F,G)} \rangle \subset \langle F,L^{\mu_P(F,H)} \rangle = \langle F,H \rangle. \qquad \square$$

Example 2.27. Proposition 2.26 is false without the smoothness assumption on F: For the real curve $F = x^2 - y^2 = (x-y)(x+y)$ (i. e. the union of the two diagonals in $\mathbb{A}^2$, with singular point 0), $G = x$, and $H = y$, we have $\langle F,G \rangle = \langle x,y^2 \rangle$ and $\langle F,H \rangle = \langle y,x^2 \rangle$. Hence $\mu_0(F,G) = \mu_0(F,H) = 2$, but $\langle F,G \rangle \neq \langle F,H \rangle$ (since $y \notin \langle x,y^2 \rangle$, as otherwise we would have $\langle x,y^2 \rangle = \langle x,y \rangle$, in contradiction to $\mu_0(x,y^2) = 2 \neq 1 = \mu_0(x,y)$).

Remark 2.28 (Geometric interpretation of smooth curves)**.** Mainly for the ground field $K = \mathbb{R}$, our results on smooth curves have an intuitive interpretation:

(a) The Jacobi Criterion of Proposition 2.24 (a) states that P is a smooth point of a real curve F if and only if the Implicit Function Theorem [G2, Proposition 27.10] can be applied to the equation $F = 0$ around P, so that $V(F)$ is a 1-dimensional submanifold of $\mathbb{R}^2$ [G2, Definition 27.18]. Hence, in this case $V(F)$ is locally the graph of a differentiable function (expressing y as a function of x or vice versa), and thus we arrive at the intuitive interpretation of smoothness as "having no sharp corners".

(b) To interpret Proposition 2.26, let us continue the picture of (a) and consider a local (analytic) coordinate z around P on the 1-dimensional manifold $V(F)$. In accordance with the idea of intersection multiplicity at the beginning of this chapter, a curve G should have intersection multiplicity n with F at P if on F it is locally a function of the form az^n in this coordinate, with a a non-zero function at P (corresponding to a unit in $\mathcal{O}_P$). Now if $n = \mu_P(F,G) \geq \mu_P(F,H) = m$ then in the same way H is of the form bz^m for a function b non-zero at P, so that $bz^m = H$ divides $az^n = G$. This means that $\langle G \rangle \subset \langle H \rangle$ in $\mathcal{O}_P/\langle F \rangle$ (i. e. as functions on F, a point of view that we will discuss in detail starting in Chapter **??**) and thus that $\langle F,G \rangle \subset \langle F,H \rangle$ in $\mathcal{O}_P$.

(c) In fact, the analytic idea of (b) has a direct counterpart in commutative algebra that can then be applied over arbitrary ground fields: For a smooth curve F the ring $\mathcal{O}_P/\langle F \rangle$ is a so-called *discrete valuation ring* (see e. g. [G6, Chapter 12]; we will also consider this concept briefly later on in Proposition **??**). This means that the non-zero elements of this ring have a valuation – a natural number that can be interpreted as the order of the zero as a function on F, and hence as the local intersection multiplicity with F. It is then a result in commutative algebra that the non-zero ideals in a discrete valuation ring are in one-to-one correspondence with these valuations as above [G6, Corollary 12.17]. This is precisely the statement of Proposition 2.26.

Exercise 2.29 (Cusps)**.** Let P be a point on an affine curve F. We say that P is a **cusp** if $m_P(F) = 2$, there is exactly one tangent L to F at P, and $\mu_P(F,L) = 3$.

(a) Give an example of a real curve with a cusp, and draw a picture of it.

(b) If F has a cusp at P, prove that F has only one irreducible component passing through P.

(c) If F and G have a cusp at P, what is the minimum possible value for the intersection multiplicity $\mu_P(F,G)$?

Exercise 2.30.

(a) Find all singular points of the curve $F = (x^2+y^2-1)^3 + 10x^2y^2 \in \mathbb{R}[x,y]$, and determine the multiplicities and tangents to F at these points.

(b) Show that an irreducible curve F over a field of characteristic 0 has only finitely many singular points.

Can you find weaker assumptions on F that also imply that F has only finitely many singular points?

(c) Show that an irreducible cubic can have at most one singular point, and that over an algebraically closed field this singularity must be a node or a cusp as in Exercise 2.29.

3. Projective Curves

In the last chapter we have studied the local intersection behavior of curves. Our next major goal will be to consider the global situation and ask how many intersection points two curves can have in total, i. e. how many common zeros we find for two polynomials $F, G \in K[x,y]$ (where we will count each such zero with its intersection multiplicity).

For polynomials in one variable, the corresponding question would simply be how many zeros a single polynomial $f \in K[x]$ has. At least if K is algebraically closed, so that f is a product of linear factors, the answer is then of course that we always get $\deg f$ zeros (counted with multiplicities). Hence, in our current case of two polynomials $F, G \in K[x,y]$ we would also hope for a result that depends only on $\deg F$ and $\deg G$, and not on the chosen polynomials.

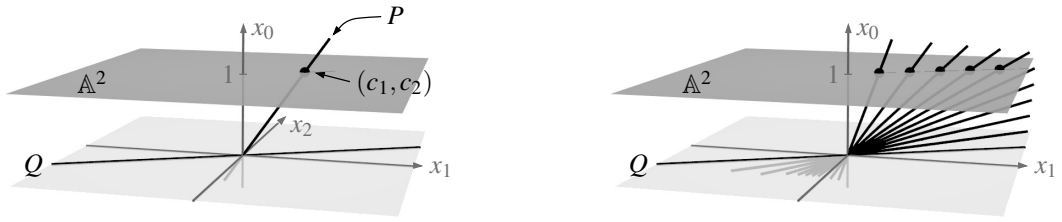
However, even in the simplest case when F and G are two distinct lines this will not work, since F and G might intersect in one point or be parallel (and hence have no intersection point). To fix this situation, the geometric idea is to add points at infinity to the affine plane $\mathbb{A}^2$, so that two lines that are parallel in $\mathbb{A}^2$ will meet there. On the other hand, two non-parallel lines (that intersect already in $\mathbb{A}^2$) should not meet at infinity any more as this would then lead to two intersection points. Hence, we have to add one point at infinity for each direction in the affine plane, so that parallel lines with the same direction meet there, whereas others do not.

This new space with the added points at infinity will be called the *projective plane*. In the case $K = \mathbb{R}$ we can also think of it as a compactification of the affine plane $\mathbb{A}^2$. It is the goal of this chapter to study this process in detail, leading to plane curves that are "compactified" by points at infinity. For two such compactified curves we will then compute the number of intersection points in the next chapter, and the answer will then indeed depend only on the degrees of the curves.

