This is Chapter 4 by Gerhard Frey and Tanja Lange of the Handbook of Elliptic and Hyperelliptic Curve Cryptography, Henri Cohen, Christophe Doche, and Gerhard Frey, Editors, CRC Press 2006.

Chapter 4

Background on Curves and Jacobians

Gerhard Frey and Tanja Lange

Contents in Brief

This chapter introduces the main characters of this book — curves and their Jacobians. To this aim we give a brief introduction to algebraic and arithmetic geometry. We first deal with arbitrary varieties and abelian varieties to give the general definitions in a concise way. Then we concentrate on Jacobians of curves and their arithmetic properties, where we highlight elliptic and hyperelliptic curves as main examples. The reader not interested in the mathematical background may skip the complete chapter as the chapters on implementation summarize the necessary mathematical properties. For full details and proofs we refer the interested reader to the books [CAFL 1996, FUL 1969, LOR 1996, SIL 1986, STI 1993, ZASA 1976].

Throughout this chapter let K denote a *perfect field* (cf. Chapter 2) and $\overline{K}$ its algebraic closure. Let L be an extension field of K. Its absolute Galois group $\mathrm{Aut}_L(\overline{L})$ is denoted by G_L.

4.1 Algebraic varieties

We first introduce the basic notions of algebraic geometry in projective and affine spaces.

4.1.1 Affine and projective varieties

Before we can define curves we need to introduce the space where they are defined and it is also useful to have coordinates at hand.

4.1.1.a Projective space

We shall fix a field K as above. As a first approximation of the *n-dimensional projective space* $\mathbb{P}^n/K := \mathbb{P}^n$ *over* K we describe its set of $\overline{K}$-rational points as the set of $(n+1)$-tuples

$$\mathbb{P}^n(\overline{K}) := \big\{(X_0 : X_1 : \ldots : X_n) \mid X_i \in \overline{K}, \text{ at least one } X_i \text{ is nonzero}\big\}/\sim$$

where $\sim$ is the equivalence relation

$$(X_0 : X_1 : \ldots : X_n) \sim (Y_0 : Y_1 : \ldots : Y_n) \Longleftrightarrow \exists\, \lambda \in \overline{K}\ \ \forall i : X_i = \lambda Y_i.$$

The coordinates are called *homogeneous coordinates*. The equivalence classes are called *projective points*. Next we endow this set with a K-rational structure by using Galois theory.

Definition 4.1 Let L be an extension field of K contained in $\overline{K}$. Its absolute Galois group G_L operates on $\mathbb{P}^n(\overline{K})$ via the action on the coordinates. Obviously, this preserves the equivalence classes of $\sim$. The set of L-rational points $\mathbb{P}^n(L)$ is defined to be equal to the subset of $\mathbb{P}^n$ fixed by G_L. In terms of coordinates this means:

$$\mathbb{P}^n(L) := \big\{(X_0 : \ldots : X_n) \in \mathbb{P}^n \mid \exists \lambda \in \overline{K}\ \ \forall i : \lambda X_i \in L\big\}.$$

Note that in this definition for an L-rational point one does not automatically have $X_i \in L$. However, if $X_j \neq 0$ then $\forall i : X_i/X_j \in L$.

Let $P \in \mathbb{P}^n(\overline{K})$. The smallest extension field L of K such that $P \in \mathbb{P}^n(L)$ is denoted by $K(P)$ and called the *field of definition of* P. One has

$$K(P) = \bigcap_{G_L \cdot P = P} L.$$

Let $S \subset \mathbb{P}^n(\overline{K})$ and L be a subfield of $\overline{K}$ containing K. Then S is called *defined over* L if and only if for all $P \in S$ the field $K(P)$ is contained in L, or, equivalently, $G_L \cdot S = S$.

Remark 4.2 Let L be any extension field of K, not necessarily contained in $\overline{K}$. We can define points in the n-dimensional projective space over L in an analogous way and an embedding of $\overline{K}$ into $\overline{L}$ induces a natural inclusion of points of the projective space over K to the one over L. This is a special case of *base change*.

To be more rigorous, one should not only look at the points of $\mathbb{P}^n$ over extension fields of K as sets, but endow $\mathbb{P}^n$ with the structure of a topological space with respect to the Zariski topology. This will explain the role of the base field K much better.

First recall that a polynomial $f(X_0, \ldots, X_n) \in K[X_0, \ldots, X_n]$ is called *homogeneous of degree* d if it is the sum of monomials of the same degree d. This is equivalent to requiring that $f(\lambda X_0, \ldots, \lambda X_n) = \lambda^d f(X_0, \ldots, X_n)$ for all $\lambda \in \overline{K}$. Especially, this implies that the set

$$D_f(L) := \{P \in \mathbb{P}^n(L) \mid f(P) \neq 0\}$$

is well defined.

One defines a topology on $\mathbb{P}^n(\overline{K})$ by taking the sets $D_f(\overline{K}) =: D_f$ as basic *open sets*. The L-rational points are denoted by $D_f(L) = \mathbb{P}^n(L) \bigcap D_f$. To describe *closed sets* we need the notion

of homogeneous ideals. An *ideal* $I \subseteq K[X_0, X_1, \ldots, X_n]$ *is homogeneous* if it is generated by homogeneous polynomials. For $I \neq \langle X_0, \ldots, X_n \rangle$, define

$$V_I := \{P \in \mathbb{P}^n(\overline{K}) \mid f(P) = 0,\ \forall f \in I\}$$

and $V_I(L) = V_I \bigcap \mathbb{P}^n(L)$. One sees immediately that V_I is well defined. So a subset $S \subset \mathbb{P}^n(\overline{K})$ is closed with respect to the Zariski topology attached to the projective space over K if it is the set of simultaneous zeroes of homogeneous polynomials lying in $K[X_0, \ldots, X_n]$.

Example 4.3 The set of points of the projective n-space $\mathbb{P}^n$ and the empty set $\emptyset$ are closed sets as they are the roots of the constant polynomials 0 and 1. By the same argument they are also open sets.

Example 4.4 Let $f \in K[X_0, X_1, \ldots, X_n]$ be a homogeneous polynomial. The closed set $V_{(f)}$ is called a *hypersurface*.

Example 4.5 Define $U_i := D_{X_i}$, thus

$$U_i(L) = \big\{(X_0 : X_1 : \ldots : X_n) \in \mathbb{P}^n(L) \mid X_i \neq 0\big\}$$

and let $W_i := V_{(X_i)}$ with

$$W_i(L) = \big\{(X_0 : X_1 : \ldots : X_n) \in \mathbb{P}^n(L) \mid X_i = 0\big\}.$$

The U_i are open sets, the W_i are closed.

Example 4.6 Let $(k_0, \ldots, k_n) \in K^{n+1}$ and not all $k_i = 0$. Take $f_{ij}(X_0, \ldots, X_n) := k_j X_i - k_i X_j$ and $I = \big(\{f_{ij} \mid 0 \leqslant i, j \leqslant n\}\big)$. Obviously, I is a homogeneous ideal and taking $(k_0 : \ldots : k_n)$ as a homogeneous point, I is independent of the representative. Then $V_I(L) = \big\{(k_0 : \ldots : k_n)\big\},\ \forall L$. This shows that K-rational points are closed with respect to the Zariski topology. This is not true if P is not defined over K. The smallest closed set containing P is the G_K-orbit $G_K \cdot P$.

From now on we write X for $(X_0, \ldots, X_n)$. If $T \subset K[X]$ is a finite set of homogeneous polynomials we define $V(T)$ to be the intersection of the $V_{(f_i)}, f_i \in T$. Let $I = (T)$ be the ideal generated by the f_i. Then $V(T) = V_I$.

4.1.1.b Affine space

As in the projective space we begin with the set of $\overline{K}$-rational points of the *affine space of dimension* n *over* K given by the set of n-tuples

$$\mathbb{A}^n := \big\{(x_1, \ldots, x_n) \mid x_i \in \overline{K}\big\}.$$

The set of L-rational points is given by

$$\mathbb{A}^n(L) := \big\{(x_1, \ldots, x_n) \mid x_i \in L\big\}$$

which is the set of G_L-invariant points in $\mathbb{A}^n(\overline{K})$ under the natural action on the coordinates.

As in the projective case one has to consider $\mathbb{A}^n$ as a topologic space with respect to the Zariski topology, defined now in the following way: For $f \in K[x_1, \ldots, x_n]$ let

$$D_f(L) := \{P \in \mathbb{A}^n(L) \mid f(P) \neq 0\}$$

and take these sets as base for the open sets.

Closed sets are given in the following way: for an ideal $I \subseteq K[x_1, \ldots, x_n]$ let

$$V_I(L) = \{P \in \mathbb{A}^n(L) \mid f(P) = 0,\ \forall f \in I\}.$$

A set $S \subset \mathbb{A}^n$ is closed if there is an ideal $I \subseteq K[x_1, \ldots, x_n]$ with $S = V_I$.

Example 4.7 Let $(k_1, \ldots, k_n) \in \mathbb{A}^n(K)$ and put $f_i = x_i - k_i$ and $I = \big(\{f_i \mid 1 \leqslant i \leqslant n\}\big)$. Then $V_I = \big\{(k_1, \ldots, k_n)\big\}$. Hence, the K-rational points are closed.

Please note, if $P \in \mathbb{A}^n \smallsetminus \mathbb{A}^n(K)$ the set $\{P\}$ is not closed.

Remark 4.8 For closed $S \subset \mathbb{A}^n$ assume that $S = V_I$. The ideal I is not uniquely determined by S. Obviously there is a maximal choice for such an ideal, and it is equal to the *radical ideal* (cf. [ZASA 1976, pp. 164]) defined as

$$\sqrt{I} = \big\{f \in K[x_1, \ldots, x_n] \mid \exists k \in \mathbb{N} \text{ with } f^k \in I\big\}.$$

As in the projective case we take x as a shorthand for $(x_1, \ldots, x_n)$.

4.1.1.c Varieties and dimension

To define varieties we use the definition of irreducible sets. A subset S of a topological space is called *irreducible* if it cannot be expressed as the union $S = S_1 \cup S_2$ of two proper subsets closed in S. We additionally define that the empty set is not irreducible.

Definition 4.9 Let V be an affine (projective) closed set. One calls V an *affine (projective) variety* if it is irreducible.

Example 4.10 The affine 1-space $\mathbb{A}^1$ is irreducible because $K[x_1]$ is a principal ideal domain and so every closed set is the set of zeroes of a polynomial in x_1. Therefore, any closed set is either finite or equal to $\mathbb{A}^1$. Since $\mathbb{A}^1$ is infinite it cannot be the union of two proper closed subsets.

From commutative algebra we get a criterion for when a closed set is a variety.

Proposition 4.11 A subset V of $\mathbb{A}^n$ (resp. $\mathbb{P}^n$) is an affine (projective) variety if and only if $V = V_I$ with I a (homogeneous) prime ideal in $K[x]$ (resp. $K[X]$).

We recall that the Zariski topology is defined relative to the ground field K. For extension fields L and given embeddings σ of $\overline{K}$ into $\overline{L}$ fixing K we have induced embeddings of $\mathbb{P}^n/K \to \mathbb{P}^n/L$. Due to the obvious embedding of $K[X]$ into $L[X]$ and as the topology depends on these polynomial rings, we can try to compare the Zariski topologies of affine and projective spaces over K with corresponding ones over L.

If L is arbitrary, a closed set in the space over K may not remain closed in the space over L.

But if L is algebraic over K and if S is closed in the affine (projective) space over K then its embedding $\sigma \cdot S$ is closed over L. Namely, if $S = V_I$ with $I \subseteq K[x]$ (resp. $K[X]$) then $\sigma \cdot S = V_{I \cdot L[x]}$ (resp. $\sigma \cdot S = V_{I \cdot L[X]}$).

But varieties over K do not have to be varieties over L since for prime ideals I in $K[x]$ it may not be true that $I \cdot L[x]$ is a prime ideal.

Example 4.12 Consider $I = (x_1^2 - 2x_2^2) \subseteq \mathbb{Q}[x_1, x_2]$. Over $\mathbb{Q}(\sqrt{2})$ the variety V_I splits because $x_1^2 - 2x_2^2 = (x_1 - \sqrt{2}x_2)(x_1 + \sqrt{2}x_2)$. Therefore, the property of a closed set being a variety depends on the field of consideration.

Example 4.13 Let V be an affine variety, i.e., a closed set in some $\mathbb{A}^n$ for which the defining ideal I is prime in $K[x]$. The m-fold Cartesian product V^m is also a variety, embedded in the affine space $\mathbb{A}^{nm}$. For affine coordinates choose $(x_1^1, \ldots, x_n^1, \ldots, x_1^m, \ldots, x_n^m)$, define $I_i \subseteq K[x^i]$ obtained from I by replacing x_j by x_j^i. Then the ideal of V^m is given by $\langle I_1, \ldots, I_m \rangle$.

Definition 4.14 A variety V of the affine (projective) space $\mathbb{A}^n$ ($\mathbb{P}^n$) over K is called *absolutely irreducible* if it is irreducible as closed set with respect to the Zariski topology of the corresponding spaces over $\overline{K}$.

Example 4.15

(i) The n-dimensional spaces $\mathbb{A}^n$ and $\mathbb{P}^n$ are absolutely irreducible varieties as they correspond to the prime ideal (0).

(ii) The sets $V_{(f)}$ and $V_{(F)}$ with $f \in K[x]$ and $F \in K[X]$ are absolutely irreducible if and only if f and F are absolutely irreducible polynomials, i.e., they are irreducible over $\overline{K}$.

(iii) Let S be a *finite* set in an affine or projective space over K. The set S is absolutely irreducible if and only if it consists of one (K-rational) point.

Example 4.16 Let $f(x_1, x_2) = x_2^2 - x_1^3 - a_4x_1 - a_6 \in K[x_1, x_2]$. This polynomial is absolutely irreducible, hence $V_{(f)}$ is an irreducible variety over K and over any extension field of K contained in $\overline{K}$.

The affine and the projective n-spaces are *Noetherian*, which means that any sequence of closed subsets $S_1 \supseteq S_2 \supseteq \ldots$ will eventually become stationary, i.e., there exists an index r such that $S_r = S_{r+1} = \ldots$. This holds true as any closed set corresponds to an ideal of $K[x]$ or $K[X]$, respectively, and these rings are Noetherian.

Definition 4.17 Let V be an affine (projective) variety. The *dimension* $\dim(V)$ is defined to be the supremum on the lengths of all chains $S_0 \supset S_1 \supset \cdots \supset S_n$ of distinct irreducible closed subspaces S_i of V. A variety is called a *curve* if it is a variety of dimension 1.

Example 4.18 The dimension of $\mathbb{A}^1$ is 1 as the only irreducible subsets correspond to nonzero irreducible polynomials in 1 variable. In general, $\mathbb{A}^n$ and $\mathbb{P}^n$ are varieties of dimension n.

Example 4.19 Let $0, 1 \neq f \in K[x_1, x_2]$ be absolutely irreducible. Then $V_{(f)}$ is an affine curve as the only proper subvarieties are points $P \in \mathbb{A}^2$ satisfying $f(P) = 0$.

Example 4.20 Let V be an affine variety of dimension d. Then the Cartesian product (cf. Example 4.13) V^m has dimension md by concatenating the chains of varieties.

4.1.1.d Relations between affine and projective space

Here we show how the topologies introduced for $\mathbb{P}^n$ and $\mathbb{A}^n$ are made compatible. For both spaces we defined open and closed sets via polynomials and ideals, respectively.

Let $F \in K[X_0, X_1, \ldots, X_n]$ be a homogeneous polynomial of degree d. The process of replacing

$$F(X_0, X_1, \ldots, X_n) \text{ by } F_i := F(x_1, \ldots, x_i, 1, x_{i+1}, \ldots, x_n) \in K[x_1, \ldots, x_n]$$

is called *dehomogenization with respect to* X_i. The reverse process takes a polynomial $f \in K[x]$ and maps it to

$$f_i := X_i^d f(X_0/X_i, X_1/X_i, \ldots, X_{i-1}/X_i, X_{i+1}/X_i, \ldots, X_n/X_i),$$

where d is minimal such that f_i is a polynomial in $K[X]$. By applying these transformations, we relate homogeneous (prime) ideals in $K[X]$ to (prime) ideals in $K[x]$ and conversely. So we can expect that we can relate affine spaces with projective spaces including properties of the Zariski topologies.

Example 4.21 The open sets $U_i = D_{X_i} \subset \mathbb{P}^n$ are mapped to $\mathbb{A}^n$ by dehomogenizing their defining polynomial X_i with respect to X_i. The inverse mappings are given by

$$\begin{array}{rcl} \phi_i : \mathbb{A}^n & \to & U_i \\ (x_1, \ldots, x_n) & \mapsto & (x_1 : \ldots : x_i : 1 : x_{i+1} : \ldots : x_n) \end{array}$$

Therefore, for any $0 \leqslant i \leqslant n$ we have a canonical bijection between U_i and $\mathbb{A}^n$ which is a homeomorphism as it maps closed sets of U_i to closed sets in $\mathbb{A}^n$.

The sets $U_0, \ldots, U_n$ cover the projective space $\mathbb{P}^n$. This covering is called the *standard covering*. The maps ϕ_i can be seen as inclusions $\mathbb{A}^n \subset \mathbb{P}^n$.

If V is a projective closed set such that $V = V_{I(V)}$ with homogeneous ideal $I(V) \subseteq \overline{K}[X_0, \ldots, X_n]$ we denote by V_i the set $\phi_i^{-1}(V \cap U_i)$ for $0 \leqslant i \leqslant n$. The resulting set is a closed affine set with ideal obtained by dehomogenizing all polynomials in $I(V)$ with respect to X_i. This way, V is covered by the $n+1$ sets $\phi_i(V_i)$.

For the inverse process we need a further definition:

Definition 4.22 Let $V_I \subseteq \mathbb{A}^n$ be an affine closed set. Using one of the ϕ_i, embed V_I into $\mathbb{P}^n$ by

$$V_I \subset \mathbb{A}^n \xrightarrow{\phi_i} \mathbb{P}^n.$$

The *projective closure* $\overline{V}_I$ of V_I is the closed projective set defined by the ideal $\overline{I}$ generated by the homogenized polynomials $\{f_i \mid f \in I\}$.

