## C. Curves and function fields

An elliptic curve is often regarded as a synonymous for a smooth Weierstraß curve. But in fact an elliptic curve is a much broader concept the essence of which can be expressed algebraically in the language of algebraic function fields.

This text does not aspire to provide a formal introduction into that theory. Nevertheless this introductory section presents several of its concepts and notions. The aim is to sketch what is the connection between the geometry of curves and the algebra of function fields.

Let us start by making some notational conventions and introductory definitions.

Let $K$ be a field, and let $\bar{K}$ be an algebraic closure of $K$. Both $K$ and $\bar{K}$ are regarded as fixed.

The *$n$-dimensional affine space* $\bar{K}^n$ is denoted by $\mathbb{A}^n$, and the set $K^n$ by $\mathbb{A}^n(K)$. The elements of $\mathbb{A}^n(K)$ are called *$K$-rational points*.

If $f_1, \dots, f_k \in K[x_1, \dots, x_n]$ are polynomials, then $V_{f_1,\dots,f_k}$ denotes the set of all $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{A}^n$ such that $f_i(\alpha) = f_i(\alpha_1, \dots, \alpha_n) = 0$ for all $i \in \{1, \dots, k\}$.

A *planar affine curve* over $K$ is any subset of $\mathbb{A}^2$ than can be expressed as $V_f$, where $f \in K[x_1, x_2]$, $\deg(f) \geq 0$.

In other words, planar affine curves are the zero points of nonzero polynomials in two variables. Since $K[x_1, x_2]$ is a UFD (unique factorization domain) each polynomial $f \in K[x_1, x_2]$, $\deg(f) \geq 1$, may be expressed uniquely, up to scalar multiples, as $f_1 \cdots f_k$, where each $f_i$ is an irreducible polynomial.

If $f = f_1 \cdots f_k$, $k \geq 1$, then $V_f = V_{f_1} \cup \cdots \cup V_{f_k}$. For example, if $f = x_1 x_2$, then $V_f$ is the union of the coordinate lines.

The case of $k > 1$ will be discussed only briefly. The main focus is upon the case $k = 1$.

C.1. **Coordinate rings and function fields.** Suppose that $C$ is an affine planar curve. There are many $g \in K[x_1, x_2]$ such that $g(\alpha) = 0$ for every $\alpha \in C$. The set of all such $g$ is closed under addition, and also under multiplication by another element of $K[x_1, x_2]$. This set is thus an ideal of the ring $K[x_1, x_2]$. It may be proved that this ideal is the principal ideal of a polynomial $f = f_1 \cdots f_k$, where $k \geq 1$, where each $f_i$ is irreducible, $1 \leq i \leq k$, and where $(f_i) \neq (f_j)$ if $1 \leq i < j \leq k$. The latter condition says that the principal ideals of $f_i$ and $f_j$ are different. Since both $f_i$ and $f_j$ are irreducible, this means, in fact, that $f_i$ is not a scalar multiple of $f_j$. (A scalar multiple always refers to a multiplication by a nonzero element of $K$. The group of nonzero elements of $K$ is denoted by $K^*$).

For polynomials $g, h \in K[x_1, x_2]$ write $g \sim h$ if $g(\alpha) = h(\alpha)$ for each $\alpha \in C$. This is clearly an equivalence upon $K[x_1, x_2]$ such that $g \sim h$ if and only if $g - h$ vanishes on all points of $C$. In other words $g \sim h$ if and only if $g - h \in (f)$. Classes of $\sim$ thus coincide with cosets of the ideal $(f)$.

Where there is an ideal, there is also a factor ring. The ring $K[x_1, x_2]/(f)$ is determined only by the curve $C$ since $f$ is determined by $C$ uniquely, up to a scalar multiple. Hence it is correct to put

$$K[C] = K[x_1, x_2]/(f).$$

The ring $K[C]$ is called the *coordinate ring* of the curve $C$. Elements of $K[C]$ are cosets $a + (f)$, where $a$ runs through $K[x_1, x_2]$.