Remark 3.1 (Geometric idea of projective spaces)**.** Algebraically, the idea for adding points at infinity is to embed the affine space $\mathbb{A}^n$ in the vector space K^{n+1} by prepending a new coordinate (typically called x_0) equal to 1, i. e. by the map

$$\mathbb{A}^n \to K^{n+1},\ (x_1,\dots,x_n) \mapsto (1,x_1,\dots,x_n),$$

and considering the 1-dimensional linear subspace in K^{n+1} spanned by this vector. For example, in this way a point $(c_1,c_2) \in \mathbb{A}^2$ corresponds to the line through the origin and $(1,c_1,c_2) \in K^3$, denoted by P in the picture below on the left.



We will define the projective plane as the set of all such 1-dimensional linear subspaces of K^3. It then consists of all lines through the origin coming from points of $\mathbb{A}^2$ as above – together with lines contained in the plane where $x_0 = 0$ that do not arise in this way, such as Q in the picture above. As shown on the right, these lines can be thought of as limits of lines coming from an unbounded sequence of points in $\mathbb{A}^2$. They can therefore be interpreted as the "points at infinity" that we were looking for.

Let us now turn this idea into a precise definition.

Definition 3.2 (Projective spaces)**.** For $n \in \mathbb{N}$, we define the **projective n-space** over K as the set of all 1-dimensional linear subspaces of K^{n+1}. It is denoted by $\mathbb{P}^n_K$ or simply $\mathbb{P}^n$.

Notation 3.3 (Homogeneous coordinates)**.** Obviously, a 1-dimensional linear subspace of K^{n+1} is uniquely determined by a spanning non-zero vector in K^{n+1}, with two such vectors giving the same linear subspace if and only if they are scalar multiples of each other. In other words, we have

$$\mathbb{P}^n = (K^{n+1} \backslash \{0\}) / \sim$$

with the equivalence relation

$$(x_0, \dots, x_n) \sim (y_0, \dots, y_n) \quad :\Leftrightarrow \quad x_i = \lambda y_i \text{ for some } \lambda \in K^* \text{ and all } i.$$

The equivalence class of $(x_0, \dots, x_n)$ is usually denoted by $(x_0 : \dots : x_n) \in \mathbb{P}^n$. We call $x_0, \dots, x_n$ the **homogeneous** or **projective coordinates** of the point $(x_0 : \dots : x_n)$. Hence, in this notation for a point in $\mathbb{P}^n$ the numbers $x_0, \dots, x_n$ are not all zero, and they are defined only up to a common scalar multiple.

Remark 3.4 (Geometric interpretation of $\mathbb{P}^n$)**.** There are two ways to interpret the projective space $\mathbb{P}^n$ geometrically:

(a) As in Remark 3.1, we can embed the affine space $\mathbb{A}^n$ in $\mathbb{P}^n$ by the map

$$\mathbb{A}^n \to \mathbb{P}^n, \ (x_1, \dots, x_n) \mapsto (1 : x_1 : \dots : x_n)$$

whose image is the subset $U_0 := \{(x_0 : \dots : x_n) : x_0 \neq 0\}$ of $\mathbb{P}^n$. We will often consider $\mathbb{A}^n$ as a subset of $\mathbb{P}^n$ in this way, i. e. by setting $x_0 = 1$. The other coordinates $x_1, \dots, x_n$ are then called the **inhomogeneous** or **affine coordinates** on U_0.

The remaining points of $\mathbb{P}^n$ are of the form $(0 : x_1 : \dots : x_n)$. By forgetting their coordinate x_0 (which is zero anyway) they form a set that is naturally bijective to $\mathbb{P}^{n-1}$, corresponding to the 1-dimensional linear subspaces of K^n. As in Remark 3.1 we can regard them as *points at infinity*; there is hence one such point for each direction in K^n. In short-hand notation, one often writes this decomposition as $\mathbb{P}^n = \mathbb{A}^n \cup \mathbb{P}^{n-1}$ and calls $\mathbb{A}^n$ and $\mathbb{P}^{n-1}$ the *affine* and *infinite part* of $\mathbb{P}^n$, respectively.

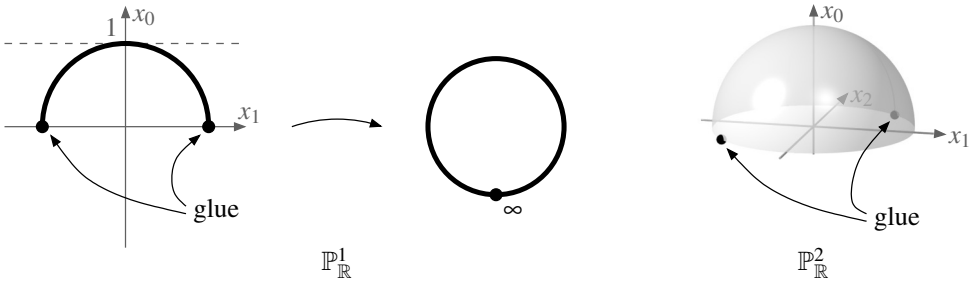
(b) By the symmetry of the homogeneous coordinates, the subsets $U_i := \{(x_0 : \dots : x_n) : x_i \neq 0\}$ of $\mathbb{P}^n$ are naturally bijective to $\mathbb{A}^n$ for all $i = 0, \dots, n$, in the same way as for $i = 0$ in (a). As every point of $\mathbb{P}^n$ has at least one non-zero coordinate, it lies in one of the U_i, and hence in a subset of $\mathbb{P}^n$ that just looks like the ordinary affine space $\mathbb{A}^n$. In this sense we can say that projective space "looks everywhere the same"; the fact that we interpreted the points with $x_0 = 0$ as points as infinity above was just due to our special choice of $i = 0$ in (a).

Example 3.5. By Remark 3.4 (a), we have $\mathbb{P}^1 = \mathbb{A}^1 \cup \mathbb{P}^0$. The affine part consists of the points $(1 : x_1)$ for $x_1 \in K$, and the infinite part contains the single point $(0 : 1)$. Denoting this point at infinity by ∞, we can therefore write $\mathbb{P}^1 = \mathbb{A}^1 \cup \{\infty\}$.