The points added to get the projective closure are called *points at infinity*. Note that in the definition we need to use the ideal *generated* by the f_i's, a set of generators of I does not automatically homogenize to a set of generators of $\overline{I}$. These processes lead to the following lemma that describes the relation between affine and projective varieties.

Lemma 4.23 We choose one embedding ϕ_i from $\mathbb{A}^n$ to $\mathbb{P}^n$ and identify $\mathbb{A}^n$ with its image. Let $V \subseteq \mathbb{A}^n$ be an affine variety, then $\overline{V}$ is a projective variety and

$$V = \overline{V} \cap \mathbb{A}^n.$$

Let $V \subseteq \mathbb{P}^n$ be a projective variety, then $V \cap \mathbb{A}^n$ is an affine variety and either

$$V \cap \mathbb{A}^n = \emptyset \text{ or } V = \overline{V \cap \mathbb{A}^n}.$$

If V is a projective variety defined over K then $V \cap \mathbb{A}^n$ is empty or an affine variety defined over K. There is always at least one i such that $V \cap \phi_i \mathbb{A}^n =: V_{(i)}$ is nonempty. We call $V_{(i)}$ a *nonempty affine part of* V.

For example, let $C \subset \mathbb{P}^n$ be a projective curve. The intersections $C \cap U_i$ lead to affine curves $C_{(i)}$. Starting from an affine curve $C_a \subset \mathbb{A}^n$ one can embed the points of C_a into $\mathbb{P}^n$ via ϕ_i. The result will not be closed in the Zariski topology of $\mathbb{P}^n$ so one needs to include points from $\mathbb{P}^n \setminus U_i$ to obtain the projective closure $\overline{C}_a$.

Example 4.24 Consider the projective line $\mathbb{P}^1$. It is covered by two copies of the affine line $\mathbb{A}^1$. When embedding $\mathbb{A}^1$ in $\mathbb{P}^1$ via ϕ_0 we miss a single point $(0:1)$ which is called the *point at infinity* denoted by ∞.

Example 4.25 Let V be a projective variety embedded in $\mathbb{P}^n$. To define the m-fold Cartesian product one uses the construction for affine varieties (cf. Example 4.13) for affine parts V_a and "glues them together."

Warning: it is not possible to embed V^m in $\mathbb{P}^{mn}$ in general. One has to use constructions due to Segre [HAR 1977, pp. 13] and ends up in a higher dimensional space.

4.2 Function fields

Definition 4.26 Let V be an affine variety in the n-dimensional space $\mathbb{A}^n$ over K with corresponding prime ideal I. Denote by

$$K[V] := K[x_1, \ldots, x_n]/I$$

the quotient ring of $K[x_1, \ldots, x_n]$ modulo the ideal I. This is an integral domain, called the coordinate ring of V. The *function field* $K(V)$ *of* V is the quotient field

$$K(V) := \mathrm{Quot}(K[V]).$$

The maximal algebraic extension of the field K contained in $K(V)$ is called the *field of constants of* $K(V)/K$.

Definition 4.27 Let V be a projective variety over K. Let $V_a \subseteq \mathbb{A}^n$ be a nonempty affine part of V. Then the *function field* $K(V)$ is defined as $K(V_a)$.

One can check that $K(V)$ is independent of the choice of the affine part V_a. Thus, the notation $K(V)$ makes sense. But note that $K[V_a]$ depends on the choice of V_a.

Obviously, the elements $f \in K(V)$ can be represented by fractions of polynomials $f = g/h$, $f, g \in K[x_1, \ldots, x_n]$ or as fractions of homogeneous polynomials of the same degree $f = g/h$, $f, g \in K[X_0, X_1, \ldots, X_n]$. Then functions $f_1 = g_1/h_1$ and $f_2 = g_2/h_2$ are equal if $g_1h_2 - g_2h_1 \in I(V)$.

In Example 4.12, the splitting was induced by an algebraic extension of the ground field. We can formulate a criterion for V to be absolutely irreducible:

Proposition 4.28 A variety V is absolutely irreducible if and only if K is algebraically closed in $K(V)$, i.e., K is the full constant field of $K(V)$ (cf. [STI 1993, Cor. III.6.7]).

Example 4.29 Consider $\mathbb{A}^n$ as affine part of $\mathbb{P}^n$. Its coordinate ring $K[\mathbb{A}^n] = K[x_1, \ldots, x_n]$ is the polynomial ring in n variables. The function field of $\mathbb{P}^n$ is the field of rational functions in n variables.

From now on, we assume that V is absolutely irreducible.

Let L be an algebraic extension field of K. As pointed out above the set V is closed under the Zariski topology related to the new ground field L and again irreducible by assumption. We denote this variety by V_L. We get

Proposition 4.30 If V is affine then $K[V_L] = K[V] \cdot L$. If V is affine or projective then $K(V_L) = K(V) \cdot L$.

The proof of this proposition follows immediately from the fact that for affine V with corresponding prime ideal I we get $V_L = V_{I \cdot L[x]}$.

Example 4.31 Consider the projective curve $C = \mathbb{P}^1$ and the affine part $C_a = \mathbb{A}^1$. For any field $K \subseteq L \subseteq \overline{K}$ the coordinate ring of C_a is the polynomial ring in one variable $L[C_a] = L[x_1]$ and the function field is the function field in one variable $L(x_1)$.

A function field $K(V)$ of a projective variety V is finitely generated. Since K is perfect the extension is also separably generated. Therefore, the transcendence degree of $K(V)/K$ is finite.

Lemma 4.32 Let $K(V)$ be the function field corresponding to the projective variety V. The dimension of V is equal to the transcendence degree of $K(V)$.

4.2.1 Morphisms of affine varieties

We want to define maps between affine varieties that are continuous with respect to the Zariski topologies. We shall call such maps *morphisms*. We begin with $V = \mathbb{A}^n$.

Definition 4.33 A *morphism φ from $\mathbb{A}^n$ to the affine line $\mathbb{A}^1$* is given by a polynomial $f(x) \in K[x]$ and defined by

$$\begin{array}{rcl} \varphi : \mathbb{A}^n & \to & \mathbb{A}^1 \\ P = (a_1, \ldots, a_n) & \mapsto & f\big((a_1, \ldots, a_n)\big) =: f(P). \end{array}$$

One sees immediately that f is uniquely determined by φ.

To ease notation we shall identify f with φ. Hence the set of morphisms from $\mathbb{A}^n$ to the affine line is identified with $K[x]$. In fact we can make the set of morphisms to a K-algebra in the usual way by adding and multiplying values. As K-algebra it is then isomorphic to $K[x]$.

As desired, the map f is continuous with respect to the Zariski topology. It maps closed sets to closed sets, varieties to varieties, and for extension fields L of K we get $f\left(\mathbb{A}^n(L)\right) \subset \mathbb{A}^1(L)$.

Definition 4.34 A *morphism φ from $\mathbb{A}^n$ to $\mathbb{A}^m$* (for $n, m \in \mathbb{N}$) is given by an m-tuple

$$\big(f_1(x), \ldots, f_m(x)\big)$$

of polynomials in $K[x]$ mapping $P \in \mathbb{A}^n$ to $\big(f_1(P), \ldots, f_m(P)\big)$.

Since φ is determined by $f_1, \ldots, f_m$, the set of morphisms from $\mathbb{A}^n$ to $\mathbb{A}^m$ can be identified with $K[x]^m$. Again one checks without difficulty that morphisms are continuous with respect to the Zariski topology and map varieties to varieties.

Let V be an affine variety in $\mathbb{A}^n$ with corresponding prime ideal $I \subset K[x]$.

Definition 4.35 A *morphism from $V \subset \mathbb{A}^n$ to a variety $W \subset \mathbb{A}^m$* is given by the restriction to V of a morphism from $\mathbb{A}^n$ to $\mathbb{A}^m$ with image in W.

We denote the set of morphisms from V to W by $\mathrm{Mor}_K(V, W)$.

Example 4.36 As basic example take $W = \mathbb{A}^1$. For $V = \mathbb{A}^1$ we already have $\mathrm{Mor}_K(\mathbb{A}^1, \mathbb{A}^1) = K[x]$. For an arbitrary variety $V = V_I$ one has that $\mathrm{Mor}_K(V, \mathbb{A}^1)$ is as K-algebra isomorphic to $K[V] = K[x]/I$.

Remark 4.37 Take $\varphi \in \mathrm{Mor}_K(V, W)$ and $f \in \mathrm{Mor}_K(W, \mathbb{A}^1) = K[W]$. Then $f \circ \varphi$ is an element of $\mathrm{Mor}_K(V, \mathbb{A}^1) = K[V]$, and so we get an *induced K-algebra morphism*

$$\varphi^* : K[W] \to K[V].$$

The morphism φ^* is injective if and only if φ is surjective. If φ^* is surjective then φ is injective.

Definition 4.38 The map φ is an isomorphism if and only if φ^* is an isomorphism. This means that the inverse map of φ is again a morphism, i.e., given by polynomials.

Two varieties V and W are called isomorphic if there exists an isomorphism from V to W, and we have seen that this is equivalent to the fact that $K[V]$ is isomorphic to $K[W]$ as K-algebra.

Example 4.39 Assume that $\mathrm{char}(K) = p > 0$. Then the exponentiation with p is an automorphism ϕ_p of K since K is assumed to be perfect. The map ϕ_p is called the (absolute) Frobenius automorphism of K (cf. Section 2.3.2).

We can extend ϕ_p to points of projective spaces over K by sending the point $(X_0, \ldots, X_n)$ to $(X_0^p, \ldots, X_n^p)$. We apply ϕ_p to polynomials over K by applying it to the coefficients.

If V is a projective variety over K with ideal I we can apply ϕ_p to I and get a variety $\phi_p(V)$ with ideal $\phi_p(I)$. The points of V are mapped to points on $\phi_p(V)$.

The corresponding morphism from V to $\phi_p(V)$ is called the *Frobenius morphism* and is again denoted by ϕ_p. We note that ϕ_p is *not* an isomorphism as the polynomial rings $K[V]/K[\phi_p(V)]$ form a proper inseparable extension.

4.2.2 Rational maps of affine varieties

Let $V \subset \mathbb{A}^n$ be an affine variety with ideal $I = I(V)$ and take $\varphi \in K[V]$ with representing element $f \in K[x]$.

By definition, the set D_f consists of the points P in $\mathbb{A}^n$ in which $f(P) \neq 0$. It is open in the Zariski topology of $\mathbb{A}^n$, and hence $U_\varphi := D_f \cap V$ is open in V. Its complement V_φ in V is the zero locus of φ. It is not equal to V if and only if U_φ is not empty, and this is equivalent to $f \notin I$.

We assume now that $f \notin I$. For $P \in U_\varphi$ define $(1/\varphi)(P) := f(P)^{-1}$.

Definition 4.40 Assume that U is a nonempty open set of an affine variety V and let the map r_U be given by

$$\begin{array}{rccc} r_U : & U & \to & \mathbb{A}^1 \\ & P & \mapsto & (\psi/\varphi)(P) \end{array}$$

for some $\psi, \varphi \in K[V]$ and $U \subset U_\varphi$. Then r_U is a *rational map from V to $\mathbb{A}^1$* with *definition set U*.

We introduce an equivalence relation on rational maps: for given V the rational map r_U is equivalent to $r'_{U'}$ if for all points $P \in U \cap U'$ we have: $r_U(P) = r'_{U'}(P)$.

Definition 4.41 The equivalence class of a rational map from V to $\mathbb{A}^1$ is called a *rational function* on V.

Proposition 4.42 Let V be an affine variety. The set of rational functions on V is equal to $K(V)$. The addition (resp. multiplication) in $K(V)$ corresponds to the addition (resp. multiplication) of rational functions defined by addition (resp. multiplication) of the values.

Let $V \subset \mathbb{A}^n$. As in the case of morphisms we can extend the notion of rational maps from the case $W = \mathbb{A}^1$ to the general case that $W \subset \mathbb{A}^m$ is a variety:

Definition 4.43 A *rational map r from V to W* is an m-tuple of rational functions $(r_1, \ldots, r_m)$ with $r_i \in K(V)$ having representatives R_i defined on a nonempty open set $U \subset V$ with $R(U) := \big(R_1(U), \ldots, R_m(U)\big) \subset W$.

A rational map r from V to W is *dominant* if (with the notation from above) $R(U)$ is dense in W, i.e., if the smallest closed subset in W containing $R(U)$ is equal to W.

A rational map $r : V \to W$ is *birational* if there exists an inverse rational map $r' : W \to V$ such that $r' \circ r$ is equivalent to Id_V and $r \circ r'$ is equivalent to Id_W.

If there exists a birational map from V to W the varieties are called *birationally equivalent*.

Example 4.44 Consider the rational maps

$$r^{ij} : \mathbb{A}^n \to \mathbb{A}^n,\ r^{ij} = (r_1^{ij}, \ldots, r_n^{ij}),$$

where (for $i \leqslant j$)

$$r_k^{ij}(x_1,\ldots,x_n) := \begin{cases} x_k/x_j, & k < i \\ 1/x_j, & k = i \\ x_{k-1}/x_j, & i < k \leqslant j \\ x_k/x_j, & j < k. \end{cases}$$

The case $i > j$ works just the same. For fixed j and arbitrary i the maps r^{ij} are defined on D_{x_j}.

Using the embeddings ϕ_i of $\mathbb{A}^n$ into $\mathbb{P}^n$ one has the description

$$r^{ij} = \phi_j^{-1} \circ \phi_i.$$

The inverse map is just r^{ji} and so r^{ij} represents a birational map regular on $D_{x_j} \cap D_{x_i}$. It describes the coordinate transition of affine coordinates with respect to ϕ_i to affine coordinates with respect to ϕ_j on $\mathbb{P}^n$.

Proposition 4.45 Assume that the rational map r from V to W is dominant. Then the composition of r with elements in $K(W)$ induces a field embedding r^* of $K(W)$ into $K(V)$ fixing elements in K, generalizing the definition made for morphisms in Remark 4.37.

If r is birational then $K(V)$ is isomorphic to $K(W)$ as K-algebra.

Example 4.46 A projective curve C corresponds to a function field of transcendence degree 1. Since K is perfect, there are elements $x_1, x_2 \in K(C)$ and an irreducible polynomial $f(x_1, x_2)$ such that $K(C) = \mathrm{Quot}\big(K[x_1,x_2]/\big(f(x_1,x_2)\big)\big)$. Hence, C (and every affine part of dimension 1 of C) is birationally equivalent to the plane curve $V_{(f)}$ and of course to its projective closure $\overline{V}_{(f)} \subset \mathbb{P}^2$.

Example 4.47 We consider again the Frobenius morphism ϕ_p from Example 4.39. The map

$$\phi_p^* : K\big(\phi_p(V)\big) \to K(V)$$

has as its image $K(V)^p$ since the coordinate functions of V are exponentiated by p under the map ϕ_p.

4.2.3 Regular functions

We continue to assume that V is an affine variety.

Definition 4.48 A rational function $f \in K(V)$ is *regular at a point* $P \in V$ if f has as representative a rational map $\tilde{f}$ with set of definition U containing P.

In other words f is regular at $P \in V$ if there is an open neighborhood U of P where $f_{|U} = (g/h)_{|U}$ for $g, h \in K[x]$ and $P \in D_h$. If this is the case we say that f is defined at P with value $f(P) = g(P)/h(P)$.

Definition 4.49 For two varieties $V \subset \mathbb{A}^n$, $W \subset \mathbb{A}^m$ a rational map $r : V \to W$ *is regular at* P if there is a nonempty open set U of V containing P such that the restriction of r to U is given by an m-tuple of rational maps defined on U.

In other words: a map r is regular if locally it can be represented via m-tuples of quotients of polynomials in $K[x]$ which are defined at $P \in U$.

4.2.4 Generalization to projective varieties

We want to generalize the definitions of morphisms to projective varieties.

Definition 4.50 Let $V \subset \mathbb{P}^n$ and $W \subset \mathbb{P}^m$ be projective varieties. Let φ be a map from V to W such that the following holds:

(i) The set $V = \bigcup_{i=1}^{n} V_i$ with $V_i = V \cap U_i$ the standard affine parts of V.

(ii) The morphism $\varphi_i := \varphi_{|V_i}$ is an affine morphism to an affine part W_i of W.

(iii) The polynomials $\left(f_1^i(x), \ldots, f_m^i(x)\right)$ describing φ on V_i with respect to the standard affine coordinates are transformed into the polynomials $\left(f_1^j(x), \ldots, f_m^j(x)\right)$ describing φ_j in the standard affine coordinates related to V_j under the coordinate transformation considered in Example 4.44.

Then *φ is a morphism from V to W*: $\varphi \in \mathrm{Mor}_K(V, W)$.

The notions of rational functions of projective varieties V and of regularity in a point P of such functions are easier to define since they are local definitions.

We define rational maps as equivalence classes of rational maps defined on the affine parts of V compatible with the transition maps on intersections of standard affine pieces U_i (cf. Example 4.44). To define regularity at P we first choose an affine part V_i of V containing P and then require that there is an open neighborhood U of P in V_i such that the rational map obtained by restriction is defined on U.

A rational map from W to $\mathbb{P}^1$ is called a *rational function of V*.

Proposition 4.51 The set of rational functions on a projective variety V forms a field isomorphic to $K(V)$ which is equal to the field of rational functions on a nonempty affine part of V.

A function $f : V \to K$ is regular at $P \in V$ if there is an open neighborhood U of P where $f = g/h$ for homogeneous polynomials $g, h \in K[X]$ of the same degree and $h(Q) \neq 0,\ \forall Q \in U$.

4.3 Abelian varieties

We want to use the concepts introduced above for a structure that will become most important for the purposes of the book.

Remark 4.52 Already in the definition we shall restrict ourselves to the cases that will be considered in the sequel. So we shall assume throughout the whole section that all varieties are defined over K and are *absolutely irreducible.*

4.3.1 Algebraic groups

We combine the concept of groups with the concept of varieties in a functorial way.

