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. Surprisingly however, it turns out to be 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** 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 $F = F_1{}^{a_1} \cdot \cdots \cdot F_k^{a_k}$ 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 $F_1,\dots,F_k$ 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.

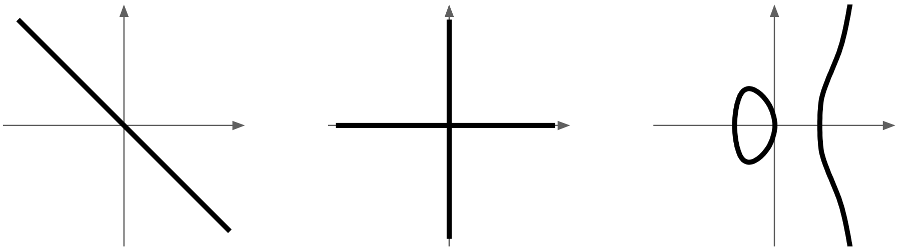
(a) The curve $x+y$ is a line, and hence irreducible (as a polynomial of degree 1 cannot be a product of two non-constant polynomials). Its square $(x+y)^2$ has the same set of points as $x+y$, but it is a quadric. It is neither irreducible nor reduced.

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 polynomials without zeros, the set of points $V(F)$ might be empty and thus does not determine back F.

We will see now that these are essentially the only two problems that can arise. 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 6.19] — 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 5 in order not to exclude the important and 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 an $x \in K$ with $F(x,y) \neq 0$ (as $F(\,\cdot\,,y)$ has only finitely many zeros). □

01

Proposition 1.12. *If two curves F and G have no common component then their intersection $V(F,G)$ is finite.*

Proof. 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 $H, F', G' \in K[x,y]$ of positive y-degree and non-zero $a \in K[x]$. 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 decomposition $F = HF'$ and $G = HG'$ with $H, F', G' \in K[x,y]$ 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 10.22]. 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 non-zero $c \in K[x]$.

But if then $P \in V(F,G)$ 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*

$$G \,|\, F \;\Leftrightarrow\; V(G) \subset V(F).$$

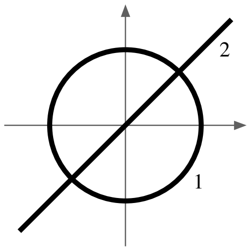
In particular, the irreducible components of F (but not their multiplicities, see Example 1.7 (a)) can be recovered from $V(F)$.

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 this means that F and G must have a common component. As G is irreducible, this is only possible if $G \,|\, F$. □

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;

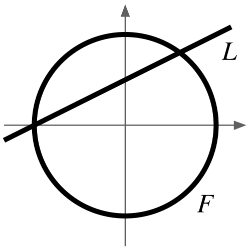
(c) $F \cup G$ for the curve FG (see Remark 1.4 (a));

(d) $G \subset F$ instead of $G \,|\, F$.

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 $\lambda, u, v \in \mathbb{Z}$.