Such a description of $K[C]$ is complete, correct and exhaustive. Nevertheless it is somewhat formal. Such a description will be called *algebraic*. Another term for it might be *syntactic*.

To move from syntax to semantics let us return to the above definition of $\sim$. By this definition, $g \sim h$ if and only if polynomials $g$ and $h$ *behave* identically upon $C$. The ring $K[C]$ may be understood as a collection of all possible polynomial

behaviours on $C$. Note that in this way $K[C]$ could be defined without introducing any ideal since polynomials upon $C$ may be both added and multiplied in a natural way. Such an approach to $K[C]$ will be termed *geometric* or, perhaps more exactly, *functional*.

Note that elements of $K[C]$ are defined with respect to all points of $C$. This is important to realize especially when working with finite fields. Points of $C$ that are not $K$-rational always have to be taken into account. At first glance this may be regarded as superfluous since the group of an elliptic curve over $K$ is defined only upon the $K$-rational points. However, there exist important and efficient algorithms that determine properties of such a group (like the order) that work with points that are not $K$-rational.

Note also that if $K$ is finite then two elements of $K[C]$ may agree upon all $K$-rational points and yet be different.

Let $f \in K[x_1, x_2]$ be a polynomial of degree at least one and let $K[C] = K[x_1, x_2]/(f)$, $C = V_f$. The ring $K[C]$ is a domain if and only if $f$ is irreducible. This is exactly when the curve $C$ is called *irreducible*.

Recall that if $R$ is a domain, then it is possible to construct the *fraction field* $F$, where $a/b = c/d$ if and only if $ad - bc = 0$.

Suppose that $C$ is an irreducible planar affine curve. The fraction field of $K[C]$ will be denoted by $K(C)$ and called the *function field* of $C$.

The functions to which the name "function field" refers are the rational functions $a/b \in K(x_1, x_2)$. Note that $K(x_1, x_2)$ may be defined as the fraction field of the domain $K[x_1, x_2]$.

The algebraic approach to $K(C)$ stresses the formal description of its elements. Each element of $K(C)$ is equal to some $(a + (f))/(b + (f))$, where $C = V_f$, $f \in K[x_1, x_2]$ irreducible. Elements $a, b$ run through $K[x_1, x_2]$, with $b \notin (f)$. The latter condition is equivalent to $b + (f) \neq 0_{K(C)}$. By the definition of fraction fields

$$\frac{a + (f)}{b + (f)} = \frac{c + (f)}{d + (f)} \;\Leftrightarrow\; ad - bc \in (f). \tag{C.1}$$

The functional interpretation of $K(C)$ is similar to that of $K[C]$. However, there is a technical difficulty which has to be cosidered. For $\sigma \in K(C)$ there are many $a/b \in K[x_1, x_2]$ such that $\sigma = (a + (f))/(b + (f))$. Each such $a/b$ is said to be a *representative* of $\sigma$. Since $b \notin (f)$ there are only finitely many $\alpha \in C$ such that $b(\alpha) = 0$ (this is not a completely obvious fact, but the proof is relatively easy). Hence each representative of $\sigma$ yields a mapping $C \to \bar{K}$ that is defined *nearly everywhere*, that is up to finitely many points of $C$. The technical difficulty mentioned above rests in the fact that if $c/d$ is another representative of $\sigma$, then the points $\alpha \in C$ where $b(\alpha) = 0$ may be different from those where $d(\alpha) = 0$. However, (C.1) implies that if $b(\alpha) \neq 0$ and $d(\alpha) \neq 0$, then $a(\alpha)/b(\alpha) = c(\alpha)/d(\alpha)$.

With each $\sigma \in K(C)$ there thus may be associated a function $C \to \bar{K}$ that is defined for every $\alpha \in C$ for which there exists a representative $a/b$ of $\sigma$ such that $b(\alpha) \neq 0$. If $a/b$ is such a representative, then $\sigma(\alpha) = a(\alpha)/b(\alpha)$. This definition is correct, as follows from (C.1).