Definition 4.53 An (absolutely irreducible) *algebraic group $\mathcal{G}$ over a field K* is an (affine or projective) absolutely irreducible variety defined over K together with three additional ingredients:

(i) the addition, i.e., a morphism
$$m : \mathcal{G} \times \mathcal{G} \to \mathcal{G},$$

(ii) the inverse, i.e., a morphism
$$i : \mathcal{G} \to \mathcal{G},$$

(iii) the neutral element, i.e., a K-rational point

$$0 \in \mathcal{G}(K),$$

satisfying the usual group laws:

$$m \circ (\mathrm{Id}_{\mathcal{G}} \times m) = m \circ (m \times \mathrm{Id}_{\mathcal{G}}) \text{ (associativity)},$$

$$m_{|\{0\}\times\mathcal{G}} = p_2,$$

where p_2 is the projection of $\mathcal{G} \times \mathcal{G}$ on the second argument, and

$$m \circ (i \times \mathrm{Id}_{\mathcal{G}}) \circ \delta_{\mathcal{G}} = c_0,$$

where $\delta_{\mathcal{G}}$ is the diagonal map from $\mathcal{G}$ to $\mathcal{G} \times \mathcal{G}$ and c_0 is the map which sends $\mathcal{G}$ to 0.

Let L be an extension field of K. Let $\mathcal{G}(L)$ denote the set of L-rational points. The set $\mathcal{G}(L)$ is a group in which the sum and the inverse of elements are computed by evaluating morphisms that are defined over K, that do not depend on L, and in which the neutral element is the point 0.

A surprising fact is that if $\mathcal{G}$ is a projective variety the group law m is necessarily commutative.

Definition 4.54 Projective algebraic groups are called *abelian varieties*.

From now on we shall require m to be *commutative*. We can use a classification theorem which yields that $\mathcal{G}$ is an extension of an abelian variety by an affine (i.e., the underlying variety is affine) algebraic group. So, for cryptographic purposes we can assume that $\mathcal{G}$ is either affine or an abelian variety as by Theorem 2.23 one is interested only in (sub)groups of prime order.

Affine commutative group schemes that are interesting for cryptography are called *tori*. The reader can find the definition and an interesting discussion on how to use them for DL systems in [SIRU 2004].

Remark 4.55 To make the connection with abelian groups more obvious we replace "$m(P, Q)$" with the notation $P \oplus Q$ for $P, Q \in \mathcal{G}(\overline{K})$ and $i(P)$ by $-P$.

We shall concentrate on abelian varieties from now on and shall use as standard notation $\mathcal{A}$ instead of $\mathcal{G}$.

4.3.2 Birational group laws

Assume that we are given an abelian variety $\mathcal{A}$. Since we want to use $\mathcal{A}$ for DL systems we shall not only need structural properties of $\mathcal{A}$ but explicitly compute with its points. In general this seems to be hopeless. Results of Mumford [MUM 1966] and Lange–Ruppert [LARU 1985] show that the number of coordinate functions and the degree of the addition formulas both grow exponentially with the dimension of the abelian variety. Therefore, we have to use special abelian varieties on which we can describe the addition at least on open affine parts.

By definition $\mathcal{A}$ can be covered by affine subvarieties V_i. Choose one such $V := V_i$. For l depending on V one finds coordinate functions $X_1, \ldots, X_l$ defining V by polynomial relations

$$\big\{f_1(X_1, \ldots, X_l), \ldots, f_k(X_1, \ldots, X_l)\big\}.$$

The L-rational points $V(L) \subset \mathcal{A}(L)$ are the elements $(x_1, \ldots, x_l) \in L^l$, where the polynomials f_i vanish simultaneously. The addition law can be restricted to $V \times V$ and induces a morphism

$$m_V : V \times V \to \mathcal{A}.$$

For generic points of $V \times V$ the image of m_V is again contained in V. So m_V is given by *addition functions* $R_i \in K(X_1, \ldots, X_l; Y_1, \ldots, Y_l)$ such that for pairs of L-rational points in $V \times V$ we get

$$\big((x_1, \ldots, x_l) \oplus (y_1, \ldots, y_l)\big) = \big(R_1(x_1, \ldots, x_l; y_1, \ldots, y_l), \ldots, R_l(x_1, \ldots x_l; y_1, \ldots, y_l)\big).$$

Remark 4.56 This is a birational description of the addition law that is true outside proper closed subvarieties of $V \times V$. The set of points where this map is not defined is of small dimension and hence with high probability one will not run into it by chance. But it can happen that we use pairs of points on purpose (e.g., lying on the diagonal in $V \times V$) for which we need an extra description of m.

We shall encounter examples of abelian varieties with birational description of the group law in later chapters. In fact it will be shown that one can define abelian varieties from elliptic and hyperelliptic curves — they constitute even the main topics of this book.

4.3.3 Homomorphisms of abelian varieties

We assume that $\mathcal{A}$ and $\mathcal{B}$ are abelian varieties over K with addition laws $\oplus$ (resp. $\oplus'$). Let φ be an element of $\mathrm{Mor}_K(\mathcal{A}, \mathcal{B})$.

Example 4.57 Let $P \in \mathcal{A}(K)$ and define

$$\begin{aligned} t_P : \mathcal{A} &\to \mathcal{A} \\ Q &\mapsto P \oplus Q. \end{aligned}$$

Here, t_P is called the *translation by* P and lies in $\mathrm{Mor}_K(\mathcal{A}, \mathcal{A})$.

A surprising fact is that for all $\varphi \in \mathrm{Mor}_K(\mathcal{A}, \mathcal{B})$ we have

$$\varphi(P \oplus Q) = \varphi(P) \oplus' \varphi(Q)$$

for all points P, Q of $\mathcal{A}$ if and only if $\varphi(0)$ is the neutral element of $\mathcal{B}$. In other words every morphism from $\mathcal{A}$ to $\mathcal{B}$ is a *homomorphism* with respect to the addition laws up to the translation map $t_{-(\varphi(0))}$ in $\mathcal{B}$. The set of homomorphisms from $\mathcal{A}$ to $\mathcal{B}$ is denoted by $\mathrm{Hom}_K(\mathcal{A}, \mathcal{B})$.

Let L be an extension field of K and take $\varphi \in \mathrm{Hom}_K(\mathcal{A}, \mathcal{B})$. We get a group homomorphism $\varphi_L : \mathcal{A}(L) \to \mathcal{B}(L)$ which is given by evaluating polynomials with coefficients in K. An important observation is that φ_L commutes with the action of the Galois group G_K of K.

The set of homomorphisms $\mathrm{Hom}_K(\mathcal{A}, \mathcal{B})$ becomes a $\mathbb{Z}$-module in the usual way: for $\varphi_1, \varphi_2 \in \mathrm{Hom}_K(\mathcal{A}, \mathcal{B})$ and points P of $\mathcal{A}$ define

$$(\varphi_1 + \varphi_2)(P) := \big(\varphi_1(P) \oplus \varphi_2(P)\big).$$

In many cases it is useful to deal with vector spaces instead of modules, and so we define

$$\mathrm{Hom}_K(\mathcal{A}, \mathcal{B})^0 := \mathrm{Hom}_K(\mathcal{A}, \mathcal{B}) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

In the next chapter we shall see that $\mathrm{Hom}_K(\mathcal{A}, \mathcal{B})^0$ is a finite dimensional vector space over $\mathbb{Q}$.

Remark 4.58 Homomorphisms of abelian varieties behave in a natural way under base change: let L be an extension field of K and let $\mathcal{A}_L, \mathcal{B}_L$ be the abelian varieties obtained by scalar extension to L, $\mathrm{Hom}_L(\mathcal{A}, \mathcal{B}) := \mathrm{Hom}_L(\mathcal{A}_L, \mathcal{B}_L)$. The Galois group G_L acts in a natural way on $\mathrm{Mor}_L(\mathcal{A}_L, \mathcal{B}_L)$ and hence on $\mathrm{Hom}_L(\mathcal{A}, \mathcal{B})$.

Lemma 4.59 With the notations from above we get

(i) Let L_0 be the algebraic closure of K in L. Then $\mathrm{Hom}_L(\mathcal{A},\mathcal{B}) = \mathrm{Hom}_{L_0}(\mathcal{A},\mathcal{B})$.
(ii) For L contained in $\overline{K}$ we get $\mathrm{Hom}_L(\mathcal{A},\mathcal{B}) = \mathrm{Hom}_{\overline{K}}(\mathcal{A},\mathcal{B})^{G_L}$.

Because of the next results we can think of abelian varieties as behaving like abelian groups.

Proposition 4.60 Take $\varphi \in \mathrm{Hom}_K(\mathcal{A},\mathcal{B})$.

(i) The image $\mathrm{Im}(\varphi)$ of φ is a subvariety of $\mathcal{B}$, which becomes an abelian variety by restricting the addition law from B, i.e., it is an abelian subvariety of $\mathcal{B}$.
(ii) The kernel $\ker(\varphi)$ of φ is by definition the inverse image of $0_{\mathcal{B}}$. It is closed (in the Zariski topology) in $\mathcal{A}$. Its points consist of all points in $\mathcal{A}(\overline{K})$ that are mapped to $0_{\mathcal{B}}$ by $\varphi_{\overline{K}}$ and hence form a subgroup of $\mathcal{A}(\overline{K})$.
(iii) The kernel $\ker(\varphi)$ contains a maximal absolutely irreducible subvariety $\ker(\varphi)^0$ containing $0_{\mathcal{A}}$. This subvariety is called the *connected component of the unity of* $\ker(\varphi)$. It is an abelian subvariety of $\mathcal{A}$.
(iv) For the dimension one has

$$\dim\big(\mathrm{Im}(\varphi)\big) + \dim\big(\ker(\varphi)^0\big) = \dim(\mathcal{A}).$$

Remark 4.61 Warning: in general it is not true that the sequence of abelian groups

$$0 \to \ker(\varphi)(L) \to \mathcal{A}(L) \to \mathrm{Im}\big(\varphi(L)\big) \to 0$$

is exact. This holds, however, if $L = \overline{K}$.

4.3.4 Isomorphisms and isogenies

To study abelian varieties it is (as usual) important to have an insight into isomorphisms between them. Very closely related to isomorphisms are homomorphisms which preserve the dimension of the abelian variety. They are intensively used both in theory and in applications to cryptography.

Definition 4.62 We assume that $\mathcal{A},\mathcal{B}$ are abelian varieties over K.

(i) The map $\varphi \in \mathrm{Hom}_K(\mathcal{A},\mathcal{B})$ is an *isogeny* if and only if $\mathrm{Im}(\varphi) = \mathcal{B}$ and $\ker(\varphi)$ is finite.
(ii) The morphism φ is an *isomorphism* if and only if there is a $\psi \in \mathrm{Hom}_K(\mathcal{B},\mathcal{A})$ with $\varphi\circ\psi = \mathrm{Id}_{\mathcal{B}}$ and $\psi\circ\varphi = \mathrm{Id}_{\mathcal{A}}$. So necessarily one has $\ker(\varphi) = \{0_{\mathcal{A}}\}$.
(iii) The variety $\mathcal{A}$ *is isogenous to* $\mathcal{B}$ ($\mathcal{A} \sim \mathcal{B}$) if and only if there exists an isogeny in $\mathrm{Hom}_K(\mathcal{A},\mathcal{B})$.
(iv) The variety $\mathcal{A}$ *is isomorphic to* $\mathcal{B}$ ($\mathcal{A} \simeq \mathcal{B}$) if and only if there exists an isomorphism in $\mathrm{Hom}_K(\mathcal{A},\mathcal{B})$.

Let $\varphi \in \mathrm{Hom}_K(\mathcal{A},\mathcal{B})$ be dominant. By mapping $f \in K(\mathcal{B})$ to $f\circ\varphi$ we get an injection φ^* of $K(\mathcal{B})$ into $K(\mathcal{A})$ (cf. Remark 4.45).

Proposition 4.63 The homomorphism $\varphi \in \mathrm{Hom}_K(\mathcal{A},\mathcal{B})$ is an isogeny if and only if $\dim(\mathcal{A}) = \dim(\mathcal{B})$ and $\dim\big(\ker(\varphi)^0\big) = 0$.

Equivalently we have that φ is dominant and $K(\mathcal{A})$ is a finite algebraic extension of $\varphi^*\big(K(\mathcal{B})\big)$.

The relations $\simeq$ and $\sim$ (cf. Corollary 4.76) are equivalence relations between abelian varieties. Hence we can speak about (K-)isogeny classes (resp. (K-)isomorphism classes) of abelian varieties over K.

Definition 4.64 Let φ be an isogeny from $\mathcal{A}$ to $\mathcal{B}$. The *degree of* φ is defined as $[K(\mathcal{A}) : \varphi^*\big(K(\mathcal{B})\big)]$.

The isogeny φ is called *separable* if and only if $K(\mathcal{A})/\varphi^*\big(K(\mathcal{B})\big)$ is a separable extension. It is called *(purely) inseparable* if $K(\mathcal{A})/\varphi^*\big(K(\mathcal{B})\big)$ is purely inseparable. In this case $\ker(\varphi) = \{0\}$ but nevertheless φ is not an isomorphism in general.

As for abelian groups we can describe the abelian varieties that are isomorphic to a homomorphic image of $\mathcal{A}$.

Let $\mathcal{C}$ be a closed set (with respect to the Zariski topology) in $\mathcal{A}$ with $\mathcal{C}(\overline{K})$ a subgroup of $\mathcal{A}(\overline{K})$. Then there exists an (up to K-isomorphisms unique) abelian variety $\mathcal{B}$ defined over K and a unique $\pi := \pi_{\mathcal{C}} \in \mathrm{Hom}_K(\mathcal{A}, \mathcal{B})$ such that

- $\mathrm{Im}(\pi) = \mathcal{B}$,
- $\ker(\pi) = \mathcal{C}$ and
- $K\big(\mathcal{A})/\pi^*(K(\mathcal{B})\big)$ is separable.

Definition 4.65 With the notation from above we call $\mathcal{B} =: \mathcal{A}/\mathcal{C}$ the *quotient of* $\mathcal{A}$ *modulo* $\mathcal{C}$. Hence, $\mathcal{B}(\overline{K}) = \mathcal{A}(\overline{K})/\mathcal{C}(\overline{K})$.

For general homomorphisms $\varphi \in \mathrm{Hom}_K(\mathcal{A}, \mathcal{B})$ we get:

$$\varphi = \psi \circ \pi_{\ker(\varphi)}$$

where ψ is a purely inseparable isogeny from $\mathcal{A}/\ker(\varphi)$ to $\mathrm{Im}(\varphi)$.

Hence we can classify all abelian varieties defined over K that are separably isogenous to $\mathcal{A}$ up to isomorphisms:

Proposition 4.66 The K-isomorphism classes of abelian varieties that are K-separably isogenous to $\mathcal{A}$ correspond one-to-one to the finite subgroups $C \subseteq \mathcal{A}(\overline{K})$ that are invariant under the action of G_K. They are isomorphic to $\mathcal{A}/C$. The field $K(\mathcal{A})$ is a separable extension of $\pi^*\big(K(\mathcal{A}/C)\big)$, which is a Galois extension with Galois group canonically isomorphic to C: the automorphisms of $K(\mathcal{A})$ fixing $\pi^*\big(K(\mathcal{A}/C)\big)$ are induced by translation maps t_P with $P \in \ker(\pi)$, i.e., $\pi^*\big(K(\mathcal{A}/C)\big)$ consists of the functions on $\mathcal{A}$ that are invariant under translations of the argument by points in C.

To describe all abelian varieties that are K-isogenous to $\mathcal{A}$ we have to compose separable isogenies with purely inseparable ones. As seen the notion of finite subgroups of $\mathcal{A}(\overline{K})$ is not sufficient for this; we would have to go to the category of *group schemes* to repair this deficiency. This is beyond the scope of this introduction. For details see e.g., [MUM 1974, pp. 93].

For our purposes there is a most prominent inseparable isogeny, the *Frobenius homomorphism*. Assume that $\mathrm{char}(K) = p > 0$. We recall that we have defined the Frobenius morphism ϕ_p (cf. Example 4.39) for varieties over K. It is easily checked that $\phi_p(\mathcal{A})$ is again an abelian variety over K. By the description of ϕ_p^* it follows at once that ϕ_p is a purely inseparable isogeny of degree $p^{\dim(\mathcal{A})}$ and its kernel is $\{0\}$.

Now we consider the special case that $\mathcal{B} = \mathcal{A}$.

Definition 4.67 The homomorphisms $\mathrm{End}_K(\mathcal{A}) := \mathrm{Hom}_K(\mathcal{A}, \mathcal{A})$ are the *endomorphisms of* $\mathcal{A}$.

The set $\mathrm{End}_K(\mathcal{A})$ is a ring with composition as multiplicative structure.

Example 4.68 Assume that $K = \mathbb{F}_p$. Then ϕ_p induces the identity map on polynomials over K and so $\phi_p(\mathcal{A}) = \mathcal{A}$. Therefore, $\phi_p \in \mathrm{End}_K(\mathcal{A})$. It is called the *Frobenius endomorphism*.

A slight but important generalization is to consider $K = \mathbb{F}_q$ with $q = p^d$. Then $\phi_q := \phi_p^d$ is the relative Frobenius automorphism fixing K element wise. We can apply the considerations made above to ϕ_q and get a totally inseparable endomorphism of $\mathcal{A}$ of degree $p^{\,d\dim(\mathcal{A})}$ which is called the (relative) Frobenius endomorphism of $\mathcal{A}$.

To avoid quotient groups we introduce a further definition.

Definition 4.69 An abelian variety is *simple* if and only if it does not contain a proper abelian subvariety.

Assume that $\mathcal{A}$ is simple. It follows that $\varphi \in \mathrm{Hom}_K(\mathcal{A}, \mathcal{B})$ is either the zero map or has a finite kernel, hence its image is isogenous to $\mathcal{A}$.

Proposition 4.70 If $\mathcal{A}$ is simple then $\mathrm{End}_K(\mathcal{A})$ is a ring without zero divisors and $\mathrm{End}_K(\mathcal{A})^0 := \mathrm{End}_K(\mathcal{A}) \otimes \mathbb{Q}$ is a skew field.

One proves by induction with respect to the dimension that every abelian variety is isogenous to the direct product of simple abelian varieties. So we get

Corollary 4.71 $\mathrm{End}_K(\mathcal{A})^0$ is isomorphic to a product of matrix rings over skew fields.

4.3.5 Points of finite order and Tate modules

We come to most simple but important examples of elements in $\mathrm{End}_K(\mathcal{A})$.