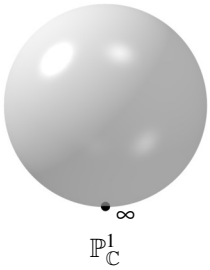
Remark 3.6 (Topology of projective spaces over $\mathbb{R}$ and $\mathbb{C}$)**.** Over the real or complex numbers, every point in $\mathbb{P}^n$ has a representative on the unit sphere $\{(x_0, \dots, x_n) : |x_0|^2 + \dots + |x_n|^2 = 1\}$ by normalizing. In other words, $\mathbb{P}^n$ can be written as the image of this compact unit sphere under the quotient map $(x_0, \dots, x_n) \mapsto (x_0 : \dots : x_n)$. In accordance with our motivation at the beginning of this chapter, this means that $\mathbb{P}^n$ is itself compact (with the quotient topology [G5, Definition 5.3 and Corollary 5.8 (c)]).

(a) For $K = \mathbb{R}$, every 1-dimensional linear subspace of K^{n+1} meets the unit sphere in exactly two points, which are negatives of each other. Hence, all points $(x_0 : \dots : x_n) \in \mathbb{P}^n$ have a representative on the upper half of the unit sphere, i. e. where $x_0 \geq 0$, and this representative is unique except for points on its boundary where $x_0 = 0$ (i. e. for points at infinity). As in the following picture, we can therefore visualize $\mathbb{P}^n_{\mathbb{R}}$ as the space obtained from the upper half unit sphere by identifying opposite points on the boundary. For $n = 1$ we have only one pair of gluing points, corresponding to one point at infinity as in Example 3.5, and obtain

topologically a circle. For $n = 2$, each point on the boundary of the upper half unit sphere has to be identified with its negative, which leads to a space that cannot be embedded in $\mathbb{R}^3$.



(b) For $K = \mathbb{C}$, only $\mathbb{P}^1_{\mathbb{C}}$ can be visualized in $\mathbb{R}^3$. By Example 3.5 it is just the complex plane together with a point ∞. It is therefore topologically a sphere as in the picture on the right.



Having studied projective spaces, we now want to consider subsets of $\mathbb{P}^n$ given by polynomial equations. However, polynomials in homogeneous coordinates are not well-defined functions on $\mathbb{P}^n$: For example, for the polynomial $f = x_0^2 + x_1$ we have $f(1,-1) = 0$ and $f(-1,1) = 2$ although $(1:-1) = (-1:1) \in \mathbb{P}^1$. We can solve this problem by using homogeneous polynomials as follows.

Remark 3.7. Let

$$f = \sum_{i_0+\cdots+i_n=d} a_{i_0,\ldots,i_n}\, x_0^{i_0} \cdot \cdots \cdot x_n^{i_n} \quad \in K[x_0,\ldots,x_n]$$

be a homogeneous polynomial of degree d. Then

$$f(\lambda x_0,\ldots,\lambda x_n) = \sum_{i_0+\cdots+i_n=d} a_{i_0,\ldots,i_n}\, \lambda^{i_0+\cdots+i_n} x_0^{i_0} \cdot \cdots \cdot x_n^{i_n} = \lambda^d f(x_0,\ldots,x_n)$$

for all $\lambda \in K$. In particular, we see:

(a) Although f is not a well-defined function on $\mathbb{P}^n$, its zero locus is well-defined on $\mathbb{P}^n$, i. e. we have

$$f(\lambda x_0,\ldots,\lambda x_n) = 0 \quad \Leftrightarrow \quad f(x_0,\ldots,x_n) = 0$$

for all $\lambda \in K^*$. In the following, we will therefore write this condition simply as $f(P) = 0$ for $P = (x_0 : \cdots : x_n)$.

(b) If g is another homogeneous polynomial of degree d then

$$\frac{f(\lambda x_0,\ldots,\lambda x_n)}{g(\lambda x_0,\ldots,\lambda x_n)} = \frac{\lambda^d f(x_0,\ldots,x_n)}{\lambda^d g(x_0,\ldots,x_n)} = \frac{f(x_0,\ldots,x_n)}{g(x_0,\ldots,x_n)},$$

and so the quotient $\frac{f}{g}$ is a well-defined function on the subset of $\mathbb{P}^n$ where g does not vanish.

04

Definition 3.8 (Projective varieties)**.** For a subset $S \subset K[x_0,\ldots,x_n]$ of homogeneous polynomials we call

$$V(S) := \{P \in \mathbb{P}^n : f(P) = 0 \text{ for all } f \in S\} \quad \subset \mathbb{P}^n$$

the (projective) **zero locus** of S. Subsets of $\mathbb{P}^n$ that are of this form are called **(projective) varieties**. If $S = \{f_1,\ldots,f_k\}$ is a finite set, we will write $V(S) = V(\{f_1,\ldots,f_k\})$ also as $V(f_1,\ldots,f_k)$. To distinguish the projective from the affine zero locus of Definition 1.3 (b), we will sometimes denote it by $V_{\mathrm{p}}(S) \subset \mathbb{P}^n$ as opposed to $V_{\mathrm{a}}(S) \subset \mathbb{A}^{n+1}$.

In this class we will mostly restrict ourselves to the case of the projective plane $\mathbb{P}^2$. We will then usually denote the homogeneous coordinates by x, y, and z, with z corresponding to the variable x_0 defining the points at infinity as in Remark 3.4 (a).

Remark 3.9. The properties of Remark 1.4 hold analogously for the projective zero locus: For any two homogeneous polynomials $f, g \in K[x,y,z]$ we have

(a) $V(f) \cup V(g) = V(fg)$;
(b) $V(f) \cap V(g) = V(f,g)$.

Exercise 3.10. By a *projective coordinate transformation* we mean a map $f\colon \mathbb{P}^n \to \mathbb{P}^n$ of the form

$$(x_0 : \cdots : x_n) \mapsto (f_0(x_0,\ldots,x_n) : \cdots : f_n(x_0,\ldots,x_n))$$

for linearly independent homogeneous linear polynomials $f_0,\ldots,f_n \in K[x_0,\ldots,x_n]$.

Now let $P_1,\ldots,P_{n+2} \in \mathbb{P}^n$ be points such that any $n+1$ of them are linearly independent in K^{n+1}, and in the same way let $Q_1,\ldots,Q_{n+2} \in \mathbb{P}^n$ be points such that any $n+1$ of them are linearly independent. Show that there is a projective coordinate transformation f with $f(P_i) = Q_i$ for all $i = 1,\ldots,n+2$.

Exercise 3.11. Show:

(a) If $F, G \in K[x_0,\ldots,x_n]$ are polynomials such that $F \mid G$ and G is homogeneous, then F is homogeneous.
(b) Every homogeneous polynomial in two variables over an algebraically closed field is a product of linear polynomials.