The functional field $K(C)$ may be regarded as a collection of all partial mappings $C \to \bar{K}$ that may be obtained in such a way.

C.2. **Discrete valuations.** Let $C$ be an irreducible planar affine curve. It turns out that many important properties of $C$ depend only upon the algebraic structure of the function field $K(C)$.

The key notion in the algebraic analysis of $K(C)$ is the notion of *discrete valuation*. This is something quite natural that arose from the most basic properties of primes as they occur in every UFD.

Let $R$ be a UFD and let $F$ be the fraction field of $R$. For each irreducible $p \in R$ define $v_p(r)$, $r$ a nonzero element of $R$, as the largest $k \geq 0$ such that $p^k \mid r$. By definition, $v_p(0) = \infty$.

Extend the definition of $v_p(r)$ from $R$ to $F$ by setting $v_p(r/s) = v_p(r) - v_p(s)$.

Put $\nu = v_p$. The following properties are true for all $a, b \in F$:

$$\nu(ab) = \nu(a) + \nu(b); \tag{DV1}$$

$$\nu(a+b) \geq \min\{\nu(a), \nu(b)\}, \tag{DV2}$$

$$\nu(a) = \infty \;\Leftrightarrow\; a = 0; \text{ and} \tag{DV3}$$

$$\exists a \in F,\ \nu(a) = 1. \tag{DV4}$$

Let now $F$ be a field (no assumption is now being made about $F$ being a fraction field of a domain $R$). A mapping $\nu\colon F \to \mathbb{Z} \cup \{\infty\}$ is called a *discrete valuation* if it fulfils (DV1)–(DV3). Discrete valuations that also fulfil (DV4) are called *normalized*.

Suppose that $F = K(C)$. The discrete valuations of $F$ that are considered when investigating the curve $C$ are those that fulfil this additional condition:

$$\nu(a) = 0 \text{ for every } a \in K^*.$$

They will be called valuations *over* $K$.

Let us pay attention to the way how the field $K$ is embedded into $K(C)$. Both $K[C]$ and $K(C)$ are vector spaces over $K$. The unit in both of them is equal to $1 + (f)$, where $C = V_f$, $f \in K[x_1, x_2]$ irreducible. Consider $\lambda \in K$. The element $\lambda$ is identified in both $K[C]$ and $K(C)$ with $\lambda \cdot 1_{K[C]} = \lambda \cdot 1_{K(C)} = \lambda + (f)$. The functional interpretation of $\lambda + (f)$ is clear: each $\alpha \in C$ is mapped upon $\lambda$.

For unique factorization domains (UFD) the notion of discrete valuation does not seem to bring much new. That is not completely true as shown by the ensuing analysis of $K(x)$. Furthermore, the coordinate ring $K[C]$ is rarely a UFD, and yet $K(C)$ contains many (in fact, infinitely many) normalized discrete valuations over $K$.

If $F = K(x)$ (the ring of rational functions in one variable), then each irreducible polynomial $p \in K[x]$ yields a normalized discrete valuation $v_p$. Besides them there exists exactly one normalized discrete valuation over $K$. This valuation is denoted by $v_\infty$ and defined by $v_\infty(a/b) = \deg(b) - \deg(a)$.

Suppose now, for a while, that $\bar{K} = K$. In such a case the monic irreducible polynomials are the polynomials $x - \lambda$. With the exception of $v_\infty$ each normalized discrete valuation over $K$ thus may be identified with a unique point of the affine line $\mathbb{A}^1$. To give a geometric meaning to $v_\infty$ extend the affine line $\mathbb{A}^1$ to the projective line $\mathbb{P}^1$. This means to add just one point. This point is called the *point at infinity*.

The connection "one point—one discrete valuation" is not limited to the projective line. The connection is valid for all irreducible projective planar curves over $\bar{K}$ that satisfy a certain additional condition. This will be precised later.