For $n \in \mathbb{N}$ define

$$[n] : \mathcal{A} \to \mathcal{A}$$

as the $(n-1)$-fold application of the addition $\oplus$ to the point $P \in \mathcal{A}$. For $n = 0$ define $[0]$ as zero map, and for $n < 0$ define $[n] := -[|n|]$. By identifying n with $[n]$ we get an injective homomorphism of $\mathbb{Z}$ into $\mathrm{End}_K(\mathcal{A})$.

By definition $[n]$ commutes with every element in $\mathrm{End}_K(\mathcal{A})$ and with G_K and so lies in the center of the G_K-module $\mathrm{End}_K(\mathcal{A})$.

The kernel of $[n]$ is finite if and only if $n \neq 0$. Hence $[n]$ is an isogeny for $n \neq 0$. It is an isomorphism if $|n| = 1$.

Definition 4.72 Let $n \in \mathbb{N}$.

(i) The kernel of $[n]$ is denoted by $\mathcal{A}[n]$.

(ii) The points in $\mathcal{A}[n]$ are called *n-torsion points*.

(iii) There exists a homogeneous ideal defined over K such that $\mathcal{A}[n](\overline{K})$ is the set of points on $\mathcal{A}(\overline{K})$ at which the ideal vanishes. It is called the *n-division ideal*.

For the latter we recall that $\mathcal{A}$ is a projective variety with a fixed embedding into a projective space.

For elliptic curves (cf. Section 4.4.2.a) which are abelian varieties of dimension one the n-division ideal is a principal ideal. The generating polynomial is called the *n-division polynomial*. We will give the division polynomials explicitly in Section 4.4.5.a together with a recursive construction.

A fundamental result is

Theorem 4.73 The degree of $[n]$ is equal to $n^{2\dim(\mathcal{A})}$. The isogeny $[n]$ is separable if and only if n is prime to $\mathrm{char}(K)$. In this case $\mathcal{A}[n](\overline{K}) \simeq (\mathbb{Z}/n\mathbb{Z})^{2\dim(\mathcal{A})}$. If $n = p^s$ with $p = \mathrm{char}(K)$ then $\mathcal{A}[p^s](\overline{K}) = \mathbb{Z}/p^{ts}\mathbb{Z}$ with $t \leqslant \dim(\mathcal{A})$ independent of s.

A proof of these facts can be found in [MUM 1974, p. 64].

Definition 4.74 Let $p = \mathrm{char}(K)$.

(i) The variety $\mathcal{A}$ is called *ordinary* if $\mathcal{A}[p^s](\overline{K}) = \mathbb{Z}/p^{ts}\mathbb{Z}$ with $t = \dim(\mathcal{A})$.

(ii) If $\mathcal{A}[p^s](\overline{K}) = \mathbb{Z}/p^{ts}\mathbb{Z}$ then the abelian variety $\mathcal{A}$ has *p-rank t*.

(iii) If $\mathcal{A}$ is an elliptic curve, i.e., an abelian variety of dimension 1 (cf. Section 4.4.2.a), it is called *supersingular* if it has p-rank 0.

(iv) The abelian variety $\mathcal{A}$ is supersingular if it is isogenous to a product of supersingular elliptic curves.

Remark 4.75 If an abelian variety $\mathcal{A}$ is supersingular then it has p-rank 0. The converse is only true for abelian varieties of dimension $\leqslant 2$.

Corollary 4.76 Let φ be an isogeny from $\mathcal{A}$ to $\mathcal{B}$ of degree $n = \prod_{i=1}^{t} \ell_i^{k_i}$ with ℓ_i primes.

(i) There is a sequence φ_i of isogenies from abelian varieties $\mathcal{A}_i$ to $\mathcal{A}_{i+1}$ with $\mathcal{A}_1 = \mathcal{A}$ and $\mathcal{A}_{t+1} = \mathcal{B}$ with $\deg(\varphi_i) = \ell_i^{k_i}$ and $\varphi = \varphi_t \circ \varphi_{t-1} \circ \cdots \circ \varphi_1$.

(ii) Assume that n is prime to $\mathrm{char}(K)$. Let $B_n = \varphi\big(\mathcal{A}[n](\overline{K})\big)$. Then B_n is G_K-invariant, $\mathcal{B}/B_n$ is isomorphic to $\mathcal{A}$ and $\pi_{B_n} \circ \varphi = [n]$.

(iii) If $\mathcal{A}$ is ordinary then taking $\varphi = \phi_p$

$$[p] = \phi_p \circ \pi_{\mathcal{A}[p]} = \pi_{\phi_p(\mathcal{A}[p])} \circ \phi_p.$$

Example 4.77 Assume that $K = \mathbb{F}_p$ and that $\mathcal{A}$ is an ordinary abelian variety over K. Then there is a uniquely determined separable endomorphism $\overline{V}_p \in \mathrm{End}_K(\mathcal{A})$ called *Verschiebung* with

$$[p] = \phi_p \circ \overline{V}_p = \overline{V}_p \circ \phi_p$$

of degree $p^{\dim(\mathcal{A})}$, where ϕ_p is the absolute Frobenius endomorphism

Corollary 4.78 Let ℓ be a prime different from $\mathrm{char}(K)$ and $k \in \mathbb{N}$. Then

$$[\ell]\mathcal{A}[\ell^{k+1}] = \mathcal{A}[\ell^k].$$

We can interpret this result in the following way: the collection of groups

$$\ldots \mathcal{A}[\ell^{k+i}], \ldots, \mathcal{A}[\ell^k], \ldots$$

forms a projective system with connecting maps $[\ell^i]$ and so we can form their *projective limit* $\varprojlim \mathcal{A}[\ell^k]$. The reader should recall that the system with groups $\mathbb{Z}/\ell^k\mathbb{Z}$ has as projective limit the ℓ-adic integers $\mathbb{Z}_\ell$ (cf. Chapter 3). In fact there is a close connection:

Definition 4.79 Let ℓ be a prime different from $\mathrm{char}(K)$. The *ℓ-adic Tate module of $\mathcal{A}$* is

$$T_\ell(\mathcal{A}) := \varprojlim \mathcal{A}[\ell^k].$$

Corollary 4.80 The Tate module $T_\ell(\mathcal{A})$ is (as $\mathbb{Z}_\ell$-module) isomorphic to $\mathbb{Z}_\ell^{2\dim(\mathcal{A})}$.

4.3.6 Background on ℓ-adic representations

The torsion points and the Tate modules of abelian varieties are used to construct most important representations. The basic fact provided by Proposition 4.73 is that for all $n \in \mathbb{N}$ prime to $\mathrm{char}(K)$ the groups $\mathcal{A}[n](\overline{K})$ are free $\mathbb{Z}/n\mathbb{Z}$-modules and for primes ℓ different from $\mathrm{char}(K)$ the Tate modules $T_\ell(\mathcal{A})$ are free $\mathbb{Z}_\ell$-modules each of them having rank equal to $2\dim(\mathcal{A})$. Hence $\mathrm{Aut}_K(\mathcal{A}[n])$, respectively $\mathrm{Aut}_{\mathbb{Z}_\ell}\big(T_\ell(\mathcal{A})\big)$, can be identified (by choosing bases) with the group

of invertible $2\dim(\mathcal{A}) \times 2\dim(\mathcal{A})$-matrices over $\mathbb{Z}/n\mathbb{Z}$, respectively $\mathbb{Z}_\ell$. Likewise one can identify $\mathrm{End}_K(\mathcal{A}[n])$ and $\mathrm{End}_{\mathbb{Z}_\ell}\big(T_\ell(\mathcal{A})\big)$ with the $2\dim(\mathcal{A}) \times 2\dim(\mathcal{A})$-matrices over $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}_\ell$, respectively.

The first type of these representations relates the arithmetic of K to the arithmetic of $\mathcal{A}$ via Galois theory. This will become very important in the case that K is a finite field or a finite algebraic extension of either $\mathbb{Q}$ or a p-adic field $\mathbb{Q}_p$.

The Galois action of G_K on $\mathcal{A}(\overline{K})$ maps $\mathcal{A}[\ell^k]$ into itself and extends in a natural way to $T_\ell(\mathcal{A})$. Hence both the groups of points in $\mathcal{A}[n]$ and in $T_\ell(\mathcal{A})$ carry the structure of a G_K-module and so they give rise to representations of G_K.

Definition 4.81 For a natural number n prime to $\mathrm{char}(K)$ the *representation induced by the action of G_K on $\mathcal{A}[n]$* is denoted by $\rho_{\mathcal{A},\,n}$.

For primes ℓ prime to $\mathrm{char}(K)$ the representation induced by the action on $T_\ell(\mathcal{A})$ is denoted by $\tilde{\rho}_{\mathcal{A},\,\ell}$ and is called the *ℓ-adic Galois representation attached to $\mathcal{A}$.*

Second, we take $\varphi \in \mathrm{End}_K(\mathcal{A})$. It commutes with $[n]$ for all natural numbers and so it operates on $T_\ell(\mathcal{A})$ continuously with respect to the ℓ-adic topology. Let $T_\ell(\varphi)$ denote the corresponding element in $\mathrm{End}_{\mathbb{Z}_\ell}\big(T_\ell(\mathcal{A})\big)$.

With the results about abelian varieties we have mentioned already, it is not difficult to see that the set of points of ℓ-power order in $\mathcal{A}(\overline{K})$ is Zariski-dense, i.e., the only Zariski-closed subvariety of $\mathcal{A}$ containing all points of ℓ-power order is equal to $\mathcal{A}$ itself.

It follows that $T_\ell(\varphi) = 0$ if and only if $\varphi = 0$ and so we get an injective homomorphism T_ℓ from $\mathrm{End}_K(\mathcal{A})$ into $\mathrm{End}_{\mathbb{Z}_\ell}\big(T_\ell(\mathcal{A})\big)$.

Much deeper and stronger is the following result:

Theorem 4.82 We use the notation from above. The Tate module, T_ℓ induces a continuous $\mathbb{Z}_\ell$-module monomorphism, again denoted by T_ℓ, from $\mathrm{End}_{\mathbb{Z}_\ell}\big(T_\ell(\mathcal{A})\big) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ into $\mathrm{End}_{\mathbb{Z}_\ell}\big(T_\ell(\mathcal{A})\big)$.

For the proof see [MUM 1974, pp. 176].

It follows that $\mathrm{End}_K(\mathcal{A})$ is a free finitely generated $\mathbb{Z}$-module of rank $\leqslant \big(2\dim(\mathcal{A})\big)^2$ and so $\mathrm{End}_K(\mathcal{A}) \otimes \mathbb{Q}$ is a finite dimensional semisimple algebra over $\mathbb{Q}$. There is an extensive theory about such algebras and a complete classification. For more details see again [MUM 1974, pp. 193].

Moreover we can associate to φ the characteristic polynomial

$$\chi\big(T_\ell(\varphi)\big)(T) := \det\big(T - T_\ell(\varphi)\big),$$

which is a monic polynomial of degree $2\dim(\mathcal{A})$ with coefficients in $\mathbb{Z}_\ell$ by definition.

But here another fundamental result steps in:

Theorem 4.83 The characteristic polynomial $\chi\big(T_\ell(\varphi)\big)(T)$ does not depend on the prime number ℓ and has coefficients in $\mathbb{Z}$, hence it is a monic polynomial of degree $2\dim(\mathcal{A})$ in $\mathbb{Z}[T]$.

For the proof see [MUM 1974, p. 181].

Because of this result the following definition makes sense.

Definition 4.84 Let φ be an element in $\mathrm{End}_K(\mathcal{A})$. The characteristic polynomial $\chi(\varphi)_{\mathcal{A}}(T)$ is equal to the characteristic polynomial of $T_\ell(\varphi)$ for any ℓ different from $\mathrm{char}(K)$.

Corollary 4.85 We get

$$\deg(\varphi) = \chi(\varphi)_{\mathcal{A}}(0)$$

and more generally

$$\deg([n]-\varphi) = \chi(\varphi)_{\mathcal{A}}(n).$$

For n prime to $\mathrm{char}(K)$ the restriction of φ to $\mathcal{A}[n]$ has the characteristic polynomial

$$\chi(\varphi)_{\mathcal{A}}(T) \pmod{n}.$$

There is an important refinement of Theorem 4.82 taking into account the Galois action. As seen G_K is mapped into $\mathrm{End}_{\mathbb{Z}_\ell}\big(T_\ell(\mathcal{A})\big)$ by the representation $\tilde{\rho}_{\mathcal{A},\ell}$. By definition the image of T_ℓ commutes with the image of $\tilde{\rho}_{\mathcal{A},\ell}$ and hence we get:

Corollary 4.86 Moving to the Tate module T_ℓ induces a map from $\mathrm{End}_K(\mathcal{A})$ to $\mathrm{End}_{\mathbb{Z}_\ell[G_K]}\big(T_\ell(\mathcal{A})\big)$.

Example 4.87 Let $K = \mathbb{F}_p$ and let $\mathcal{A}$ be an abelian variety defined over K.

The Frobenius automorphism of K has a Galois ℓ-adic representation $\tilde{\rho}_{\mathcal{A},\ell}(\phi_p)$ and a representation as endomorphism of $\mathcal{A}$ in $\mathrm{End}_{\mathbb{Z}_\ell}\big(T_\ell(\mathcal{A})\big)$. By the very definition both images in $\mathrm{End}_{\mathbb{Z}_\ell}\big(T_\ell(\mathcal{A})\big)$ coincide.

It follows that the endomorphism ϕ_p attached to the Frobenius automorphism of K commutes with every element in $\mathrm{End}_K(\mathcal{A})$.

Moreover its characteristic polynomial $\chi(\phi_p)_{\mathcal{A}}(T)$ is equal to the characteristic polynomial of $\tilde{\rho}_{\mathcal{A},\ell}(\phi_p)$ for all ℓ prime to $\mathrm{char}(K)$.

For n prime to $\mathrm{char}(K)$, the kernel of $[n]-\phi_p$ has order $\chi(\phi_p)_{\mathcal{A}}(n)$.

4.3.7 Complex multiplication

The results of the section above are the key ingredients for the study of $\mathrm{End}_K(\mathcal{A})$.

For instance, it follows for simple abelian varieties $\mathcal{A}$ that a maximal subfield F of $\mathrm{End}_K(\mathcal{A})\otimes\mathbb{Q}$ is a number field of degree at most $2\dim(\mathcal{A})$ over $\mathbb{Q}$, cf. [MUM 1974, p. 182].

Definition 4.88 A simple abelian variety $\mathcal{A}$ over K has *complex multiplication* if $\mathrm{End}_K(\mathcal{A})\otimes\mathbb{Q}$ contains a number field F of degree $2\dim(\mathcal{A})$ over $\mathbb{Q}$.

If an F of this maximal degree exists then it has to be a field of *CM-type*. That means that it is a quadratic extension of degree 2 of a totally real field F_0 (i.e., every embedding of F_0 into $\mathbb{C}$ lies in $\mathbb{R}$), and no embedding of F into $\mathbb{C}$ is contained in $\mathbb{R}$. Therefore, $F = \mathrm{End}_K(\mathcal{A})\otimes\mathbb{Q}$.
If K is a field of characteristic 0 we get more:

Proposition 4.89 Let K be a field of characteristic 0. Let $\mathcal{A}$ be a simple abelian variety defined over K with complex multiplication. Then $\mathrm{End}_K(\mathcal{A})\otimes\mathbb{Q}$ is equal to a number field F of degree $2\dim(\mathcal{A})$ which is of CM-type. The ring $\mathrm{End}_K(\mathcal{A})$ is an order (cf. Definition 2.81) in F.

Example 4.90 Let K be a field of characteristic 0 and let E be an elliptic curve over K (cf. Section 4.4.2.a). Then either $\mathrm{End}_K(E) = \{[n] \mid n \in \mathbb{Z}\}$ or E has complex multiplication and $\mathrm{End}_K(E)$ is an order in an imaginary quadratic field. In either case the ring of endomorphisms of E is commutative.

The results both of the proposition and of the example are wrong if $\mathrm{char}(K) > 0$.

For instance, take a supersingular curve E defined over a finite field $\mathbb{F}_{p^2}$ (cf. Definition 4.74). Then the center of $\mathrm{End}_{\mathbb{F}_{p^2}}(E)\otimes\mathbb{Q}$ is equal to $\mathbb{Q}$, and $\mathrm{End}_{\mathbb{F}_{p^2}}(E)\otimes\mathbb{Q}$ is a quaternion algebra over an imaginary quadratic number field F (in fact there are infinitely many such quadratic number fields). Hence E has complex multiplication but $\mathrm{End}_{\mathbb{F}_{p^2}}(E)\otimes\mathbb{Q}$ is *not* commutative and *not* an order in F.

Remark 4.91 For elliptic curves (cf. Section 4.4.2.a) it is a strong requirement to have complex multiplication. If K has characteristic 0 we shall see that E has to be defined over a number field K_0, and its absolute invariant j_E which will be defined in Corollary 4.118 has to be an algebraic integer in K_0 (satisfying more conditions as we shall see in Theorem 5.47).

If $\mathrm{char}(K) = p > 0$ a necessary condition is that j_E lies in a finite field. After at most a quadratic extension of K this condition becomes sufficient.

4.4 Arithmetic of curves

From now on we concentrate on curves.

4.4.1 Local rings and smoothness

Definition 4.92 Let P be a point on an affine curve C. The set of rational functions that are regular at P form a subring $\mathcal{O}_P$ of $K(C)$.

In fact, $\mathcal{O}_P$ is a local ring with maximal ideal

$$\mathfrak{m}_P = \{f \in \mathcal{O}_P \mid f(P) = 0\}.$$

It is called the *local ring of* P.

The *residue field of* P is defined as $\mathcal{O}_P/\mathfrak{m}_P$.

One has $K(P) = \mathcal{O}_P/\mathfrak{m}_P$, hence, $\deg(P) = [K(P) : K]$.

For $S \subset C$ define $\mathcal{O}_S := \bigcap_{P \in S} \mathcal{O}_P$. It is the *ring of regular functions on* S. If S is closed then $\mathcal{O}_S$ is the localization of $K[C]$ with respect to the ideal defining S.

A rational function r on C is a morphism if and only if $r \in \mathcal{O}_C = K[C]$.

For a projective curve, the ring of rational functions on C that are regular at P is equal to $\mathcal{O}_P$, the local ring of P in a nonempty affine part of C.