The definition of projective plane curves is now completely analogous to the affine case in Definition 1.5.

Definition 3.12 (Projective curves)**.**

(a) A **projective (plane algebraic) curve** (over K) is a non-constant homogeneous polynomial $F \in K[x,y,z]$ modulo units. We call $V(F) = \{P \in \mathbb{P}^2 : F(P) = 0\}$ its **set of points**.
(b) The **degree** of a projective curve is its degree as a polynomial. As in the affine case, curves of degree $1,2,3,\ldots$ are called **lines**, **quadrics/conics**, **cubics**, and so on. The line z is referred to as the **line at infinity**.
(c) The notions of irreducible/reducible/reduced curves, as well as of irreducible components and their multiplicities, are defined in the same way as for affine curves in Definition 1.5 (c) (note that irreducible factors of homogeneous polynomials are always homogeneous by Exercise 3.11 (a)).

To study projective curves, we will often want to relate them to affine curves. For this we need the following construction.

Construction 3.13 (Homogenization and dehomogenization)**.**

(a) For a non-zero polynomial

$$f = \sum_{i+j \le d} a_{i,j}\, x^i y^j \quad \in K[x,y]$$

of degree d we define the **homogenization** of f as

$$f^{\mathrm{h}} := \sum_{i+j \le d} a_{i,j}\, x^i y^j z^{d-i-j} \quad \in K[x,y,z].$$

Note that f^{h} is homogeneous of degree $\deg f^{\mathrm{h}} = \deg f = d$, and that $z \nmid f^{\mathrm{h}}$ since f contains a term with $i+j = d$.

(b) For a non-zero homogeneous polynomial

$$f = \sum_{i+j+k=d} a_{i,j,k}\, x^i y^j z^k \quad \in K[x,y,z]$$

of degree d we define the **dehomogenization** of f to be

$$f^{\mathrm{i}} := f(z=1) = \sum_{i+j+k=d} a_{i,j,k}\, x^i y^j \quad \in K[x,y].$$

In general, f^{i} will be an inhomogeneous polynomial. If $z \nmid f$, i. e. if f contains a monomial without z, then this monomial will also be present in f^{i}, and thus $\deg f^{\mathrm{i}} = \deg f = d$.

In particular, there is a bijective correspondence

$$\left\{\begin{array}{c}\text{polynomials of degree } d \\ \text{in } K[x,y]\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{homogeneous polynomials of degree } d \\ \text{in } K[x,y,z] \text{ not divisible by } z\end{array}\right\}$$
$$\begin{array}{ccc} f & \longmapsto & f^{\mathrm{h}} \\ f^{\mathrm{i}} & \longmapsfrom & f. \end{array}$$

Example 3.14. For $f = y - x^2 \in K[x,y]$ we have $f^{\mathrm{h}} = yz - x^2 \in K[x,y,z]$, and then back again $(f^{\mathrm{h}})^{\mathrm{i}} = y - x^2 = f$.

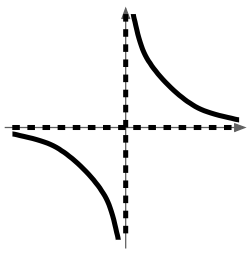
Construction 3.15 (Affine parts and projective closures)**.**

(a) For a projective curve F its affine set of points is $V_{\mathrm{p}}(F) \cap \mathbb{A}^2 = V_{\mathrm{a}}(F(z=1)) = V_{\mathrm{a}}(F^{\mathrm{i}})$. We will therefore call F^{i} the **affine part** of F. The points at infinity of F are given by $V_{\mathrm{p}}(F(z=0)) \subset \mathbb{P}^1$.

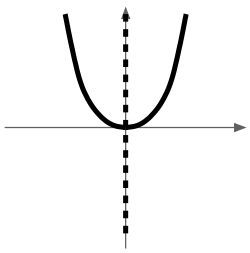
(b) For an affine curve F we call F^{h} its **projective closure**. By Construction 3.13 it is a projective curve whose affine part is again F, and that does not contain the line at infinity as a component.

However, F^{h} may contain points at infinity: If $F = F_0 + \cdots + F_d$ is the decomposition into homogeneous parts as in Notation 2.16, we have $F^{\mathrm{h}} = z^d F_0 + z^{d-1} F_1 + \cdots + F_d$ and hence $F^{\mathrm{h}}(z=0) = F_d$. So the points at infinity of F are given by the projective zero locus of the leading part of F.

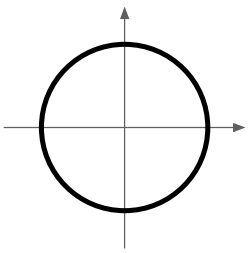
Example 3.16 (Visualization of projective curves)**.** To visualize a (real) projective curve F (that does not have the line at infinity as a component), we will often just draw its affine set of points $V_{\mathrm{a}}(F^{\mathrm{i}})$, and if desired in addition its points at infinity as directions in $\mathbb{A}^2$. The following picture shows in this way the projective closures of the three types of real conics – a hyperbola, a parabola, and an ellipse (resp. a circle) – where the dashed lines correspond to the points at infinity. We see that the hyperbola has two points at infinity (namely $(0:1:0)$ and $(1:0:0)$ in the case below), the parabola has one ($(0:1:0)$ below), and the circle no such point. Note that, including these additional points, all three cases become topologically a loop, as the unbounded ends of the affine curves meet up at the corresponding points at infinity. In fact, up to a change of coordinates, we will see in Exercise 3.28 that there is essentially only one type of real projective conic.



(a) hyperbola
$F = xy - 1$
$F^{\mathrm{h}} = xy - z^2$
points at infinity: $xy = 0$



(b) parabola
$F = y - x^2$
$F^{\mathrm{h}} = yz - x^2$
points at infinity: $x^2 = 0$



(c) ellipse
$F = x^2 + y^2 - 1$
$F^{\mathrm{h}} = x^2 + y^2 - z^2$
points at infinity: $x^2 + y^2 = 0$

Remark 3.17 (Spaces of curves as projective spaces)**.** For $d \in \mathbb{N}_{>0}$, the vector space of homogeneous polynomials of degree d in $K[x,y,z]$ has dimension $\binom{d+2}{2}$, hence it is isomorphic to K^{n+1} with $n = \binom{d+2}{2} - 1$. By definition, a projective curve of degree d is then a non-zero point of this vector space modulo scalars. Hence, the space of all such curves is just the projective space $\mathbb{P}^n$, and thus itself a projective variety.