C.3. **Planar projective curves.** The formal definition of the $n$-dimensional *projective space* $\mathbb{P}^n$ states that $\mathbb{P}^n$ is equal to the set of all 1-dimensional subspaces of $\mathbb{A}^{n+1}$. However, a projective point (i.e., an element of $\mathbb{P}^n$) is usually treated by considering its homogeneous coordinates $(\alpha_1 : \alpha_2 : \cdots : \alpha_{n+1})$. The connection to the formal definition is made by considering these coordinates as representatives of the space of all $(\lambda\alpha_1, \lambda\alpha_2, \ldots, \lambda\alpha_{n+1})$, where $\lambda$ runs through $\bar{K}$. This means that homogeneous coordinates represent the same point if and only if in all positions they differ by the same scalar multiple and that at least one position has to carry a nonzero entry.

A projective point is *K-rational* if it may be expressed as $(\alpha_1 : \cdots : \alpha_{n+1})$, where $\alpha_i \in K$ for each $i \in \{1, \ldots, n+1\}$.

It is usual to identify an affine point $(\alpha_1, \ldots, \alpha_n) \in \mathbb{A}^n$ with the projective point $(\alpha_1 : \cdots : \alpha_n : 1) \in \mathbb{P}^n$. The projective points that cannot be obtained in this way are called *points at infinity*. In $\mathbb{P}^1$ there is only one point at infinity and this point is equal to $(1 : 0)$.

Let $a = \sum a_{i_1,\ldots,i_k} x_1^{i_1} \ldots x_k^{i_k}$ be a polynomial over $K$. This polynomial is called *homogeneous* if its coefficients fulfil the implication

$$a_{i_1,\ldots,i_k} \neq 0 \text{ and } a_{j_1,\ldots,j_k} \neq 0 \;\Rightarrow\; i_1 + \ldots + i_k = j_1 + \ldots + j_k.$$

If $a \neq 0$, then this means that the degree of $a$ coincides with the degree of each nonzero term. As a convention, the unknowns of a homogeneous polyomial are written in capital letters.

If $F \in K[X_1, \ldots, X_{n+1}]$ is a homogeneous polynomial and $(\alpha_1 : \cdots : \alpha_{n+1}) \in \mathbb{P}^n$, then $F(\lambda\alpha_1, \ldots, \lambda\alpha_{n+1}) = \lambda^d F(\alpha_1, \ldots, \alpha_{n+1})$, where $d = \deg(F)$. The equation $F(\alpha_1, \ldots, \alpha_{n+1}) = 0$ thus may be interpreted by saying that the projective point $(\alpha_1 : \cdots : \alpha_{n+1})$ is a *zero* of $F$. The set of all projectives zeros is denoted by $V_F$, similarly to the affine case.

Say that $C \subseteq \mathbb{P}^2$ is a *planar projective curve* if there exists a (homogeneous) $F \in K[X_1, X_2, X_3]$, $\deg(F) \geq 1$, such that $C = V_F$.

A projective curve may be connected to an affine curve by the process of *homogenization*. The homogenization of a polynomial $f = \sum a_{ij} x_1^i x_2^j \in K[x_1, x_2]$, $d = \deg(f) \geq 0$, is the polynomial $F = \sum a_{ij} X_1^i X_2^j X_3^{d-i-j}$. Now, $(\alpha_1 : \alpha_2 : 1) \in \mathbb{P}^2$ belongs to $V_F$ if and only if $(\alpha_1, \alpha_2) \in V_f$. Hence $V_F$ may differ from $V_f$ only in points at infinity. These are the points $(\alpha_1 : \alpha_2 : 0)$ such that $\sum_{i+j=d} a_{ij} \alpha_1^i \alpha_2^j = 0$.