Definition 4.93 Let $P \in C$ for a projective curve C. The point P is *nonsingular* if $\mathcal{O}_P$ is integrally closed in $K(C)$. Otherwise the point is called *singular*. A curve is called *nonsingular* or *smooth* if every point of $C(\overline{K})$ is nonsingular.

A smooth curve satisfies that $K[C_a]$ is integrally closed in $K(C)$ for any choice of C_a. If C is projective but not smooth we take an affine covering C_i and define $\widetilde{C}_i$ as affine curve corresponding to the integral closure of $K[C_i]$. By the uniqueness of the integral closure we can glue together the curves $\widetilde{C}_i$ to a projective curve $\widetilde{C}$ called the *desingularization of the curve* C. Note that in general even for C a plane curve, $\widetilde{C}$ shall not be plane.

There is a morphism $\varphi : \widetilde{C} \to C$ that is a bijection on the nonsingular points of C. Hence projective smooth curves that are birationally equivalent are isomorphic.

Therefore, irreducible projective nonsingular curves are in one-to-one correspondence to function fields of dimension 1 over K.

To have a criterion for smoothness that can be verified more easily we restrict ourselves to affine parts of curves.

Lemma 4.94 (Jacobi criterion) Let $C_a \subseteq \mathbb{A}^n$ be an affine curve, let $f_1, \ldots, f_d \in K[x]$ be generators of $I(C_a)$, and let $P \in C_a(\overline{K})$. If the rank of the matrix $\left((\partial f_i/\partial x_j)(P)\right)_{i,j}$ is $n-1$ then the curve is nonsingular at P.

Using this lemma one can show that there are only finitely many singular points on a curve.

For a nonsingular point P the dimension of $\mathfrak{m}_P/\mathfrak{m}_P^2$ is one. Therefore, the local ring $\mathcal{O}_P$ is a discrete valuation ring.

Definition 4.95 Let C be a curve and $P \in C$ be nonsingular. The *valuation at* P on $\mathcal{O}_P$ is given by

$$v_P : \mathcal{O}_P \to \{0, 1, 2, \dots\} \cup \{\infty\},\ v_P(f) = \max\{i \in \mathbb{Z} \mid f \in \mathfrak{m}_P^i\}.$$

The valuation is extended to $K(C)$ by putting $v_P(g/h) = v_P(g) - v_P(h)$. The value group of v_P is equal to $\mathbb{Z}$.

The valuation v_P is a non-archimedean discrete normalized valuation (cf. Chapter 3).

A function t with $v(t) = 1$ is called *uniformizer for* C *at* P.

Let P_1 and P_2 be nonsingular points. Then $v_{P_1} = v_{P_2}$ if and only if $P_1 \in G_K \cdot P_2$.

Example 4.96 Let $C = \mathbb{P}^1/K$ and choose $P \in \mathbb{A}^1$. Let $f \in K(x)$. The value $v_P(f)$ of f at $P = (a) \in \overline{K}$ equals the multiplicity of a as a root of f. If a is a pole of f, the pole-multiplicity is taken with negative sign as it is the zero-multiplicity of $1/f$.

This leads to a correspondence of Galois orbits of nonsingular points of C to normalized valuations of $K(C)$ that are trivial on K. For a nonsingular curve this is even a bijection. Namely, to each valuation v of $K(C)$ corresponds a local ring defined by $\mathcal{O}_v := \{f \in K(C) \mid v(f) \geqslant 0\}$ with maximal ideal $\mathfrak{m}_v$. If C is smooth, there exists a maximal ideal $M_v \subset K[C_a]$, where C_a is chosen such that $K[C_a] \subset \mathcal{O}_v$, satisfying $\mathcal{O}_v = \mathcal{O}_{\mathfrak{p}}$. Over the algebraic closure there exist points $P_1, \dots, P_d$ such that $\mathcal{O}_v$ equals $\mathcal{O}_{P_i}$ and the P_i form an orbit under G_K. The degree of M_v is $[K[C_a]/M_v : K] = [\mathcal{O}_v/\mathfrak{m}_v : K]$. It is equal to the order of $G_K \cdot P_i$ of one of the corresponding points on C.

Two valuations of v_1, v_2 of $K(C)$ are called *equivalent* if there exists a number $c \in \mathbb{R}_{>0}$ with $v_1 = cv_2$.

Definition 4.97 The equivalence class of a valuation v of $K(C)$ which is trivial on K is called a *place* $\mathfrak{p}$ *of* $K(C)$. The set of places of F/K is denoted by $\Sigma_{F/K}$.

In every place there is one valuation with value group $\mathbb{Z}$. It is called the *normalized valuation of* $\mathfrak{p}$ and denoted by $v_{\mathfrak{p}}$.

We have seen:

Lemma 4.98 Let F/K be a function field and let C/K be a smooth projective absolute irreducible curve such that $F \simeq K(C)$ with an isomorphism φ fixing each element of K.

There is a natural one-to-one correspondence induced by φ between the places of F/K and the Galois orbits of points on C.

Example 4.99 Consider the function field $K(x_1)$ with associated smooth curve $\mathbb{P}^1/K$ and affine coordinate ring $K[x_1]$. The normalized valuations in $\Sigma_{K(C)/K}$ for which the valuation ring contains $K[x_1]$ correspond one-to-one to the irreducible monic polynomials in $K[x_1]$. There is one additional valuation with negative value at x_1, called v_∞, which is equal to the negative degree valuation, corresponding to the valuation at $p_\infty(t) = t$ in $K[t] = K[1/x_1]$. Geometrically v_∞ corresponds to $\mathbb{P}^1 \setminus \mathbb{A}^1$.

4.4.2 Genus and Riemann–Roch theorem

We want to define a group associated to the points of a curve C.

Definition 4.100 Let C/K be a curve. The *divisor group* Div_C *of* C is the free abelian group over the places of $K(C)/K$. An element $D \in \mathrm{Div}_C$ is called a *divisor*. It is given by

$$D = \sum_{\mathfrak{p}_i \in \Sigma_{K(C)/K}} n_i \mathfrak{p}_i,$$

where $n_i \in \mathbb{Z}$ and $n_i = 0$ for almost all i.

The divisor D is called a *prime divisor* if $D = \mathfrak{p}$ with $\mathfrak{p}$ a place of $K(C)/K$.

The *degree* $\deg(D)$ *of a divisor* D is given by

$$\begin{aligned} \deg : \mathrm{Div}_C &\to \mathbb{Z} \\ D &\mapsto \deg(D) = \sum_{\mathfrak{p}_i \in \Sigma_{K(C)/K}} n_i \deg(\mathfrak{p}_i). \end{aligned}$$

A divisor is called *effective* if all $n_i \geqslant 0$. By $E \geqslant D$ one means that $E - D$ is effective.

For $D \in \mathrm{Div}_C$ put

$$D_0 = \sum_{\substack{\mathfrak{p}_i \in \Sigma_{K(C)/K} \\ n_i \geqslant 0}} n_i \mathfrak{p}_i \quad \text{and} \quad D_\infty = \sum_{\substack{\mathfrak{p}_i \in \Sigma_{K(C)/K} \\ n_i \leqslant 0}} -n_i \mathfrak{p}_i,$$

thus $D = D_0 - D_\infty$.

Recall that over $\overline{K}$ each place $\mathfrak{p}_i$ corresponds to a Galois orbit of points on the projective nonsingular curve attached to $K(C)$. Thus, D can also be given in the form

$$D = \sum_{P_i \in C} n_i P_i$$

with $n_i \in \mathbb{Z}$, almost all $n_i = 0$ and $n_i = n_j$ if $P_i \in P_j \cdot G_K$.

Assume now that C is absolutely irreducible. Then we can make a base change from K to $\overline{K}$. As a result we get again an irreducible curve $C \cdot \overline{K}$ (given by the same equations as C but interpreted over $\overline{K}$) with function field $K(C) \cdot \overline{K}$.

Applying the results from above we get

$$\mathrm{Div}_{C \cdot \overline{K}} = \left\{ \sum_{P_i \in C} n_i P_i \right\}$$

with $n_i \in \mathbb{Z}$ and almost all $n_i = 0$. For all fields L between K and $\overline{K}$ the Galois group G_L operates by linear extension of the operation on points.

Proposition 4.101 Assume that C/K is a projective nonsingular absolutely irreducible curve. Let L be a field between K and $\overline{K}$ and denote by $\mathrm{Div}_{C \cdot L}$ the group of divisors of the curve over L obtained by base change from K to L. Then

$$\mathrm{Div}_{C \cdot L} = \{ D \in \mathrm{Div}_{C \cdot \overline{K}} \mid \sigma(D) = D, \ \text{for all } \sigma \in G_L \}.$$

Especially: $\mathrm{Div}_C = \mathrm{Div}_{C \cdot \overline{K}}^{G_K}$.

Important examples of divisors of C are associated to functions. We use the relation between normalized valuations of $K(C)$ which are trivial on K and prime divisors.

Definition 4.102 Let C/K be a curve and $f \in K(C)^*$. The *divisor* $\operatorname{div}(f)$ *of* f is given by

$$\begin{array}{rcccl} \operatorname{div} : K(C) & \to & \operatorname{Div}_C & & \\ f & \mapsto & \operatorname{div}(f) & = & \displaystyle\sum_{\mathfrak{p}_i \in \Sigma_{K(C)/K}} v_{\mathfrak{p}_i}(f)\mathfrak{p}_i. \end{array}$$

A divisor associated to a function is called a *principal divisor*. The set of principal divisors forms a group Princ_C.

We have a presentation of $\operatorname{div}(f)$ as difference of effective divisors as above:

$$\operatorname{div}(f) = \operatorname{div}(f)_0 - \operatorname{div}(f)_\infty.$$

The points occurring in $\operatorname{div}(f)_0$ (resp. in $\operatorname{div}(f)_\infty$) with nonzero coefficient are called *zeroes (resp. poles) of* f.

Example 4.103 Recall the setting of Example 4.99 for the curve $C = \mathbb{P}^1$. Since polynomials of degree d over fields have d zeroes (counted with multiplicities) over $\overline{K}$ we get immediately from the definition:

$$\deg(f) = 0, \text{ for all } f \in K(x_1)^*.$$

Now let C be arbitrary. Take $f \in K(C)^*$. For constant $f \in K^*$ the divisor is $\operatorname{div}(f) = 0$. Otherwise $K(f)$ is of transcendence degree 1 over K and can be interpreted as function field of the projective line (with affine coordinate f) over K. By commutative algebra (cf. [ZASA 1976]) we learn about the close connection between valuations in $K(f)$ and $K(C)$, the latter being a finite algebraic extension of $K(f)$. Namely, $\operatorname{div}(f)_\infty$ is the conorm of the negative degree valuation on $K(f)$ and hence has degree $[K(C) : K(f)]$ (cf. [STI 1993, p. 106]).

Since $\operatorname{div}(f)_0 = \operatorname{div}(f^{-1})_\infty$ we get:

Proposition 4.104 Let C be an absolutely irreducible curve with function field $K(C)$ and $f \in K(C)^*$.

(i) $\deg\big(\operatorname{div}(f)_0\big) = 0$ if and only if $f \in K^*$.

(ii) If $f \in K(C) \smallsetminus K$ then $[K(C) : K(f)] = \deg\big(\operatorname{div}(f)_\infty\big) = \deg\big(\operatorname{div}(f)_0\big)$.

(iii) For all $f \in K(C)^*$ we get: $\deg\big(\operatorname{div}(f)\big) = 0$.

So the principal divisors form a subgroup of the group Div_C^0 of degree zero divisors.

To each divisor D we associate a vector space consisting of those functions with pole order at places $\mathfrak{p}_i$ bounded by the coefficients n_i of D.

Definition 4.105 Let $D \in \operatorname{Div}_C$. Define

$$L(D) := \{f \in K(C) \mid \operatorname{div}(f) \geqslant -D\}.$$

It is not difficult to see that $L(D)$ is a finite dimensional K-vector space. Put $\ell(D) = \dim_K\big(L(D)\big)$.

The *Theorem of Riemann–Roch* gives a very important connection between $\deg(D)$ and $\ell(D)$.

We give a simplified version of this theorem, which is sufficient for our purposes. The interested reader can find the complete version in [STI 1993, Theorem I.5.15].

Theorem 4.106 (Riemann–Roch) Let C/K be an absolutely irreducible curve with function field $K(C)$. There exists an integer $g \geqslant 0$ such that for every divisor $D \in \mathrm{Div}_C$

$$\ell(D) \geqslant \deg(D) - g + 1.$$

For all $D \in \mathrm{Div}_C$ with $\deg(D) > 2g - 2$ one even has equality $\ell(D) = \deg(D) - g + 1$.

Definition 4.107 The number g from Theorem 4.106 is called the *genus of* $K(C)$ or the *geometric genus of* C. If C is projective nonsingular then g is called the *genus of* C.

The Riemann–Roch theorem guarantees the existence of functions with prescribed poles and zeroes provided that the number of required zeroes is at most $2g-2$ less than the number of poles. Namely, if $n_i > 0$ at $\mathfrak{p}_i$ then $f \in L(D)$ is allowed to have a pole of order at most n_i at $\mathfrak{p}_i$. Vice versa a negative n_i requires a zero of multiplicity at least n_i at $\mathfrak{p}_i$.

As an important application we get:

Lemma 4.108 Let C/K be a nonsingular curve and let $D = \sum n_i \mathfrak{p}_i$ be a K-rational divisor of C of degree $\geqslant g$. Then there is a function $f \in K(C)$ which has poles of order at most n_i (hence zeroes of order at least $-n_i$ if $n_i < 0$) in the points $P_i \in C$ corresponding to $\mathfrak{p}_i$ and no poles elsewhere. In other words: the divisor $D + (f)$ is effective.

Example 4.109 For the function field $K(x_1)$, Lagrange interpolation allows to find quotients of polynomials for any given zeroes and poles. This leads to $\ell(D) = \deg(D) + 1$. The curve $\mathbb{P}^1/K$ has genus 0.

The *Hurwitz genus formula* relates the genus of algebraic extensions $F'/F/K$. It is given in a special case in the following theorem (cf. [STI 1993, Theorem III.4.12] for the general case).

Theorem 4.110 (Hurwitz Genus Formula) Let F'/F be a tame finite separable extension of algebraic function fields having the same constant field K. Let g (resp. g') denote the genus of F/K (resp. F'/K). Then

$$2g' - 2 = [F' : F](2g - 2) \sum_{\mathfrak{p} \in \Sigma_{F/K}} \sum_{\mathfrak{p}'|\mathfrak{p}} \big(e(\mathfrak{p}'|\mathfrak{p}) - 1\big) \deg(\mathfrak{p}').$$

One of the most important applications of the Riemann–Roch theorem is to find affine equations for a curve with given function field. We shall demonstrate this in two special cases which will be the center of interest later on.

4.4.2.a Elliptic curves

Definition 4.111 A nonsingular absolutely irreducible projective curve defined over K of genus 1 with at least one K-rational point is called an *elliptic curve*.

Let C be such a smooth absolutely irreducible curve of genus 1 with at least one K-rational point P_∞ and let F/K be its function field. As $\ell(P_\infty) = 1$ we have thus $L(P_\infty) = K$.

Theorem 4.106 guarantees $\ell(2P_\infty) = 2$, hence there exists a function $x \in F$ such that $\{1, x\}$ is a basis of $L(2P_\infty)$ over K. There also exists $y \in F$ such that $\{1, x, y\}$ is a basis of $L(3P_\infty)$ over K. We easily find that $\{1, x, y, x^2\}$ is a basis of $L(4P_\infty)$ and that $L(5P_\infty)$ has basis $\{1, x, y, x^2, xy\}$.

The space $L(6P_\infty) \supset \langle\{1, x, y, x^2, xy, x^3, y^2\}\rangle$ has dimension six, hence there must be a linear dependence between these seven functions. In this relation y^2 has to have a nontrivial coefficient a. By multiplying the relation with a and by replacing y by $a^{-1}y$ we can assume that $a = 1$. The

function x^3 has to appear nontrivially, too, with some coefficient b. Multiply the relation by b^2 and replace x by $b^{-1}x$, y by $b^{-1}y$. Then the coefficients of y^2 and x^3 are equal to 1 and we get a relation

$$y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6,\ a_i \in K.$$

This is the equation of an absolutely irreducible plane affine curve. It is a fact (again obtained by the use of the theorem of Riemann–Roch) that this curve is smooth.

The projective closure $\overline{C}$ of C is given by

$$Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3,\ a_i \in K$$

with plane projective coordinates $(X : Y : Z)$. One sees at once that $\overline{C} \setminus C = \{(0 : 1 : 0)\}$ and that $P_\infty := (0 : 1 : 0)$ is smooth. Hence C is a nonsingular absolutely irreducible plane projective curve of genus 1.

Again by using the Riemann–Roch theorem one can prove that the converse holds, too. The projective curve given by

$$Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3,\ a_i \in K$$

is a curve of genus 1 if and only if it is smooth.

We have seen that the Riemann–Roch theorem yields

Theorem 4.112 A function field F/K of genus 1 with a prime divisor of degree 1 is the function field of an elliptic curve E. This curve is isomorphic to a smooth plane projective curve given by a *Weierstraß equation*

$$E : Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3,\ a_i \in K.$$

A plane nonsingular affine part E_a of E is given by

$$y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6,\ a_i \in K.$$

$E \setminus E_a$ consists of one point with homogeneous coordinates $(0 : 1 : 0)$.

Conversely nonsingular curves given by equations

$$E : Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3,\ a_i \in K$$

have function fields of genus 1 with at least one prime divisor of degree 1 and so are elliptic curves.

In the remainder of the book E will be a standard notation for an elliptic curve given by a Weierstraß equation, and we shall often abuse notation and denote by E the affine part E_a, too. Since elliptic curves are one of the central topics of this book we use the opportunity to study their equations in more detail.