It is in fact very special to algebraic geometry – and very powerful – that the spaces of (certain) varieties are again varieties, and thus can be studied with exactly the same methods as the initial objects themselves. In other categories this is usually far from being true: The space of all groups is not a group, the space of all vector spaces is not a vector space, the space of all topological spaces is not a topological space, and so on.

For the rest of this chapter, let us transfer our results on affine curves from Chapters 1 and 2 to the projective case.

Remark 3.18 (Finiteness of zero loci)**.** Let F and G be two projective curves. The finiteness results of Lemma 1.11 and Proposition 1.12 (b) hold for the affine parts of F and G (for any choice of coordinate determining the line at infinity), and thus for F and G themselves: $V(F)$ is infinite if K is algebraically closed, $\mathbb{P}^2 \backslash V(F)$ is infinite if K is infinite, and $V(F,G)$ is finite if F and G have no common component.

Remark 3.19 (Recovering F from $V(F)$)**.** Let F be a projective curve over an algebraically closed field. We can write it as $F = z^m G$ for some $m \in \mathbb{N}$ and a curve G with $z \nmid G$. Then G can be recovered from G^{i} since $G = (G^{\mathrm{i}})^{\mathrm{h}}$ by Construction 3.13, and G^{i} can be recovered from $V_{\mathrm{a}}(G^{\mathrm{i}}) = V_{\mathrm{p}}(G) \cap \mathbb{A}^2$ and a multiplicity on each component by Remark 1.14.

As the components of F are just the components of G plus possibly the line at infinity z (with multiplicity m), this means that F can be reconstructed from $V(F)$ and a multiplicity on each component, just as in the affine case.

Construction 3.20 (Local rings of $\mathbb{P}^2$)**.** For $P \in \mathbb{P}^2$ we define the **local ring** of $\mathbb{P}^2$ at P according to Remark 3.7 (b) as

$$\mathscr{O}_P := \mathscr{O}_{\mathbb{P}^2,P} := \left\{ \frac{f}{g} : f,g \in K[x,y,z] \text{ homogeneous of the same degree with } g(P) \neq 0 \right\} \cup \{0\} \subset K(x,y,z).$$

As in Definition 2.1, these rings admit a well-defined **evaluation map**

$$\mathscr{O}_P \to K, \ \frac{f}{g} \mapsto \frac{f(P)}{g(P)}$$

with kernel

$$I_P := I_{\mathbb{P}^2,P} := \left\{ \frac{f}{g} \in \mathscr{O}_P : f(P) = 0 \right\} \subset \mathscr{O}_P.$$

For a point $P = (x_0 : y_0 : 1)$ in the affine part of $\mathbb{P}^2$ it is easily checked that there is an isomorphism

$$\mathscr{O}_{\mathbb{P}^2,(x_0:y_0:1)} \to \mathscr{O}_{\mathbb{A}^2,(x_0,y_0)}, \ \frac{f}{g} \mapsto \frac{f^{\mathrm{i}}}{g^{\mathrm{i}}}$$

compatible with the evaluation maps, and thus taking $I_{\mathbb{P}^2,(x_0:y_0:1)}$ to $I_{\mathbb{A}^2,(x_0,y_0)}$. Hence the local rings are still the same as in the affine case – which is of course expected, as objects that are local around a point in $\mathbb{A}^2$ should not be affected by adding points at infinity.

Construction 3.21 (Intersection multiplicities)**.** Note that homogeneous polynomials are not elements of the local ring $\mathscr{O}_{\mathbb{P}^2,P}$. But for $F_1,\dots,F_k$ homogeneous we can still define a generated ideal

$$\langle F_1,\dots,F_k \rangle = \left\{ \frac{f_1}{g_1}F_1 + \dots + \frac{f_k}{g_k}F_k : f_i = 0 \text{ or } f_i,g_i \in K[x,y,z] \text{ homogeneous with } g_i(P) \neq 0 \text{ and } \deg(f_iF_i) = \deg g_i \text{ for all } i \right\}$$

in $\mathscr{O}_P$. As in the affine case we can therefore define the **intersection multiplicity** of two curves F,G at a point $P \in \mathbb{P}^2$ as

$$\mu_P(F,G) := \dim \mathscr{O}_P/\langle F,G \rangle \quad \in \mathbb{N} \cup \{\infty\}. \tag{$*$}$$

For a point $P = (x_0 : y_0 : 1)$ in the affine part of $\mathbb{P}^2$ one can verify directly that the isomorphism $\mathscr{O}_{\mathbb{P}^2,(x_0:y_0:1)} \cong \mathscr{O}_{\mathbb{A}^2,(x_0,y_0)}$ of Construction 3.20 takes $\langle F,G \rangle$ to $\langle F^{\mathrm{i}},G^{\mathrm{i}} \rangle$. Hence we have

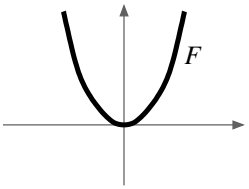
$\mu_{(x_0:y_0:1)}(F,G) = \mu_{(x_0,y_0)}(F^{\mathrm{i}},G^{\mathrm{i}})$, i. e. intersection multiplicities in the affine part can be computed exactly as in Chapter 2. At other points, the multiplicity can be computed similarly by choosing another (non-zero) coordinate to define the line at infinity as in Remark 3.4 (b). We will therefore probably never use the global definition $(*)$ of the multiplicity above for actual computations; its only purpose is to ensure that the result does not depend on the choice of coordinate defining the line at infinity.

Moreover, in the same way as in Remark 2.4 (a) intersection multiplicities are invariant under projective coordinate transformations as in Exercise 3.10, and they satisfy all the other properties of the multiplicities in Remark 2.4, Lemma 2.5, and Proposition 2.10.

Example 3.22. Let us compute the intersection multiplicity of the curve $F = yz - x^2$ (whose affine part is shown on the right) with the line $G = z$ at infinity at the common point $P = (0:1:0)$. For this we choose the affine part given by $y = 1$ and affine coordinates x and z. We then obtain

$$\mu_P(F,G) = \mu_{(0,0)}(z - x^2, z) = 2$$

by Example 2.11.



Construction 3.23 (Tangents and multiplicities of points, smooth and singular points)**.** The remaining concepts of Chapter 2 are also transferred easiest to a projective curve F using affine parts. So for a point $P = (x_0:y_0:1) \in \mathbb{P}^2$ in the affine part $\mathbb{A}^2$, we define the **multiplicity** $m_P(F)$ of F at P to be $m_{(x_0,y_0)}(F^{\mathrm{i}})$ in the sense of Definition 2.18. A **tangent** to F at P is the projective closure of a tangent to F^{i} at (x_0,y_0). If P is not in the affine part, we choose a different coordinate for the line at infinity as in Example 3.22 (it can be checked that this does not depend on the choice of coordinate).