If $F$ is a homogenization of $f$, then $f$ is irreducible if and only if $F$ is irreducible (this is not difficult to prove). A planar projective curve $C$ is said to be *irreducible* if it may be expressed as $V_F$, where $F \in K[X_1, X_2, X_3]$ is an irreducible homogeneous polynomial. There is only one irreducible planar projective curve that may not be obtained by a homogenization of an affine (irreducible) curve, and that is the line $X_3 = 0$. This is because an irreducible homogeneous polynomial $F$ that is divisible by $X_3$ has to be a scalar multiple of $X_3$.

Let $C$ be a planar projective curve. Then there is no reasonable way how to define the coordinate ring of $C$. This is because we have to consider only those mappings $C \to K$ that give the same value for each expression of a point $\alpha \in C$ by homogeneous coordinates. Such a behaviour cannot be achieved by using polynomials only. However, if $A, B \in K[X_1, X_2, X_3]$ are homogeneous of the same degree, then $A(\alpha)/B(\alpha)$ is independent of the choice of homogeneous coordinates of $\alpha = (\alpha_1 : \alpha_2 : \alpha_3) \in \mathbb{P}^3$. This is utilized to define the *function field* $K(C)$, provided $C = V_F$, $F \in K[X_1, X_2, X_3]$ irreducible. Nonzero elements of $K(C)$ are $(A + (F))/(B + (F))$, where $A$ and $B$ are as above.

If $F$ is a homogenization of $f \in K[x_1, x_2]$, then, as may be proved, $K(V_F) \cong K(V_f)$. This means that the algebraic structure of an irreducible planar affine curve is not influenced by homogenization.

C.4. **Smoothness.** Consider a polynomial $f \in K[x_1, \ldots, x_n]$ and let $\alpha \in \mathbb{A}^n$ be such that $f(\alpha) = 0$, i.e., $\alpha \in V_f$. Say that $f$ is *smooth* or (equivalently) *nonsingular* at $\alpha$ if $(\partial f/\partial x_i)(\alpha) \neq 0$ for at least one $i \in \{1, \ldots, n\}$.

Let $C$ be a planar affine curve, $K[C] = K[x_1, x_2]/(f)$. A point $\alpha \in C$ is said to be *smooth* (or *nonsingular*) if $f$ is smooth at $\alpha$. The remaining points of $C$ are *singular*. If $\alpha \in C$ is a singular point, then it is also said that $C$ has a *singularity* at $\alpha$. An affine curve with no singularity is called *smooth (nonsingular)*.

Similarly, if $F \in K[X_1, X_2, X_3]$ is homogeneous and $\alpha \in \mathbb{P}^2$ is such that $F(\alpha) = 0$, then $F$ is said to be smooth (or nonsingular) at $\alpha$ if $(\partial F/\partial X_i)(\alpha) \neq 0$ for at least one $i \in \{1, 2, 3\}$. Notions of smoothness and singularity are being transferred to planar curves like in the affine case.

Suppose that the homogeneous polynomial $F$ is not equal to 0. Then

$$X_1 \frac{\partial F}{\partial X_1} + X_2 \frac{\partial F}{\partial X_2} + X_3 \frac{\partial F}{\partial X_3} = dF, \text{ where } d = \deg(F).$$

This can be used to prove that if $F$ is a homogenization of $f$ and $f$ is smooth at $\alpha = (\alpha_1, \alpha_2)$, then $F$ is smooth at $(\alpha_1 : \alpha_2 : 1)$. This means that the smoothness of a point of an affine curve is not influenced by homogenization.