Short normal forms and invariants

Let E be an elliptic curve defined over K with affine Weierstraß equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

We shall simplify this equation under assumptions about the characteristic of K. To achieve this we shall map (x, y) to (x', y') by invertible linear transformations. These transformations correspond to morphisms of the affine part of E to the affine part of another elliptic curve E', and since the infinite point remains unchanged we get an isomorphism between E and E'. Having done the

transformation we change notation and denote the transformed curve by E with coordinates (x, y) again.
First assume that the characteristic of K is odd. We make the following transformations

$$x \mapsto x' = x \quad \text{and} \quad y \mapsto y' = y + \frac{1}{2}\Big(a_1 x + \frac{a_3}{2}\Big).$$

The equation of E expressed in the coordinates (x', y') and then, following our convention to change notation and to write x for x' and y for y' is:

$$E : y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}$$

where $b_2 = a_1^2 + 4a_2,\ b_4 = 2a_4 + a_1 a_3$ and $b_6 = a_3^2 + 4a_6$.

Now we assume in addition that the characteristic of K is prime to 6. We transform

$$x \mapsto x' = x + \frac{b_2}{12} \quad \text{and} \quad y \mapsto y' = y$$

and — applying our conventions — get the equation

$$E : y^2 = x^3 - \frac{c_4}{48}x - \frac{c_6}{864},$$

where c_4 and c_6 are expressed in an obvious way in terms of b_2, b_4, b_6 as

$$c_4 = b_2^2 - 24b_4 \quad \text{and} \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

So if $\mathrm{char}(K)$ is prime to 6, we can always assume that an elliptic curve is given by a *short Weierstraß equation* of the type

$$y^2 = x^3 + a_4 x + a_6.$$

Next we have to decide which Weierstraß equations define isomorphic elliptic curves. We can and will restrict ourselves to isomorphisms that fix the point at infinity, i.e., we fix one rational point on E or equivalently we fix one place of degree 1 in the function field of E, which is the place P_∞ used when we derived the equation in Section 4.4.2.a.

To make the discussion not too complicated we shall continue to assume that the characteristic of K is prime to 6 and so we have to look for invertible transformations of the affine coordinates for which the transformed equation is again a short Weierstraß equation.

So let E be given by

$$E : y^2 = x^3 + a_4 x + a_6.$$

One sees immediately that the conditions imposed on the transformations imply

$$x \mapsto x' = u^{-2}x \quad \text{and} \quad y \mapsto y' = u^{-3}y$$

with $u \in K^*$, and that the resulting equation is

$$E' : y'^2 = x'^3 + u^4 a_4 x + u^6 a_6.$$

Proposition 4.113 Assume that the characteristic of K is prime to 6 and let E be an elliptic curve defined over K. Let E be given by a short Weierstraß equation

$$E : y^2 = x^3 + a_4 x + a_6.$$

- If $a_4 = 0$ then the coefficient of x is equal to 0 in all short Weierstraß equations for E, and a_6 is determined up to a sixth power in K^*.
- If $a_6 = 0$ then the absolute term in all short Weierstraß equations for E is equal to 0 and a_4 is determined up to a forth power in K^*.
- If $a4a_6 \neq 0$ then a_6/a_4 is determined up to a square in K^*.

Conversely:

- If $a_4 = 0$ then E is isomorphic to E' if in a short Weierstraß form of E' the coefficient a'_4 of x is equal to 0 and a'_6/a_6 is a sixth power in K^*.
- If $a_6 = 0$ then E is isomorphic to E' if in a short Weierstraß form of E' the absolute term is equal to 0 and a'_4/a_4 is a fourth power in K^*.
- If $a_4 a_6 \neq 0$ then E is isomorphic to E' if in a short Weierstraß form of E' we have: there is an element $v \in K^*$ with $a'_4 = v^2 a_4$ and $a'_6 = v^3 a_6$.

Corollary 4.114 Assume that the characteristic of K is prime to 6 and let E be given by a short Weierstraß equation

$$E : y^2 = x^3 + a_4 x + a_6.$$

- If $a_4 = 0$ then for every $a'_6 \in K^*$ the curve E is isomorphic to

$$E' : y^2 = x^3 + a'_6 \quad \text{over} \quad K\big((a_6/a'_6)^{1/6}\big).$$

- If $a_6 = 0$ then for every $a'_4 \in K^*$ the curve E is isomorphic to

$$E' : y^2 = x^3 + a'_4 x \quad \text{over} \quad K\big((a_4/a'_4)^{1/4}\big).$$

- If $a_4 a_6 \neq 0$ then for every $v \in K^*$ the curve E is isomorphic to

$$\widetilde{E}_v : y^2 = x^3 + a'_4 x + a'_6 \ \text{ with } \ a'_4 = v^2 a_4 \ \text{ and } \ a'_6 = v^3 a_6 \ \text{ over } \ K(\sqrt{v}).$$

The curves occurring in the Corollary are called *twists of* E. The curves $\widetilde{E}_v$ are called *quadratic twists* of E. Note that E is isomorphic to $\widetilde{E}_v$ over K if and only if v is a square in K^*. Therefore up to isomorphisms there is only one quadratic twist of a curve with $a_4 a_6 \neq 0$.

We want to translate the results of the proposition and of the lemma into "invariants" of E that can be read off from any Weierstraß equation.

Recall that a crucial part of the definition of elliptic curves was that the affine part has no singular points. This is translated into the condition that the discriminant of the equation of E is not equal to 0. This discriminant is a polynomial in the coefficients a_i, which is particularly easy to write down if we have a short Weierstraß equation. So let E be given by

$$E : y^2 = x^3 + a_4 x + a_6 := f(x).$$

Definition 4.115 The discriminant Δ_E of E is equal to the polynomial discriminant of $f(x)$ which is (up to a sign) the product of the differences of the zeroes of $f(x)$, which we endow with a constant for historical reasons:

$$\Delta_E = -16(4a_4^3 + 27a_6^2).$$

We note that this definition is to be taken with caution: it depends on the chosen Weierstraß equation and not only on the isomorphism class of E. To make the discriminant well defined we have to consider it modulo 12-th powers in K^*.

To get an invariant of the isomorphism class of E we use the transformations of a_4, a_6, and Δ_E under transformations of Weierstraß forms.

Definition 4.116 The absolute invariant (sometimes called j-invariant) j_E of E is defined by

$$j_E = 12^3 \frac{-4a_4^3}{\Delta_E}.$$

Lemma 4.117 Assume that the characteristic of K is prime to 6 and let E be given by a short Weierstraß equation

$$E : y^2 = x^3 + a_4x + a_6.$$

The absolute invariant j_E depends only on the isomorphism class of E.

(i) We have $j_E = 0$ if and only if $a_4 = 0$.
(ii) We have $j_E = 12^3$ if and only if $a_6 = 0$.
(iii) If $j \in K$ is not equal to $0, 12^3$ then E is a quadratic twist of the elliptic curve

$$E_j : y^2 = x^3 - \frac{27j}{4(j-12^3)}x + \frac{27j}{4(j-12^3)}.$$

Corollary 4.118 Assume that the characteristic of K is prime to 6. The isomorphism classes of elliptic curves E over K are, up to twists, uniquely determined by the absolute invariants j_E, and for every $j \in K$ there exists an elliptic curve with absolute invariant j.

If K is algebraically closed then the isomorphism classes of elliptic curves over K correspond one-to-one to the elements in K via the map $E \mapsto j_E$.

Of course it is annoying that we have to restrict ourselves to fields whose characteristic is prime to 6. In fact this is not necessary at all; completely analogous discussions can be done for characteristics 2 and 3 and can be found in [SIL 1986] and also in Chapter 13.

We give a very short sketch of the discussions there.

We start with a general Weierstraß equation for E over a field with odd characteristic.

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

and recall the definitions of $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$, $b_6 = a_3^2 + 4a_6$, and $c_4 = b_2^2 - 24b_4$.

In addition we define

$$b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2.$$

Definition 4.119 The discriminant of E is

$$\Delta_E := -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

and the absolute invariant of E is

$$j_E = c_4^3/\Delta_E.$$

If the characteristic of K is equal to 2 one also finds normal forms for E (cf. Section 13.3). Either $a_1 = 0$ and then $j_E := 0$. Otherwise we can find an equation for E with $a_3 = a_4 = 0$ and $a_1 = 1$. Then $j_E = a_6^{-1}$.

We summarize the definitions in Table 4.1. Using these extra considerations one easily sees that the conclusions of Corollary 4.118 hold without any restrictions about the characteristic of the ground field.

Theorem 4.120 Let K be a field. The isomorphism classes of elliptic curves E over K are, up to twists, uniquely determined by the absolute invariants j_E, and for every $j \in K$ there exists an elliptic curve E with absolute invariant $j_E = j$.

If K is algebraically closed then the isomorphism classes of elliptic curves over K correspond one-to-one to the elements in K via the map $E \mapsto j_E$.

Table 4.1 Short Weierstraß equations.

$\operatorname{char} K$	Equation	Δ	j
$\neq 2,\ 3$	$y^2 = x^3 + a_4x + a_6$	$-16(4a_4^3 + 27a_6^2)$	$1728a_4^3/4\Delta$
3	$y^2 = x^3 + a_4x + a_6$	$-a_4^3$	0
3	$y^2 = x^3 + a_2x^2 + a_6$	$-a_2^3a_6$	$-a_2^3/a_6$
2	$y^2 + a_3y = x^3 + a_4x + a_6$	a_3^4	0
2	$y^2 + xy = x^3 + a_2x^2 + a_6$	a_6	$1/a_6$

4.4.2.b Hyperelliptic curves

Definition 4.121 A nonsingular curve C/K of genus $g > 1$ is called a *hyperelliptic curve* if the function field $K(C)$ is a separable extension of degree 2 of the rational function field $K(x)$ for some function x. Let ω denote the nontrivial automorphism of this extension. It induces an involution ω_* on C with quotient $\mathbb{P}^1$. The fixed points $P_1, \ldots, P_{2g+2}$ of ω_* are called *Weierstraß points*.

From a geometrical point of view, C is a hyperelliptic curve if there exists a generically étale morphism π of degree 2 to $\mathbb{P}^1$. The Weierstraß points are exactly the points in which π is ramified.

Classically, elliptic curves are not subsumed under hyperelliptic curves. The main difference is that for $g > 1$ the rational subfield of index 2 is unique. That implies that the function x is uniquely determined up to transformations

$$x \mapsto \frac{ax+b}{cx+d} \text{ with } a,b,c,d \in K \text{ and } ad - bc \neq 0.$$

For elliptic curves this is wrong. If, for instance, K is algebraically closed then there exist infinitely many rational subfields of index 2. In this book we will often consider elliptic curves as hyperelliptic curves of genus one since most of the arithmetic properties we are interested in are the same.

We now use the Riemann–Roch theorem to find an equation describing a plane affine part of C.

The definition implies that there exists a divisor D of degree 2, which is the conorm of the negative degree valuation on $K(x)$ (cf. [STI 1993, p. 106]).

From the construction we have that $L(D)$ has basis $\{1, x\}$ and, hence, $\ell(D) = 2$. For $1 \leqslant j \leqslant g$ we have that $\ell(jD) \geqslant 2j$ and the elements $\{1, x, \ldots, x^j\}$ are linearly independent in $L(jD)$. As $\deg\big((g+1)D\big) = 2(g+1) > 2g-2$, Theorem 4.106 implies that

$$\ell\big((g+1)D\big) = \deg\big((g+1)D\big) - g + 1 = g + 3.$$

Hence, besides the $g+2$ elements $1, x, \ldots, x^{g+1}$ there must be a $(g+3)$-th function $y \in L\big((g+1)D\big)$ independent of the powers of x.

Therefore, $y \notin K[x]$. The space $L\big(2(g+1)D\big)$ has dimension $3g+3$. It contains the $3g+4$ functions

$$1, x, \ldots, x^{g+1}, y, x^{g+2}, xy, \ldots, x^{2(g+1)}, x^{g+1}y, y^2.$$

Therefore there must exist a linear combination defined over K among them. In this relation y^2 has to have some nontrivial coefficient a as $y \notin K[x]$. By multiplying the relation with a and by replacing y by $a^{-1}y$ we can assume that $a = 1$.

This leads to an equation

$$y^2 + h(x)y = f(x),\ h(x), f(x) \in K[x],$$

where $\deg(h) \leqslant g+1$ and $\deg(f) \leqslant 2g+2$.

To determine the exact degrees we use the *Hurwitz genus formula* stated in Theorem 4.110. In our case $[K(C) : K(x)] = 2$ and thus $e(\mathfrak{p}'|\mathfrak{p}) \leqslant 2$. To simplify we shall assume that the characteristic of K is odd. After applying the usual transformation $y \mapsto y - h(x)/2$ we can assume that $h(x) = 0$. Then the fixed points of ω_* are points with y-coordinate equal to 0 or are points lying over $x = \infty$. The latter case occurs if and only if D is a divisor of the form $2P_\infty$, i.e., if there is only one point P_∞ lying over ∞ on the nonsingular curve with function field $K(C)$. Moreover the x-coordinates of these points correspond to the places of $K(x)$ which ramify in the extension $K(C)/K(x)$.

By the genus formula the number of the ramified points has to be equal to $2g + 2$. Hence $f(x)$ has to have $2g+2$ different zeroes if ∞ is not ramified, and $2g+1$ different zeroes if ∞ is ramified. As a result we get: the degree of $f(x)$ is equal to $2g + 2$ if $D = P_1 + P_2$ with different P_1, P_2 and equal to $2g + 1$ if $D = 2P_\infty$, and $f(x)$ has no double zeroes.

Moreover the affine curve given by the equation

$$C_a : y^2 + h(x)y = f(x),\ h(x), f(x) \in K[x]$$

is nonsingular.

Theorem 4.122 A function field F/K of genus $g > 1$ with an automorphism ω^* of order 2 with rational fixed field is the function field of a plane affine curve given by an equation

$$C : y^2 + h(x)y = f(x),\ h(x), f(x) \in K[x], \tag{4.1}$$

where $2g + 1 \leqslant \deg f \leqslant 2g + 2$ and $\deg h \leqslant g + 1$ without singularities.

Conversely the nonsingular projective curve birationally isomorphic to an affine nonsingular curve given by an equation of this type is a hyperelliptic curve of genus g.

The homogenized equation has a singularity at infinity exactly if there is a single point in $\pi^{-1}(\infty)$ and then the degree of $f(x)$ is equal to $2g + 1$. In this case we can achieve a monic f. Let b be the leading coefficient. Multiplying the equation by b^{2g} and replacing $y \mapsto y/b^g, x \mapsto x/b^2$ we obtain

$$C_a : y^2 + h(x)y = f(x) \text{ with } h(x), f(x) \in K[x], \deg(f) = 2g + 1, \deg(h) \leqslant g \text{ and } f \text{ monic.}$$

In the sequel we shall always characterize hyperelliptic curves by their affine plane parts and assume them given by equations of the form (4.1).

Short Weierstraß equations

Later on we shall concentrate on the case that $\deg(f) = 2g + 1$, i.e., curves having a K-rational Weierstraß point. In this case we can simplify the equations analogously to the case of elliptic curves. We distinguish between the case of K having odd or even characteristic.

Let C be a hyperelliptic curve of genus g defined over a field of characteristic $\neq 2$ by an equation of the form (4.1) with $\deg(f) = 2g+1$. The transformation $y \mapsto y - h(x)/2$ leads to an isomorphic curve given by

$$C : y^2 = f(x), f \in K[x] \text{ and } \deg(f) = 2g + 1. \tag{4.2}$$

The Jacobi criterion (cf. Lemma 4.94) states that C is nonsingular if and only if no point on the curve satisfies both partial derivative equations $2y = 0$ and $f'(x) = 0$. The points with $y = 0$ are just the points $P_i = (x_i, 0)$, where $f(x_i) = 0$. The second condition shows that the singular points are just the Weierstraß points for which the first coordinate is a multiple root of f. Therefore, a necessary and sufficient criterion for (4.2) to be nonsingular is that f has only simple roots over the algebraic closure.

Let

$$f(x) = x^{2g+1} + \sum_{i=0}^{2g} f_i x^i.$$

If additionally $\mathrm{char}(K)$ is coprime to $2g$, the transformation $x \mapsto x - f_{2g}/(2g)$ allows to give

$$f(x) = x^{2g+1} + f_{2g-1}x^{2g-1} + \cdots + f_1 x + f_0 \text{ with } f_i \in K.$$

Let C be a hyperelliptic curve of genus g over a field of characteristic 2. Assume first that $h(x) = 0$, i.e., $y^2 = f(x)$ like above.

The partial derivatives are $2y = 0$ and $f'(x)$. Any of the $2g+1$ roots x_P of f' can be extended to a point (x_P, y_P) satisfying $y_P^2 = f(x_P)$ and both partial derivatives. Hence, $h(x) = 0$ immediately leads to a singular point and so we must have $h(x) \neq 0$.

4.4.2.c Differentials

We shall now give another application of the theorem of Riemann–Roch. For this we have to introduce differentials. We shall do this in the abstract setting of function fields. If the ground field K is equal to $\mathbb{C}$ this concept coincides with the "usual" notion of differentials known from calculus.

Let $K(C)$ be the function field of a curve C defined over K. To every $f \in K(C)$ we attach a symbol df, the *differential* of f lying in a $K(C)$-vector space $\Omega\big(K(C)\big)$, which is the free vector space generated by the symbols df modulo the following relations.

For $f, g \in K(C)$ and $\lambda \in K$ we have

(R1) $$d(\lambda f + g) = \lambda df + dg$$

(R2) $$d(fg) = f dg + g df.$$

Recall that a *derivation* of $K(C)$ is a K-linear map

$$D : K(C) \to K(C)$$

vanishing on K with

$$D(fg) = D(f)g + D(g)f.$$

Let $x \in K(C)$ be such that $K(C)$ is a finite separable extension of $K(x)$. Then there is exactly one derivation D of $K(C)$ with $D(x) = 1$ (cf. [ZASA 1976]) call this derivation the *partial derivative with respect to* x and denote the image of $f \in K(C)$ under this derivation by $\partial f/\partial x$.

The relation between derivations and differentials is given by the *chain rule.*

Lemma 4.123 (Chain rule) Let x be as above and $f \in K(C)$. Then $df = (\partial f/\partial x)dx$.

Corollary 4.124 The $K(C)$-vector space of differentials $\Omega(K(C))$ has dimension 1.

It is generated by dx for any $x \in K(C)$ for which $K(C)/K(x)$ is finite separable.

Let P be a point on C. Take a uniformizer for C at P, i.e., a function $t_P \in K(C)$ that generates the maximal ideal M_P of the place associated to P. So t_P is a function that vanishes at P with multiplicity 1. It follows that $K(C)/K(t_P)$ is finite separable.