We say that $P \in F$ is a **smooth** or **regular** point if $m_P(F) = 1$; its unique tangent is then denoted by T_PF. Otherwise, P is called a **singular** point of F. The curve F is said to be **smooth** or **regular** if all its points are smooth; otherwise F is called **singular**.

As in the affine case, there is a simple criterion to determine all singular points of a given projective curve. To prove it, we need a simple lemma first.

Lemma 3.24. *For any homogeneous polynomial $F \in K[x,y,z]$ of degree d we have*

$$x\frac{\partial F}{\partial x} + y\frac{\partial F}{\partial y} + z\frac{\partial F}{\partial z} = dF.$$

Proof. For $F = \sum_{i+j+k=d} a_{i,j,k}x^iy^jz^k$ we have $x\frac{\partial F}{\partial x} = \sum_{i+j+k=d} i\,a_{i,j,k}x^iy^jz^k$. An analogous formula holds for the other partial derivatives, and hence we conclude

$$x\frac{\partial F}{\partial x} + y\frac{\partial F}{\partial y} + z\frac{\partial F}{\partial z} = \sum_{i+j+k=d} (i+j+k)\,a_{i,j,k}x^iy^jz^k = dF. \qquad \square$$

05

Proposition 3.25 (Projective Jacobi Criterion)**.** *Let P be a point on a projective curve F.*

(a) *P is a singular point of F if and only if $\frac{\partial F}{\partial x}(P) = \frac{\partial F}{\partial y}(P) = \frac{\partial F}{\partial z}(P) = 0$.*

(b) *If P is a smooth point of F the tangent to F at P is given by*

$$T_PF = \frac{\partial F}{\partial x}(P)\cdot x + \frac{\partial F}{\partial y}(P)\cdot y + \frac{\partial F}{\partial z}(P)\cdot z.$$

Proof. Without loss of generality we may assume that $P = (x_0:y_0:1)$ is in the affine part of F.

(a) By the affine Jacobi criterion of Proposition 2.24 (a) we know that P is a singular point of F if and only if $\frac{\partial F^{\mathrm{i}}}{\partial x}(x_0,y_0) = \frac{\partial F^{\mathrm{i}}}{\partial y}(x_0,y_0) = 0$. As dehomogenizing F (which is just setting $z = 1$) commutes with taking partial derivatives with respect to x and y, this is equivalent to $\frac{\partial F}{\partial x}(P) = \frac{\partial F}{\partial y}(P) = 0$. This is in turn equivalent to $\frac{\partial F}{\partial x}(P) = \frac{\partial F}{\partial y}(P) = \frac{\partial F}{\partial z}(P) = 0$ by Lemma 3.24 since $F(P) = 0$ by assumption.

(b) By Proposition 2.24 (b) the affine tangent to F at P is given by

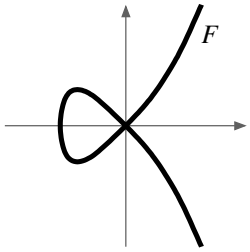
$$\begin{aligned}&\frac{\partial F^{\mathrm{i}}}{\partial x}(x_0,y_0)\cdot(x-x_0)+\frac{\partial F^{\mathrm{i}}}{\partial y}(x_0,y_0)\cdot(y-y_0)\\ &\quad=\frac{\partial F}{\partial x}(P)\cdot x+\frac{\partial F}{\partial y}(P)\cdot y-\left(\frac{\partial F}{\partial x}(P)\cdot x_0+\frac{\partial F}{\partial y}(P)\cdot y_0\right)\\ &\quad\overset{3.24}{=}\frac{\partial F}{\partial x}(P)\cdot x+\frac{\partial F}{\partial y}(P)\cdot y+\frac{\partial F}{\partial z}(P).\end{aligned}$$

By definition, T_PF is now obtained by taking the projective closure, i. e. the homogenization of this polynomial. □

Remark 3.26. If the ground field K has characteristic 0, Lemma 3.24 tells us for any point $P \in \mathbb{P}^2$ that the conditions $\frac{\partial F}{\partial x}(P) = \frac{\partial F}{\partial y}(P) = \frac{\partial F}{\partial z}(P) = 0$ already imply $F(P) = 0$. In contrast to the affine case in Example 2.25, we therefore do not have to check explicitly that the point lies on the curve when computing singular points with the Jacobi criterion.

Example 3.27. Let $F = y^2z - x^2z - x^3$ be the projective closure of the real affine curve $y^2 - x^2 - x^3$ of Example 2.21 (b). We have

$$\frac{\partial F}{\partial x} = -2xz - 3x^2, \quad \frac{\partial F}{\partial y} = 2yz, \quad \frac{\partial F}{\partial z} = y^2 - x^2.$$



It is checked immediately that the only common zero of these three polynomials is the point $(0:0:1)$, i. e. the origin of the affine part of F. So by Proposition 3.25 this is the only singular point of F (note that we have already seen in Example 2.25 using the affine Jacobi criterion that the origin is the only singular point of the affine part of F).

In particular, the point $(0:1:0) \in F$ at infinity is a smooth point of F, and the tangent to F there is by Proposition 3.25

$$\frac{\partial F}{\partial x}(0:1:0)\cdot x+\frac{\partial F}{\partial y}(0:1:0)\cdot y+\frac{\partial F}{\partial z}(0:1:0)\cdot z = z,$$

i. e. the line at infinity.

Exercise 3.28. Let F and G be two real smooth projective conics with non-empty set of points. Show that there is a projective coordinate transformation of $\mathbb{P}^2$ as in Exercise 3.10 that takes F to G.

Exercise 3.29. For a projective curve F in the homogeneous coordinates x_0, x_1, x_2 we define the associated *Hessian* to be $H_F := \det\left(\frac{\partial^2 F}{\partial x_i \partial x_j}\right)_{i,j=0,1,2}$.

(a) Show that the Hessian is compatible with coordinate transformations, i. e. if a projective coordinate transformation as in Exercise 3.10 takes F to F' then up to multiplication with a unit it takes H_F to $H_{F'}$.

(b) Let $P \in F$ be a smooth point, and assume that the characteristic of the ground field K is 0. Show that $H_F(P) = 0$ if and only if $\mu_P(F, T_PF) \geq 3$. Such a point is called an *inflection point* of F.

Hint: By part (a) and Exercise 3.10 you may assume after a coordinate transformation that $P = (0:0:1)$ and $T_PF = x_1$.

