Plane Algebraic Curves

Andreas Gathmann

Class Notes RPTU Kaiserslautern 2026

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.

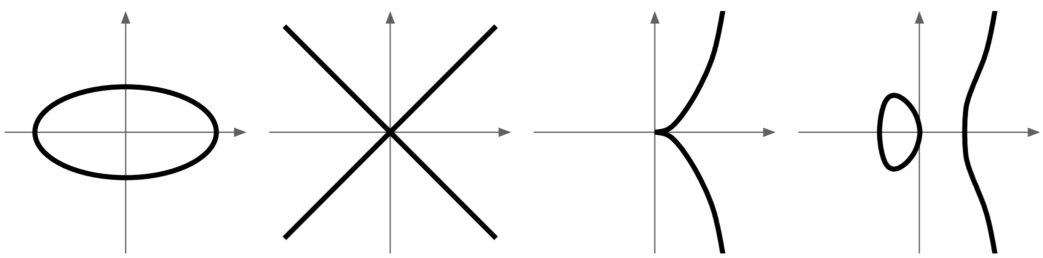
(b) In algebra (as e. g. in the “Algebraic Structures” or “Introduction to Algebra” classes [G1, G3]), a central topic are polynomials in one variable over K.

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) | $x^2-y^2=0$ (b) | $y^2-x^3=0$ (c) | $y^2+x-x^3=0$ (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 $x(x-1)(x+1)$.

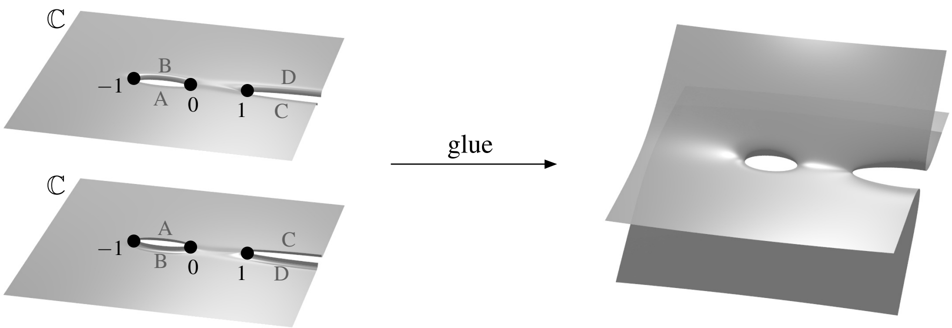
This is not the correct topological picture however, because a non-zero complex number does not have a distinguished first and second root that could correspond to the first and second copy of the complex plane. Rather, the two roots of a complex number get exchanged if we run around the origin once: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

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

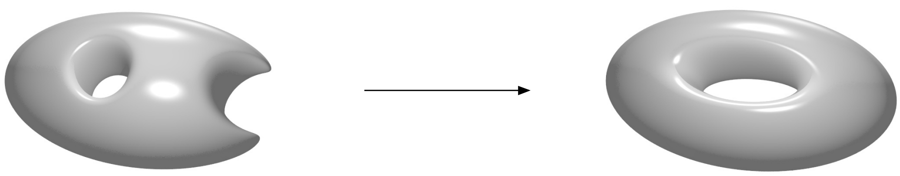
around the complex origin, the square root of this number would have to be defined by

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

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.

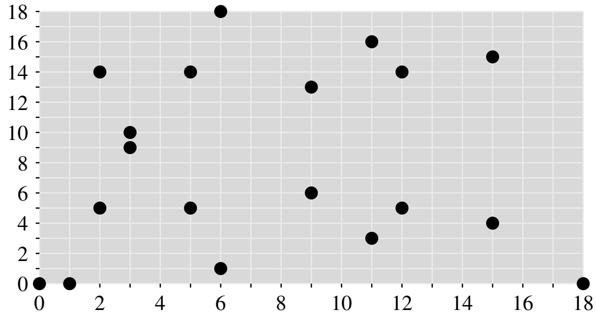


This is now actually a topologically correct picture of the given curve. To make the situation a little nicer, we can compactify it by adding a point at infinity, which corresponds to identifying the two planes at their infinitely far points as well (the precise construction will be described in Chapter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

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

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

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

Unless stated otherwise, the *degree* of a term $a_{i_1,\dots,i_n}\, x_1^{i_1}\cdot\,\cdots\,\cdot x_n^{i_n}$ as above is meant to be the total degree $i_1+\cdots+i_n$ 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

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

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 $1,2,3,\ldots$ 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 $F = F_1{}^{a_1} \cdot \cdots \cdot F_k^{a_k}$ 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 $F_1,\ldots,F_k$ are then called the **(irreducible) components** of F and $a_1,\ldots,a_k$ 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.

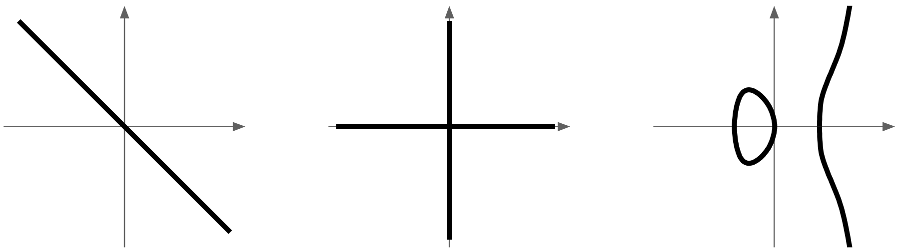
(a) The curve $x+y$ is a line, and hence irreducible (as a polynomial of degree 1 cannot be a product of two non-constant polynomials). Its square $(x+y)^2$ has the same set of points as $x+y$, but it is a quadric. It is neither irreducible nor reduced.

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 $K = \{c_1, \dots, c_n\}$ 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 $R = K[x_1, \dots, x_n]$, for which $\operatorname{Quot} R$ is denoted $K(x_1, \dots, x_n)$ 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 $\mathbb{A}^2_K \backslash V(F)$ 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 $a_0, \dots, a_n \in K[y]$ 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
01 an $x \in K$ with $F(x,y) \neq 0$ (as $F(\cdot\,,y)$ has only finitely many zeros). □

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