Let $\omega \in \Omega\big(K(C)\big)$ be a differential of C. We attach a divisor $\mathrm{div}(\omega) = \sum_{P \in C} n_P P$ given by the following recipe: for $P \in C$ choose a uniformizer t_P and express ω by $\omega = f_P dt_P$ with $f_P \in K(C)$. Then

$$n_P = v_P(f_P).$$

Lemma 4.125 The sum $\mathrm{div}(\omega) = \sum_{P \in C} n_P P$ defines a divisor of C that is independent of the choice of the uniformizers t_P. The degree of $\mathrm{div}(\omega)$ is equal to $2g - 2$.

For a proof of the lemma see [STI 1993].

Definition 4.126 A differential ω is *holomorphic* if $\mathrm{div}(\omega)$ is an effective divisor.

The set of holomorphic differentials of C forms a K-vector space $\Omega^0(K(C))$.

A consequence of the Riemann–Roch theorem is:

Theorem 4.127 The K-vector space $\Omega^0\big(K(C)\big)$ has dimension g.

Example 4.128 Let E be an elliptic curve defined over K and given by an affine Weierstraß equation $G(x,y)=0$, where

$$G(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6, \text{ with } a_i \in K.$$

The differential $1/\big(\partial G(x,y)/\partial y\big)dx$ is holomorphic, and up to a multiplicative constant it is the unique holomorphic differential of E. Note that it has neither poles nor zeroes.

4.4.3 Divisor class group

In this section we shall attach an abelian group to each nonsingular curve starting from the group of divisors as defined in Section 4.4.2. This construction will give us an intimate relation between the arithmetic of curves and abelian varieties.

Let C/K be an absolutely irreducible smooth projective curve. Let Div_C^0 denote the group of K-rational divisors of C of degree 0.

Recall that principal divisors have degree zero and form a subgroup $\mathrm{Princ}_C \subseteq \mathrm{Div}_C^0$.

Definition 4.129 The *divisor class group* Pic_C^0 *of* C *of degree zero* is the quotient of the group of degree zero divisors Div_C^0 by the principal divisors. It is also called the *Picard group of* C.

Hence, two divisors D_1 and D_2 are in the same class if there exists an $f \in K(C)$ with $\mathrm{div}(f) = D_1 - D_2$.

Example 4.130 Let ω and ω' be two differentials of C that are not equal to 0. Then $\mathrm{div}(\omega)$ is in the same class as $\mathrm{div}(\omega')$.

In contrast to the group of divisors, the divisor class group has many torsion elements. If the field K is finite, it is even a finite group.

We now give an example of how to deal with torsion elements.

4.4.3.a Divisor classes of order equal to char(K)

We assume that K is a field of characteristic $p > 0$. Let C be a projective absolutely irreducible nonsingular curve of genus g defined over K. Let $\mathrm{Pic}_C^0[p]$ be the group of divisor classes of C with order dividing p.

In [SER 1958] we find the following result.

Proposition 4.131 There is a monomorphism α from $\mathrm{Pic}_C^0[p]$ into $\Omega^0(C)$, the K-vector space of holomorphic differentials on C given by the following rule: choose a K-rational divisor D with $pD = \mathrm{div}(f)$ where f is a function on C. Then the divisor class $\overline{D}$ of D is mapped under α to the holomorphic differential $(1/f)df$.

Note that $(1/f)df$ is holomorphic since the multiplicity of the zeroes of f is divisible by $p = \mathrm{char}(K)$. Next we choose a point $P_0 \in C(K)$. Let t be a uniformizer of C at P_0 (i.e., $t \in K(C)$ with $t(P_0) = 0$ and $\partial f/\partial t(P_0) \neq 0$). We take $(1/f)df$ as in the proposition and express it via the chain rule in the form $\big((\partial f/\partial t)/f\big)dt$. Let $(a_0, a_1, \ldots, a_{2g-2})(f)$ be the tuple whose coordinates

are first coefficients of the power series expansion of $(\partial f/\partial t)/f$ at P_0 and assume that there is another holomorphic differential hdt with h having the same power series expansion as $(\partial f/\partial t)/f$ modulo t^{2g-1}. Then $(1/f)df - hdt$ is a holomorphic differential whose divisor has a coefficient $\geqslant 2g-1$ at P_0 and so its degree is $\geqslant 2g-1$. But this implies that it is equal to 0 and so $(1/f)df = hdt$.

Hence we get

Proposition 4.132 Let K be a field of characteristic $p > 0$ and C a curve of genus g defined over K. For divisor classes $\overline{D} \in \mathrm{Pic}_C^0[p]$ choose a divisor $D \in \overline{D}$ and take $f \in K(C)$ with $pD = \mathrm{div}(f)$.

The map

$$\begin{array}{rcl} \Phi : \mathrm{Pic}_C^0[p] & \to & K^{2g-1} \\ \overline{D} & \mapsto & (a_0, a_1, \ldots, a_{2g-2})(f) \end{array}$$

is an injective homomorphism.

Remark 4.133 For applications later on we shall be interested mostly in the case that K is a finite field $\mathbb{F}_q$. Moreover, computational aspects will become important. If we want to use Proposition 4.132 in practice to identify $\mathrm{Pic}_C^0[p](\mathbb{F}_q)$ with a subgroup of $\mathbb{F}_q^{2g-1}$ we must be able to compute the first coefficients of the power series expansion of $(1/f)df$ at P_0 fast. The problem is that the degree of f can be very large. Nevertheless this can be done in polynomial time (depending on g and $\lg q$). The method is similar to the one we shall use later on for computing the Tate pairing (see Chapter 16) and so we refer here to [RÜC 1999] for details.

4.4.4 The Jacobian variety of curves

We come back to a projective absolutely irreducible curve C defined over the field K and the study of its divisor class group.

A first and easily verified observation is that G_K acts in a natural way on $\mathrm{Pic}^0_{C\cdot\overline{K}}$ and that

$$\mathrm{Pic}_C^0 = (\mathrm{Pic}^0_{C\cdot\overline{K}})^{G_K}$$

where $\mathrm{Pic}^0_{C\cdot\overline{K}}$ is the divisor class group of degree 0 of the curve over $\overline{K}$ obtained by base change from C.

More generally, take any field L between K and $\overline{K}$. Then $\mathrm{Pic}^0_{C\cdot L} = (\mathrm{Pic}^0_{C\cdot\overline{K}})^{G_L}$.

In the language of categories this means that for a fixed curve C, the Picard groups corresponding to curves obtained from C by base change define a functor Pic^0 from the set of intermediate fields L between K and $\overline{K}$ to the category of abelian groups.

It is very important that this functor can be represented by an absolutely irreducible smooth projective variety J_C defined over K. For all fields L between K and $\overline{K}$ we have that the functors of sets $L \mapsto J_C(L)$, the set of L-rational points of J_C, can be identified in a natural way with $L \mapsto \mathrm{Pic}^0_{C\cdot L}$.

But even more is true: J_C has the structure of an *algebraic group*. Since J_C is projective and absolutely irreducible this means that J_C *is an abelian variety*.

In particular, this implies that $J_C(L)$ is a group in which the group composition $\oplus$ is given by the evaluation of rational functions (if one takes affine coordinates) or polynomials (in projective coordinates) with coefficients in K on pairs $(P_1, P_2) \in J_C(L)^2$.

As a result we can introduce coordinates for elements in Pic_C^0 and compute by using algebraic formulas.

Definition 4.134 The variety J_C is called the *Jacobian (variety) of* C.

By using Theorem 4.106 we can give a birational description of J_C, which (essentially) proves its existence and makes it accessible for computations. It is based on the following lemma.

Lemma 4.135 Let C/K be a nonsingular, projective, absolutely irreducible curve of genus g with a K-rational point P_∞ corresponding to the place $\mathfrak{p}_\infty$. For every K-rational divisor class $\overline{D}$ of degree 0 of C there exists an effective divisor D of degree $\deg(D) = g$ such that $D - g\,\mathfrak{p}_\infty \in \overline{D}$.

Proof. Take any $D' \in \overline{D}$ with $D' = D_1 - D_2$ as difference of two effective K-rational divisors. In the first step we choose l large enough so that $l - \deg(D_2) > g$ and by Lemma 4.108 find a function f_1 such that $-D_2 + (f_1) + l\,\mathfrak{p}_\infty$ is effective.

By replacing D' by $D' + (f_1)$ we can assume that $D' = D - k\,\mathfrak{p}_\infty$ with D effective and $k = \deg(D)$. If $k > g$ (otherwise we are done) we apply Lemma 4.108 to the divisor $D - (k-g)\,\mathfrak{p}_\infty$ and find a function f such that $D - (k-g)\,\mathfrak{p}_\infty + (f) := D_0$ is effective and therefore $D + (f) - k\,\mathfrak{p}_\infty = D_0 - g\,\mathfrak{p}_\infty$ is an element of $\overline{D}$ of the required form. □

Let C be as in Lemma 4.135 and take the g-fold Cartesian product C^g of C. As per Example 4.25, C^g is a projective variety of dimension g. Recall that an affine part of it is given in the following way:
Take C_a as a nonempty affine part of C in some affine space $\mathbb{A}^n$ with affine coordinates $(x_1, \ldots, x_n)$ and denote by $C^{(i)}$ an isomorphic copy of C with coordinates $(x_1^i, \ldots, x_n^i)$. Then C_a^g can be embedded into the affine space $\mathbb{A}^{gn}$ with coordinates $(x_1^1, \ldots, x_n^1, \ldots, x_1^g, \ldots, x_n^g)$.

Let S_g be the symmetric group acting on $\{1, \ldots, g\}$. It acts in a natural way on C^g by permuting the factors. On the affine part described above this action is given by permuting the sections $(x_1^i, \ldots, x_n^i)$. The action of S_g defines an equivalence relation on C^g. We denote the quotient by C^g/S_g.

It is not difficult to see that C^g/S_g is a projective variety defined over K. On the affine part C_a^g/S_g one proves this as follows: take the ring of polynomials $K[x^1, \ldots, x^g]$ where x^j is shorthand for the n variables $x_1^j, \ldots, x_n^j$. On this ring, the group S_g acts by permuting $\{x^1, \ldots, x^g\}$. The polynomials fixed under S_g are symmetric and form a ring $R = K[x^1, \ldots, x^g]^{S_g}$. By a theorem of Noether (cf. [ZASA 1976]) there is a number m and an ideal I in $K[Y_1, \ldots, Y_m]$ with $R = K[Y_1, \ldots, Y_m]/I$. Hence, C_a^g/S_g is isomorphic to $V_I \subset \mathbb{A}^m$.

Let $\underline{P}$ be a point in $C^g/S_g(L)$ for a field L between K and $\overline{K}$. Then $\underline{P}$ is the equivalence class of a g-tuple $(P_1, \ldots, P_g)$ with $P_i \in C$ and for all $\sigma \in G_L$ we get: there is a permutation $\pi \in S_g$ such that $(\sigma P_1, \ldots, \sigma P_g) = (P_{\pi(1)}, \ldots, P_{\pi(g)})$.

This means that for any P_i the tuple $(P_1, \ldots, P_g)$ contains the whole Galois orbit $G_L \cdot P_i$. Assume that it consists of k disjoint G_L-orbits, each of them corresponding to a place $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ of $K(C)\cdot L$. Hence the formal sum $P_1 + \cdots + P_g$ corresponds to the L-rational divisor $\mathfrak{p}_1 + \cdots + \mathfrak{p}_k$ which is positive and of degree g.

This way we get a map ϕ_L from $C^g(L)$ to $\mathrm{Pic}^0_{C\cdot L}$ defined by

$$\phi_L(\underline{P}) \mapsto (\mathfrak{p}_1 + \cdots + \mathfrak{p}_k - g\,\mathfrak{p}_\infty),$$

where $(\mathfrak{p}_1 + \cdots + \mathfrak{p}_k - g\,\mathfrak{p}_\infty)$ is the divisor class of degree zero associated to $\mathfrak{p}_1 + \cdots + \mathfrak{p}_k$.

Using the alternative description of L-rational divisors as sums of points on C that consist of Galois orbits under G_L we get a more elegant description of ϕ_L: let $(P_1, \ldots, P_g) \in C^g$ be a representative of $\underline{P} \in C^g/S_g$. Define $\phi(\underline{P})$ as the divisor class of $P_1 + \cdots + P_g - g\,P_\infty$ in $\mathrm{Pic}^0_{C\cdot\overline{K}}$. Then ϕ_L is the restriction of ϕ to $\mathrm{Pic}^0_{C\cdot L}$.

Theorem 4.136 Assume that C is a curve of genus $g > 0$ with a K-rational point P_∞. Then C^g/S_g is birationally isomorphic to J_C, and the map ϕ defined above represents a birational part of the functorial isomorphism between $J_C(L)$ and $\mathrm{Pic}^0_{C.L}$. It maps the symmetry class $\underline{P}_\infty$ of the point $(P_\infty, \ldots, P_\infty)$ to the zero class and so $\underline{P}_\infty$ corresponds to the neutral element of the algebraic group J_C .

4.4.5 Jacobian variety of elliptic curves and group law

We come back to elliptic curves as introduced in Definition 4.111 and make concrete all of the considerations discussed above.

Assume that E is an elliptic curve with function field $K(E)$. Hence, E can be given as plane projective cubic without singularities and with (at least) one K-rational point P_∞. Clearly $E^1/S_1 = E$.

Let $\overline{D} \in \mathrm{Pic}^0_E$ be a divisor class of degree 0, $D \in \overline{D}$ a K-rational divisor. By the Riemann–Roch theorem 4.106 the space $L(D + P_\infty)$ has dimension 1. So there is an effective divisor in the class of $D + P_\infty$, and since this divisor has degree 1 it is a prime divisor corresponding to a point $P \in E(K)$, and $\phi_K(P) = \overline{D}$. So, $E(K)$ is mapped bijectively to Pic^0_E, the preimage of a divisor class $\overline{D}$ is the point P on E corresponding to the uniquely determined prime divisor in the class of $D + P_\infty$ with $D \in \overline{D}$.

This implies that E is isomorphic to its Jacobian as projective curve. So $E(K)$ itself is an abelian group with the chosen point P_∞ as neutral element, and the addition of two points is given by rational functions in the coordinates in the points.

Hence E is an abelian variety of dimension 1 (and vice versa) and we can apply all the structural properties of abelian varieties discussed above to study the structure of $E(K)$ (in dependence of K). This and the description of the addition with respect to carefully chosen equations for E will be among the central parts of the algorithmic and applied parts of the book (cf. Chapter 13).

Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points with $x_1 \neq x_2$ of the affine curve

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

The isomorphism maps them to divisor classes with representatives $D_P = P - P_\infty$ and $D_Q = Q - P_\infty$ of degree 0. The space $L(D_P + D_Q + P_\infty)$ has dimension 1 by Riemann–Roch. Hence, there exists a function passing through P and Q and having a pole of order at most 1 in P_∞. Such a function is given by the line $l(x, y) = y - \lambda x - \mu = 0$ connecting P and Q. It has

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \quad \text{and} \quad \mu = y_1 - \lambda x_1.$$

As $D_P + D_Q + P_\infty = P + Q - P_\infty$ has degree 1 and $l \in L(D_P + D_Q + P_\infty)$, there exists an effective divisor in this class that we denote by R and which is a prime divisor. Hence, in the divisor class group we have $\overline{D}_P + \overline{D}_Q = \overline{R} + \overline{P}_\infty$, which is equivalent to $P \oplus Q = R$ on E using the isomorphism from above.

Choosing $P \neq Q$ with $x_1 = x_2$ we apply the same geometric construction and get as connecting line the parallel to the y-axis $x = x_1$. Hence, the third intersection point has to be interpreted as the point P_∞. This associates to each point $P \in E$ an inverse point $-P$ which has the same x-coordinate.

In the remaining case $P = Q$ one can use the considerations above. The function $l \in L(2P - P_\infty)$ passes through P with multiplicity 2, i.e., it is the tangent line to the curve at P. In formulas this means

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} \quad \text{and} \quad \mu = y_1 - \lambda x_1.$$

4.4.5.a Division polynomials

By Theorem 4.73 we know the structure of the group of n-torsion points on E. In that context we showed that for each n there exists a polynomial ψ_n such that the x-coordinates of n-torsion points are the roots of ψ_n. These polynomials are called *division polynomials*.

If $\mathrm{char}(K) \neq 2$, put

$$\begin{aligned} &f_0(x) = 0,\ f_1(x) = 1,\ f_2(x) = 1,\\ &f_3(x) = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8,\\ &f_4(x) = 2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + (b_4b_8 - b_6^2) \end{aligned}$$

where the b_i's are defined as in Section 4.4.2.a and for $n \geqslant 5$

$$\begin{aligned} f_{2n} &= f_n(f_{n+2}f_{n-1}^2 - f_{n-2}f_{n+1}^2),\\ f_{2n+1} &= \begin{cases} \tilde{f}^2 f_{n+2}f_n^3 - f_{n-1}f_{n+1}^3) & \text{if } n \text{ is even,}\\ f_{n+2}f_n^3 - \tilde{f}^2 f_{n-1}f_{n+1}^3) & \text{otherwise.} \end{cases} \end{aligned}$$

with $\tilde{f}(x) = 4x^3 + b_2x^2 + 2b_4x + b_6$.

If $\mathrm{char}(K) = 2$ and $E : y^2 + xy = x^3 + a_2x^2 + a_6$ then set

$$\begin{aligned} &f_0(x) = 0,\ f_1(x) = 1,\ f_2(x) = x,\\ &f_3(x) = x^4 + x^3 + a_6,\ f_4(x) = x^6 + x^2a_6. \end{aligned}$$

Otherwise $E : y^2 + a_3y = x^3 + a_4x + a_6$ and put

$$\begin{aligned} &f_0(x) = 0,\ f_1(x) = 1,\ f_2(x) = a_3,\\ &f_3(x) = x^4 + a_3^2x + a_4^2,\ f_4(x) = a_3^5. \end{aligned}$$

For $n \geqslant 5$, they can be computed recursively in both cases with the formulas

$$\begin{aligned} f_{2n+1} &= f_{n+2}f_n^3 - f_{n-1}f_{n+1}^3,\\ f_2f_{2n} &= f_{n+2}f_nf_{n-1}^2 - f_{n-2}f_nf_{n+1}^2. \end{aligned}$$

Now if $P = (x_1, y_1) \in E(\overline{K})$ is not a 2-torsion point then $P \in E[n]$ if and only if $P = P_\infty$ or $f_n(x) = 0$.