4. Bézout's Theorem

Let F and G be two projective curves without common component. We have seen already in Remark 3.18 that the intersection $F \cap G$ is finite in this case. Bézout's Theorem, which is the main goal of this chapter, will determine the number of these intersection points, where each such point P will be counted with its intersection multiplicity $\mu_P(F,G)$.

In the same way as for the number of zeros of a univariate polynomial, the result will only be nice (i. e. depend only on the degree of the polynomials) if we assume that the underlying ground field is algebraically closed. To use this assumption we will need the following result from commutative algebra that extends the defining property of an algebraically closed field to polynomials in several variables.

Fact 4.1 (Hilbert's Nullstellensatz)**.** Recall that a field K is called algebraically closed if every univariate polynomial $f \in K[x]$ without a zero in K is constant.

An obvious generalization of this statement to the multivariate case (which can be proven easily by induction of the number of variables) would be that every polynomial $f \in K[x_1,\dots,x_n]$ without a zero in $\mathbb{A}^n$ is constant. However, there is a much stronger statement that also applies to several polynomials at once, or more precisely to the ideal generated by them: *Any ideal I in $K[x_1,\dots,x_n]$ with $V(I) = \emptyset$ over an algebraically closed field K is the unit ideal $I = \langle 1 \rangle$.* This statement is called by its German name **Hilbert's Nullstellensatz** ("theorem of the zeros") [G6, Remark 10.12]. Obviously, in the case $n = 1$ of polynomials in one variable, the ideal I must be generated by a single polynomial f as $K[x_1]$ is a principal ideal domain, and thus Hilbert's Nullstellensatz just reduces to the original statement that f must be constant if it does not have a zero.

Although Bézout's Theorem requires projective curves (as we have already motivated at the beginning of Chapter 3), it is actually more convenient to perform almost all steps required in its proof for the affine case. Our first step will be to compute the sum $\sum_{P \in F \cap G} \mu_P(F,G)$ of the local intersection multiplicities of two affine curves F and G and express it in terms of one global object. In fact, in the same way as $\mu_P(F,G)$ is by definition the dimension of the quotient of the *local* ring $\mathcal{O}_P$ by the ideal $\langle F,G \rangle$, the sum of these multiplicities is just the dimension of the quotient of the *global* polynomial ring $K[x,y]$ by $\langle F,G \rangle$:

Lemma 4.2 (Summing up intersection multiplicities)**.** *Let F and G be two affine curves over K with no common component (so that $F \cap G$ is finite by Remark 3.18). We consider the natural ring homomorphism*

$$\varphi \colon K[x,y]/\langle F,G \rangle \to \prod_{P \in F \cap G} \mathcal{O}_P/\langle F,G \rangle$$

that sends the class of a polynomial $f \in K[x,y]$ to the class of $f \in \mathcal{O}_P$ in each factor $\mathcal{O}_P/\langle F,G \rangle$.

(a) *The morphism φ is surjective.*

(b) *If K is algebraically closed then φ is an isomorphism.*

In particular, we have $\sum_P \mu_P(F,G) \le \dim K[x,y]/\langle F,G \rangle$, with equality if K is algebraically closed.

Proof.

(a) Let $F \cap G = \{P_0,\dots,P_m\}$ with $P_i = (x_i,y_i)$ for $i = 0,\dots,m$. By Exercise 2.7 (a) there is a number $n \in \mathbb{N}$ such that $(x-x_i)^n = (y-y_i)^n = 0 \in \mathcal{O}_{P_i}/\langle F,G \rangle$ for all i. For the polynomial

$$f := \prod_{i : x_i \neq x_0} (x-x_i)^n \cdot \prod_{i : y_i \neq y_0} (y-y_i)^n \quad \in K[x,y]$$

we then have $f(P_0) \neq 0$, so by Exercise 2.7 (b) there is a polynomial representative $g \in K[x,y]$ for $\frac{1}{f} \in \mathcal{O}_{P_0}/\langle F,G \rangle$. The polynomial fg is then mapped by φ ...

- in the component $\mathcal{O}_{P_0}/\langle F,G\rangle$ to $fg = f\cdot\frac{1}{f} = 1$;
- in all other components $\mathcal{O}_{P_i}/\langle F,G\rangle$ for $i>0$ to 0 since $f = 0 \in \mathcal{O}_{P_i}/\langle F,G\rangle$.

By symmetry, we can find in the same way for all $i = 1,\dots,m$ a polynomial that is mapped by φ to 1 in the P_i-component and to 0 in all others. As the image of φ is a subring, it follows that φ is surjective.

(b) In view of (a) it remains to be shown that φ is injective. So let $f \in K[x,y]$ with $\varphi(f) = 0$, and consider the set $I := \{g \in K[x,y] : gf \in \langle F,G\rangle\}$. This is clearly an ideal containing $\langle F,G\rangle$ (usually called the *ideal quotient* $\langle F,G\rangle : \langle f\rangle$). By the Nullstellensatz of Fact 4.1 it suffices to prove that $V(I) = \emptyset$, since then $I = K[x,y]$, hence $1 \in I$, i. e. $f \in \langle F,G\rangle$, and thus $f = 0 \in K[x,y]/\langle F,G\rangle$.

So assume that there is a point $P \in V(I)$. As $F,G \in I$ we know that $P \in F \cap G$. Hence P is one of the points in the product in the target space of φ, and so $f = 0 \in \mathcal{O}_P/\langle F,G\rangle$ as $f \in \ker\varphi$. This means that $f = \frac{a}{g}F + \frac{b}{g}G$ for some polynomials $a,b,g \in K[x,y]$ with $g(P) \neq 0$. But then $gf = aF + bG$, hence $g \in I$, and as $P \in V(I)$ we arrive at the contradiction $g(P) = 0$. □

Remark 4.3. There are two ways to interpret the statement of Lemma 4.2:

(a) A case that often occurs in Lemma 4.2 is that F and G intersect transversely, i. e. that the intersection multiplicities $\mu_P(F,G)$ at all $P \in F \cap G$ are equal to 1. In this case every factor $\mathcal{O}_P/\langle F,G\rangle$ is isomorphic to K by Definition 2.3, and the morphism φ is just the combined evaluation map at all points of $F \cap G$. The assertion of Lemma 4.2 (a) is then simply the interpolation statement that we can always find a polynomial having prescribed values at these points – which is probably not surprising, and is in fact already achieved by a suitable linear combination of polynomials as in Step 1 in the proof. If the intersection is not transverse and $\mu_P(F,G) > 1$ at some point P, then the map φ remembers more information at P on the polynomial than just its value, such as the values of some of its partial derivatives at P.