C.5. **Places.** Let $F \in K[X_1, X_2, X_3]$ be an irreducible homogeneous polynomial. Suppose that the projective curve $C = V_F$ is smooth. If $K = \bar{K}$, then each point of $C$ determines in $K(C)$ exactly one normalized discrete valuation over $K$. The exact nature of this correspondence and its proof is beyond the extent of this overview. However, the structure of discrete valuations in $K(x)$ suggets how this correspondence may look like. Very briefly: in the affine case when $C = V_f$, $f \in K[x_1, x_2]$ irreducible, the valuation $\nu$ associated with $\alpha \in C$ treats those $\sigma \in K(C)$ that may be represented by a polynomial $g \in K[x_1, x_2]$ in such a way that $\nu(\sigma)$ indicates the degree of smoothness coincidence between $g$ and $f$. Thus $\nu(\sigma) = 0$ if $g(\alpha) \neq 0$. If $g(\alpha) = 0$ and $g$ and $f$ have different tangents, then $\nu(\sigma) = 1$. If $g(\alpha) = 0$ and the tangents coincide, then $\nu(\sigma) \geq 2$.

The correspondence described above is partly valid also for curves over $\bar{K}$ that are not smooth everywhere. What remains true is that each smooth point uniquely determines a normalized discrete valuation over $\bar{K}$. However, a singularity may determine more discrete valuations.

In context of function fields it is usual to speak about places rather than discrete valuations. A *place* is every subset of $K(C)$ that may be expressed as $\{a \in K(C); \nu(a) \geq 1\}$, where $\nu$ is a normalized discrete valuation of $K(C)$ over $K$. If $C$ is a projective curve that is smooth everywhere, then there is a natural bijection between points of $C$ and places of $\bar{K}(C)$.

The situation is more complicated if $K \neq \bar{K}$. Consider again the case of $K(x)$. Valuations of $K(x)$ over $K$ are equal to $v_p$ or $v_\infty$, where $p \in K[x]$ is irreducible. With each valuation (and thus with each place) there may be associated a positive integer that is called the *degree* of the valuation (and also of the place associated with the valuation). It turns out that $\deg(v_p) = \deg(p)$ and $\deg(v_\infty) = 1$. Note that $\deg(v_p) = 1$ if and only if $p = x - \lambda$ for some $\lambda \in K$. In $K(x)$ the places of degree one thus correspond to $K$-rational points of $\mathbb{P}^1$.

The degree may be defined for each place of a function field $K(C)$. Each smooth $K$-rational point of $C$ determines a place of degree one. If $C$ is an irreducible projective planar curve that is smooth at every $K$-rational point, then there is a natural bijection between $K$-rational points of $C$ and places of degree one.

To get a feeling what are places of degree $> 1$ consider first $K(x)$ again. If $\deg(p) > 1$ and $p \in K[x]$ is irreducible, then the place of $p$ is naturally associated with all roots of the polynomial $p$. There are thus more points of $\mathbb{P}^1$ that correspond to the place of $p$.

Something similar is true for places of a smooth curve over $K$. For simplicity let us formulate this just for affine points. Suppose that $C = V_f$ is a smooth affine curve, $f \in K[x_1, x_2]$ irreducible. Then $(\alpha_1, \alpha_2) \in C$ and $(\beta_1, \beta_2) \in C$ correspond to the same place if and only if there exists a field $L$, $K \leq L \leq \bar{K}$, and a $K$-automorphism $\psi$ of $L$ such that $\psi(\alpha_i) = \beta_i$ for both $i \in \{1, 2\}$. Recall that $K$-automorphisms are those automorphisms which fix each element of $K$.

With a little knowledge of field theory it is apparent that $L = \bar{K}$ may be always assumed. However, it is also clear that assuming $[L : K] < \infty$ is always possible too.

When working with curves it is usual to assume that the field $K$ is *perfect* (either $\mathrm{char}(K) = 0$, or $\mathrm{char}(K) = p > 0$ and the mapping $\lambda \mapsto \lambda^p$ is an automorphism of $K$). The connection between places and $K$-automorphisms, as described above, assumes that $K$ is perfect.

If $K = \mathbb{R}$ and $\bar{K} = \mathbb{C}$, then each place is either of degree 1 or degree 2. In the latter case $(\alpha_1, \alpha_2)$ forms a pair with $(\bar{\alpha}_1, \bar{\alpha}_2)$, where $\overline{a + b\mathrm{i}} = a - b\mathrm{i}$.