In addition there are explicit formulas for $[n]$ when $\mathrm{char}(K)$ is different from 2, namely

$$\begin{aligned} &[n] : E \to E\\ &P \mapsto [n]P = \begin{cases} P_\infty & \text{if } P \in E[n],\\ \left(\dfrac{\phi_n(x,y)}{\psi_n^2(x,y)}, \dfrac{\omega_n(x,y)}{\psi_n^3(x,y)}\right) & \text{if } P \in E(\overline{K}) \smallsetminus E[n]. \end{cases} \end{aligned}$$

where

$$\psi_n = \begin{cases} (2y + a_1x + a_3)f_n & \text{if } n \text{ is even,}\\ f_n & \text{otherwise} \end{cases}$$

and

$$\phi_n = x\psi_n^2 - \psi_{n-1}\psi_{n+1} \text{ and } 2\psi_n\omega_n = \psi_{2n} - \psi_n^2(a_1\phi_n + a_3\psi_n^2).$$

Note that in general these formulas are not used to compute $[n]P$ for given n and P.

4.4.6 Ideal class group

The divisor class group relies on the projective curve and leads to points on an abelian variety. For computational reasons it is sometimes easier to work with affine parts and the arithmetic of corresponding affine algebras $\mathcal{O}$.

The objects corresponding to divisors are ideals of $\mathcal{O}$ and the objects corresponding to divisor classes are ideal classes of $\mathcal{O}$. The purpose of this section is to discuss the relation between these groups.

Let C be an affine smooth curve with function field $K(C)$ and coordinate ring $\mathcal{O} = K[C]$.

We recall that $\mathcal{O}$ is a Dedekind ring and so every ideal $\neq (0)$ is a product of powers of maximal ideals M in a unique way and every maximal ideal M corresponds to a place $\mathfrak{p}_M$ of $K(C)$.

The ideals $\neq 0$ of $\mathcal{O}$ form a semigroup freely generated by the maximal ideals. To get a group one generalizes $\mathcal{O}$-ideals:

Definition 4.137 The set $B \subset K(C)$ is a *fractional $\mathcal{O}$-ideal* if there exists a function $f \in K(C)^*$ such that fB is an ideal of $\mathcal{O}$. For a maximal ideal $M \subset \mathcal{O}$ define $v_M(B) := \max\{k \in \mathbb{Z} \mid B \subset M^k\}$. Then

$$B = \prod_{M \text{ maximal in } \mathcal{O}} M^{v_M(B)}$$

and $B \subset \mathcal{O}$ if and only if all $v_M(B) \geqslant 0$.

To form the ideal class group we let two $\mathcal{O}$-ideals B_1 and B_2 be *equivalent* if and only if there exists a function $f \in K(C)$ with $v_M(B_1) = v_M(B_2) + v_M\big((f)\big)$ for all maximal ideals M of $\mathcal{O}$.

The group of $\mathcal{O}$-ideal classes is denoted by $\mathrm{Cl}(\mathcal{O})$.

4.4.6.a Relation between divisor and ideal class groups

Here we want to explain the relation between ideal class groups of rings of regular functions of affine parts of absolutely irreducible smooth projective curves C and the divisor class group of C (hence points of the Jacobian J_C).

For the simplicity of our presentation we shall assume that there is a K-rational point P_∞. Let x_1 be a nonconstant function on C with pole divisor

$$\mathrm{div}(x_1)_\infty = m_\infty P_\infty + \sum_{2 \leqslant j \leqslant t} m_j P_{\infty_j},$$

and $t \geqslant 0$, $m_\infty > 0$, $m_j > 0$ and $P_{\infty_j} \in C(\overline{K})$. Put $P_{\infty_1} = P_\infty$. Let $\mathcal{O}$ be the ring of functions on C that are regular outside of the points P_{∞_j}. So $\mathcal{O}$ is the intersection of the valuation rings $\mathcal{O}_\mathfrak{p}$ of all places $\mathfrak{p}$ of $K(C)$ with $v_\mathfrak{p}(x_1) \geqslant 0$.

It follows that $\mathcal{O}$ is the integral closure of the polynomial ring $K[x_1]$ in $K(C)$. It is the coordinate ring of the affine curve $C_\mathcal{O}$ with $C_\mathcal{O}(\overline{K}) = C(\overline{K}) \setminus \{P_{\infty_1}, \ldots, P_{\infty_t}\}$.

The inclusion $K[x_1] \to \mathcal{O}$ corresponds to a morphism $C_\mathcal{O} \to \mathbb{A}^1$, which extends to a map $\pi : C \to \mathbb{P}^1$ with $\pi^{-1}(\infty) = \{P_{\infty_1}, \ldots, P_{\infty_t}\}$. To describe a relation between points on J_C and elements of $\mathrm{Cl}(\mathcal{O})$, we state that every place of $K(C)$ is either equal to $\mathfrak{p}_M$ for some maximal ideal M of $\mathcal{O}$ or to an extension of the infinite place on $\mathbb{P}^1$ to C.

Hence, there is a one-to-one correspondence between proper ideals $A \subset \mathcal{O}$ and effective K-rational divisors D of C in which only points of $C_\mathcal{O}$ occur, given by

$$\sum n_i \mathfrak{p}_i \leftrightarrow \prod M_{\mathfrak{p}_i}^{n_i},$$

where the $\mathfrak{p}_i$ are not extensions of $\mathfrak{p}_\infty$. If A corresponds to D then $\deg(D) = \deg(A)$. This correspondence extends naturally to fractional ideals and arbitrary divisors.

Now we apply the theorem of Riemann–Roch to ideal classes of $\mathcal{O}$ to get

Lemma 4.138 With notation as above let C be a curve of genus g. Let c be an element of $\mathrm{Cl}(\mathcal{O})$. Then c contains an ideal $A \subset \mathcal{O}$ with $\deg(A) \leqslant g$.

Proof. Let $A' \in c$ be an $\mathcal{O}$-ideal and assume that $\deg(A') > g$. Take the effective divisor $D_{A'}$ associated to A' and a function f such that $D' := (f) + D_{A'} - \big(\deg(A') - g\big)P_\infty$ is effective of degree g. Let D'' be the divisor obtained from D' by removing points in $\pi^{-1}(\infty)$ and let A be the ideal obtained from D''. Then $A \in c$ and $\deg(A) \leqslant g$. □

Note that principal divisors are mapped to principal ideals. Therefore, one can consider the correspondence between divisor classes and ideal classes. We are now ready to define a homomorphism from J_C to the ideal class group $\mathrm{Cl}(\mathcal{O})$.

Define $\phi : J_C(K) \to \mathrm{Cl}(\mathcal{O})$ by the following rule: in the divisor class c take a representative D' of the form $D' = D - g\,P_\infty$, D effective. Remove from D all points in $\pi^{-1}(\infty)$ and define A as ideal in $\mathcal{O}$ like above. Then $\phi(c)$ is the class of A in $\mathrm{Cl}(\mathcal{O})$. By Lemma 4.138 ϕ is surjective.

For applications one is usually interested in the case that the kernel of ϕ is trivial, i.e., in choices for C and $\mathcal{O}$ such that $\mathrm{Cl}(\mathcal{O}) \simeq \mathrm{Pic}^0_C$. This allows us to use the interpretation via ideal classes of polynomial orders $\mathcal{O}$ for the computations whereas the interpretation as points on the Jacobian of C is used for the structural background.

So let us describe the kernel of ϕ: let c be a divisor class of degree 0 represented by the divisor $D = D_1 + D_2 - gP_{\infty_1}$, where D_i are effective divisors and $D_1 = \sum n_i P_i$ with $P_i \notin \pi^{-1}\{\infty\}$ and $D_2 = \sum m_j P_{\infty_j}$ with $P_{\infty_j} \in \pi^{-1}\{\infty\}$. If $\phi(c) = 0$ then $\prod M_{P_i}^{n_i}$ is a principal ideal (f) with $f \in \mathcal{O}$. Hence, all prime divisors occurring in the pole divisor of f correspond to points in $\pi^{-1}\{\infty\}$ and we can replace D by an equivalent divisor $D - (f)$ of degree 0, which is a sum of prime divisors all corresponding to points in $\pi^{-1}\{\infty\}$.

Proposition 4.139 We use the notation from above. The homomorphism

$$\phi : J_C(K) \to \mathrm{Cl}(\mathcal{O})$$

is surjective.

The kernel of ϕ is equal to the divisor classes of degree 0 in

$$\Big\{ \sum m_j P_{\infty_j} \,|\, \sum m_j = 0 \ \text{ and all } \ P_{\infty_j} \in \pi^{-1}\{\infty\} \Big\}.$$

Proposition 4.140 Assume that there is a cover

$$\varphi : C \to \mathbb{P}^1,$$

in which one point P_∞ is totally ramified and induces the place v_∞ in the function field $K(x_1)$ of $\mathbb{P}^1$. Let $\mathcal{O}$ be the integral closure of $K[x_1]$ in the function field of C. Then ϕ is an isomorphism and, hence, the ideal class group of $\mathcal{O}$ is (in a natural way) isomorphic to the divisor class group of C.

This gives a very nice relation of the projective algebraic geometry and the ideal theory in Dedekind rings. Due to the isomorphism the ideal class group can be used for arithmetic while the divisor class group setting provides structural background.

Definition 4.141 A nonsingular curve C/K for which there exists a cover φ in which one K-point $P_\infty \in C$ is totally ramified is called a *C_{ab}-curve*.

If the functions x and y have pole divisor aP_∞ and bP_∞, respectively, one finds an equation over K given by

$$C : \alpha_{b,0}x^b + \alpha_{0,1} + \sum_{ia+jb<ab} \alpha_{i,j}x^i y^j, \ \text{ with } \ \alpha_{i,j} \in K,$$

with $\alpha_{b,0}, \alpha_{0,1} \neq 0$.

In particular, hyperelliptic curves are C_{ab} curves if they have a K-rational Weierstraß point and if we take as affine part the curve given by a Weierstraß equation (4.1). This relation is the topic of the following section.

Example 4.142 An interesting class of curves are the *Picard curves* of genus 3. Over a field of characteristic $\mathrm{char}(K) \neq 3$ containing the third roots of unity they can by given by an equation of the form

$$y^3 = f(x),$$

where $f(x) \in K[x]$ is monic of degree 4 and has only simple roots over $\overline{K}$.

4.4.7 Class groups of hyperelliptic curves

The type of hyperelliptic curves C we consider in this book additionally satisfies that there exists one K-rational Weierstraß point of C. This point is totally ramified under a cover ϕ and is denoted by P_∞. By the considerations of the previous paragraph these curves satisfy that the ideal class group and the divisor class group are isomorphic. In Chapter 14 on the arithmetic of hyperelliptic curves we will use the ideal class group for the efficient computations inside the group. To fix notation we still speak of divisor classes usually implying this isomorphism. In Section 4.4.2.b we have shown how one can use the definition and the Riemann–Roch theorem to derive an affine plane equation. The K-rational point P_∞ allows us to use the divisor of degree one in the construction.

Recall that a hyperelliptic curve over K of genus g with at least one K-rational Weierstraß point can be given by a *Weierstraß equation*

$$y^2 + h(x)y = f(x), \text{ with } h(x) \text{ and } f(x) \in K[x], \tag{4.3}$$

where f is monic of degree $2g+1$ and $\deg(h) \leqslant g$. By abuse of language we denote affine curves given by such an equation as *imaginary quadratic curves*.

We use the equation of such curves C to describe explicitly their ideal class group.

Theorem 4.143 Let C/K be an imaginary quadratic hyperelliptic curve of genus g and let ω denote the nontrivial automorphism of $K(C)$ over $K(x)$ with a K-rational Weierstraß point P_∞ lying over the place x_∞ of $K(x)$. Let $\mathcal{O} = K[x,y]/\big(y^2 + h(x)y - f(x)\big)$.

(i) In every nontrivial ideal class c of $\mathrm{Cl}(\mathcal{O})$ there is exactly one ideal $I \subseteq \mathcal{O}$ of degree $t \leqslant g$ with the property: the only prime ideals that could divide both I and $\omega(I)$ are those resulting from Weierstraß points.

(ii) Let I be as above. Then $I = K[x]u(x) + K[x]\big(v(x) - y\big)$ with $u(x), v(x) \in K[x]$, u monic of degree t, $\deg(v) < t$ and u divides $v^2 + h(x)v - f(x)$.

(iii) The polynomials $u(x)$ and $v(x)$ are uniquely determined by I and hence by c. So $[u, v]$ can be used as coordinates for c.

Proof. Since for every ideal J we get that $J \cdot \omega(J)$ is a principal ideal we can reduce I repeatedly until the condition in (i) is satisfied without changing its class. After this process we call J reduced.

Now assume that $\deg(I) \leqslant g,\ \deg(J) \leqslant g$, with I, J reduced and that $I \sim J$. Then $I \cdot \omega(J)$ is a principal ideal in $\mathcal{O}$ and so it is equal to (b) with $b \in K(C)$ having only one pole of order $\leqslant 2g$ in P_∞. By Riemann–Roch all such functions lie in a K-vector space of dimension $g+1$ and a basis of this space is given by $\{1, x, x^2, \ldots, x^g\}$. So $b \in K[x]$ and $I \cdot \omega(J)$ is the conorm of an ideal in $K[x]$. Since I and J are reduced this means that $I = J$ and (i) is proved.

(ii). Let $I \in O$ be an ideal of degree t. Recall that $\{1, y\}$ is a basis of $\mathcal{O}$ as $K[x]$-module. We choose any basis $\{w_1 = f_1(x) + f_2(x)y,\ w_2 = g_1(x) + g_2(x)y\}$ of I as $K[x]$-module. We find relatively prime polynomials h_1, h_2 with $f_2h_1 - g_2h_2 = 0$ and choose $u_1, u_2 \in K[x]$ with $u_1h_1 - u_2h_2 = 1$. Now take $u' := h_1w_1 + h_2w_2, w_2' = u_2w_1 + u_1w_2$. Since the determinant of this transformation is 1 the pair $\{u'(x), w_2' = v_1(x) + v_2(x)y\}$ is again a basis of I. Since the rank of I is 2, $v_2(x)$ is not equal to 0. So $I \bigcap K[X]$ is generated by u'. Since I is reduced, the degree of I is equal to the degree of u' and we can and will take u monic. Now write $v_1 = au + v$ with $\deg v < t$. By replacing w_2' by $w_2' - a\,u$ we get a basis $\{u(x), v(x) + v_2(x)y\}$ of I. Since the degree of I is equal to $u(x)v_2(x)$ we get: $v_2(x)$ is constant and so we can assume $v_2(x) = -1$. The element $(v + y)(v - y) = v^2 + h(x)y - f(x) = \big(v^2 + h(x)v - f(x)\big) - h(x)(v - y)$ lies in I and so the last claim of (ii) follows.
(iii). From the proof of (ii) we have that $u(x)$ is determined by I as monic generator of $I \bigcap K[x]$. Now assume that $v' - y \in I$ with $\deg(v') < t$. Then $v' - v \in I \bigcap K[x]$ and hence $v' - v = 0$. □

Remark 4.144 We are in a very similar situation as in the case of class groups of imaginary quadratic fields. In fact, Artin has generalized the theory of ideal classes of imaginary quadratic number fields, due to Gauß, to hyperelliptic function fields connecting ideal classes of $\mathcal{O}$ with reduced quadratic forms of discriminant $f(x)$ and the addition $\oplus$ with the composition of such forms. Theorem 4.143 and its proof can easily be translated into this language.

We are now in a position to use the results obtained in the previous section and describe the divisor class group of C using the ideal class group of the affine part.

Theorem 4.145 (Mumford representation)
Let C be a genus g hyperelliptic curve with affine part given by $y^2 + h(x)y - f(x)$, where $h, f \in K[x],\ \deg f = 2g + 1,\ \deg h \leqslant g$. Each nontrivial group element $\overline{D} \in \mathrm{Pic}_C^0$ can be represented via a unique pair of polynomials $u(x)$ and $v(x),\ u, v \in K[x]$, where

(i) u is monic,

(ii) $\deg v < \deg u \leqslant g$,

(iii) $u \mid v^2 + vh - f$.

Let $\overline{D}$ be uniquely represented by $D = \sum_{i=1}^{r} P_i - rP_\infty$, where $P_i \neq P_\infty, P_i \neq -P_j$ for $i \neq j$ and $r \leqslant g$. Put $P_i = (x_i, y_i)$. Then the corresponding polynomials are defined by

$$u = \prod_{i=1}^{r} (x - x_i)$$

and the property that if P_i occurs n_i times then

$$\left(\frac{d}{dx}\right)^j \big[v(x)^2 + v(x)h(x) - f(x)\big]_{|x=x_i} = 0, \ \text{ for } 0 \leqslant j \leqslant n_i - 1.$$

A divisor with at most g points in the support satisfying $P_i \neq P_\infty, P_i \neq -P_j$ for $i \neq j$ is called a *reduced divisor*. The first part states that each class can be represented by a reduced divisor. The second part of the theorem means that for all points $P_i = (x_i, y_i)$ occurring in D we have $u\big(x_i\big) = 0$ and the third condition guarantees that $v\big(x_i\big) = y_i$ with appropriate multiplicity.

Like for elliptic curves (cf. Section 4.4.5) one can make explicit the group operations in the ideal class group. Consider the classes represented by $[u_1(x), v_1(x)]$ and $[u_2(x), v_2(x)]$ and assume them in general position. The product of the representatives is generated by

$$\langle u_1u_2, u_1(y - v_2), u_2(y - v_1), (y - v_1)(y - v_2)\rangle.$$

By Hermite reduction from the generating system we obtain a basis $\{u_3'(x), v_3'(x) + w_3'(x)y\}$. This ideal lies in the class of the product of the ideal classes but is usually not yet reduced. To reduce it one recursively applies the fact that $u \mid v^2 + hv - f$. This procedure is formalized and applied to arbitrary inputs in Cantor's algorithm, which we state in Chapter 14 on the arithmetic of hyperelliptic curves.