(b) If you have some commutative algebra background then you probably know the statement of Lemma 4.2 already: As $V(F,G)$ is 0-dimensional, the ring $K[x,y]/\langle F,G\rangle$ is Artinian, and thus by the Structure Theorem on Artinian rings it is isomorphic to the product of its localizations at its various maximal ideals [G6, Proposition 7.20]. If K is algebraically closed then these maximal ideals all correspond to points in $\mathbb{A}^2$ [G6, Corollary 10.10], and so the map φ of the lemma is an isomorphism. If K is not necessarily algebraically closed then there are maximal ideals of $K[x,y]/\langle F,G\rangle$ that are not of this form and thus "missing" in the target space of φ, so that φ is only surjective.

Of course, our goal must now be to compute the dimension of the quotient $K[x,y]/\langle F,G\rangle$. In order to do this, we need a lemma first that tells us how polynomials in the ideal $\langle F,G\rangle$ of $K[x,y]$ can be represented.

Lemma 4.4. *Let F and G be two affine curves of degrees $m := \deg F$ and $n := \deg G$, respectively, such that their leading parts F_m and G_n (as in Notation 2.16) have no common component.*

Then every $f \in \langle F,G\rangle \subset K[x,y]$ of degree $d := \deg f$ can be written as $f = aF + bG$ for two polynomials a and b with $\deg a \leq d-m$ and $\deg b \leq d-n$.

Proof. As $f \in \langle F,G\rangle$ we can write $f = aF + bG$ for some $a,b \in K[x,y]$; choose such a representation with $\deg a$ minimal.

Assume for a contradiction that $\deg a > d-m$ or $\deg b > d-n$. Then aF or bG contains a term of degree bigger than d. As $f = aF + bG$ has degree d this means that the leading terms of aF and bG must cancel in f. Hence, if a_* and b_* denote the leading terms of a and b, respectively, we have $a_*F_m = -b_*G_n$. But F_m and G_n have no common component by assumption, and so we must have $a_* = cG_n$ and $b_* = -cF_m$ for some homogeneous polynomial c. This gives us a new representation

$$f = (a-cG)F + (b+cF)G$$

in which the leading term a_* of a cancels the leading term cG_n of cG in the first bracket. Hence $\deg(a-cG) < \deg a$, contradicting the minimality of $\deg a$. □

Lemma 4.5. *Let F and G be affine curves with no common component, of degrees $m := \deg F$ and $n := \deg G$.*

(a) $\dim K[x,y]/\langle F,G\rangle \le mn$.

(b) *If the leading parts F_m and G_n have no common component either then equality holds in (a).*

Proof. For all $d \ge m+n$ consider the sequence of vector space homomorphisms

$$K[x,y]_{\le d-m} \times K[x,y]_{\le d-n} \xrightarrow{\alpha} K[x,y]_{\le d} \xrightarrow{\pi} K[x,y]/\langle F,G\rangle$$
$$(a,b) \longmapsto aF+bG$$

where $K[x,y]_{\le d}$ denotes the vector subspace of $K[x,y]$ of all polynomials of degree at most d, which has dimension $\binom{d+2}{2}$, and π is the quotient map.

The kernel of α consists of all pairs (a,b) of polynomials of degrees at most $d-m$ and $d-n$, respectively, with $aF = -bG$. As F and G have no common component, this is equivalent to $a = cG$ and $b = -cF$ for some $c \in K[x,y]_{\le d-m-n}$, so that

$$\ker\alpha = K[x,y]_{\le d-m-n} \cdot (G,-F). \tag{1}$$

Moreover, it is obvious that

$$\operatorname{im}\alpha \subset \ker\pi. \tag{2}$$

So we conclude with the homomorphism theorem

$$\begin{aligned}
\dim\operatorname{im}\pi &= \binom{d+2}{2} - \dim\ker\pi \\
&\overset{(2)}{\le} \binom{d+2}{2} - \dim\operatorname{im}\alpha \\
&= \binom{d+2}{2} - \binom{d-m+2}{2} - \binom{d-n+2}{2} + \dim\ker\alpha \\
&\overset{(1)}{=} \binom{d+2}{2} - \binom{d-m+2}{2} - \binom{d-n+2}{2} + \binom{d-m-n+2}{2} \\
&= mn.
\end{aligned}$$

Note that this bound is independent of d (as long as $d \ge m+n$), and thus also holds for the projection map $\pi\colon K[x,y] \to K[x,y]/\langle F,G\rangle$ from the full polynomial ring, which is surjective. It follows that $\dim K[x,y]/\langle F,G\rangle \le mn$, which is (a).

For (b), it suffices to establish equality in (2) above, i. e. that $\ker\pi \subset \operatorname{im}\alpha$. But this is precisely the statement of Lemma 4.4. □

We can now switch back to the projective case and prove the main result of this chapter.

Corollary 4.6 (Bézout's Theorem). *Let F and G be projective curves without common component over an infinite field K. Then*

$$\sum_{P\in F\cap G} \mu_P(F,G) \le \deg F \cdot \deg G.$$

Moreover, equality holds if K is algebraically closed.

06

References

[F] W. Fulton, *Algebraic Curves*,
http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf

[G1] A. Gathmann, *Algebraische Strukturen*, class notes TU Kaiserslautern (2023),
https://agag-gathmann.math.rptu.de/ags

[G2] A. Gathmann, *Grundlagen der Mathematik*, class notes RPTU Kaiserslautern (2025/26),
https://agag-gathmann.math.rptu.de/gdm

[G3] A. Gathmann, *Einführung in die Algebra*, class notes TU Kaiserslautern (2010/11),
https://agag-gathmann.math.rptu.de/algebra

[G4] A. Gathmann, *Einführung in die Funktionentheorie*, class notes TU Kaiserslautern (2021/22),
https://agag-gathmann.math.rptu.de/futheo

[G5] A. Gathmann, *Einführung in die Topologie*, class notes TU Kaiserslautern (2023),
https://agag-gathmann.math.rptu.de/topo

[G6] A. Gathmann, *Commutative Algebra*, class notes TU Kaiserslautern (2014),
https://agag-gathmann.math.rptu.de/commalg

[Ki] F. Kirwan, *Complex Algebraic Curves*, Cambridge University Press (1995)

[Ku] E. Kunz, *Introduction to Plane Algebraic Curves*, Birkhäuser (2005)

[W] Wikipedia entry *Curve25519* (2023),
https://en.wikipedia.org/wiki/Curve25519

Index