Carl von Ossietzky
Universität Oldenburg
Diplomstudiengang Mathematik

DIPLOMARBEIT

The Arithmetic of Elliptic and Hyperelliptic Curves with Applications to Pairing-Based Cryptography

vorgelegt von: **Andreas Peter**

Erster Gutachter: **Prof. Dr. Andreas Stein**
Zweiter Gutachter: **Prof. Dr. Heinz-Georg Quebbemann**

Oldenburg, den 24. März 2009

Contents

Chapter I

Introduction

In this first chapter, we want to introduce some basic notions that are necessary to understand *public-key cryptography*, which is one of the main applications of the theory discussed in this thesis. It serves as a motivation, and we will lay the groundwork for it in section I.1. At this point, we should warn the reader that we expect him/her to have been exposed to some cryptography before. This thesis focuses on mathematics (some of it needed for cryptography) and only wants to give a few applications, without going into too much detail. We will give references for the interested reader, who wants to learn more about cryptography. Then, in section I.2, we will explain briefly what each chapter of this thesis is about, and will make the author's special contribution very clear. Also, we want to give an overview of all results that are either new or to which the author presents new approaches. In the last section of the present chapter, we would like to clarify specific notations used in the work at hand.

I.1 Motivation: A Short Introduction to Public-Key Cryptography

To begin with, we consider the following situation: Two people, traditionally called Alice and Bob (abbreviated as A and B, respectively) want to communicate over an insecure channel (e.g. over the Internet) in such a way that an eavesdropper Eve (abbreviated as E) on the conversation is unable to understand or change the messages that are being communicated by A and B. A way to obtain such a secure communication is by using a problem that is computationally easy to set up by A and B, but computationally infeasible for E to solve. The most prominent example of such a secure way to communicate is the *RSA cyptosystem*, which is based on the *integer factorization problem*, i.e. finding a nontrivial factor of a composite integer (see chapter 8 of [MvOV96] for details). Another way would be to use the *discrete logarithm problem*, which we want to discuss in some detail in section I.1.1.

The basic idea behind public-key cryptography is that the two participants A and B both possess two keys, a *public* key and a *private* key. The former being public knowledge and the latter being known only to the participant it belongs to. There

are two ways, we want to explain here, on how those keys can be used to encrypt and decrypt messages using some (for the moment unspecified) encryption and decryption method.

The first idea is for A to use B's public key to encrypt messages that are meant for B, whereas B decrypts messages that are meant for him, by using his private key. Similarly, this would work by changing the roles of A and B. Now in order for this to work, the public and private key of B (respectively A) must be related in a certain way. This relation is usually established by the use of *one-way functions*. Loosely speaking, a one-way function is an invertible function that is easy to compute, but whose inverse is difficult to compute (for a precise definition, see [MvOV96, Ch. 1, definition 1.13, p. 8]). By using such one-way functions, each participant can randomly generate a private key, and then compute the associated public key with the chosen one-way function. This means that it is computationally infeasible to retrieve the private key from the public key. The process of computing/generating the pair of keys is called *key generation*. Although it is unproven whether such one-way functions really exist, there do exist functions that are believed to be good candidates for being one-way. We will give an explicit example of such a function in chapter VII and also in section I.1.1.

The second idea to use public and private keys is to create a single key, that should only be known to the participants A and B, which can then be used in some *symmetric-key encryption scheme* (see [MvOV96] for details on that topic). We want to present the basic idea for such a key exchange in section I.1.2, and discuss a very explicit situation in chapter VII.

I.1.1 Discrete Logarithm Systems

In this section, we want to give a first example of a function that is, in certain cases, believed to be a one-way function. The general setting is as follows: Let G be an additively written cyclic group of prime order m, generated by an element $P \in G$. For certain groups G, the surjective function

$$f : \mathbb{Z} \to G \text{ defined by } n \mapsto [n]P := \underbrace{P + \ldots + P}_{n \text{ times}}$$

is believed to be one-way. Since P has order m, it is clear that $\ker(f) = m\mathbb{Z}$. This yields the group isomorphism

$$\phi : \mathbb{Z}/m\mathbb{Z} \cong G.$$

We denote the inverse map of ϕ by $\log_P$, i.e.

$$\log_P : G \to \mathbb{Z}/m\mathbb{Z},$$

and call it the *discrete logarithm (to the base of P)*. The problem of computing it, is called the *discrete logarithm problem (to the base of P)* (abbreviated as DLP). In other words, it is the problem of determining $k \in \mathbb{Z}$ with $Q = [k]P$ when only given P and $Q \in G$. Clearly, the integer k is uniquely determined modulo m. The complexity of

the DLP depends on the choice of G with its operation $+$.

Definition I.1.1. Let G be a cyclic group with operation "$+$" that is generated by $P \in G$. The triple $(G, +, P)$ is called a *discrete logarithm (DL) system*.

Now, our task is to find suitable DL systems $(G, +, P)$ such that the DLP is hard to solve. There is one easy example of such a suitable system, which is very important.

Example I.1.2. Let $q = p^r$ be a power of a prime number $p \in \mathbb{N}$ and let $m \in \mathbb{N}$ with $m \mid q - 1$. From basic group theory, we know that there is a non-trivial element $\zeta \in \mathbb{F}_q^*$ of order m. So ζ is a primitive m-th root of unity. We take the cyclic subgroup $\langle \zeta \rangle \subseteq \mathbb{F}_q^*$ generated by ζ as our group G with the multiplication "$\cdot$" as its operation. The mapping f would then look like

$$f : \mathbb{Z} \to G, n \mapsto \zeta^n.$$

For "big" choices of m and q, the DLP is believed to be hard. In fact, the fastest known algorithms have *subexponential* execution times in theses cases (see below for more information on the complexity of algorithms). The interested reader is refered to [ACD+06, Ch. 19].

There are other groups G that appear to be good choices, too. For instance, groups associated to *elliptic* and *hyperelliptic curves* of small genus, which we want to study in this thesis (see chapters IV and V), turn out to be suitable. We will not address the DLP on these groups in all detail, but we will explain methods to attack the problem (see chapter VII). Here, we only want to remark that the DLP on such groups is, in some cases, still believed to have *exponential complexity* (cf. [ACD+06]).

Complexity of Algorithms

We have already mentioned two types of complexity, namely subexponential and exponential complexity. Here, we would like to explain what we mean by the *complexity* of an algorithm in a rather short and informal way (for a rigorous approach, see [BB96]).

First of all, we will always assume that any input of an algorithm is written in binary, and all arithmetic is performed to the base 2. So all operations an algorithm can perform are bit operations. In order to be able to define the complexity of an algorithm, we need the following notation:

Definition I.1.3. Let $f, g : \mathbb{N} \to \mathbb{R}_{\geq 0}$ be two functions. We define the *big-O notation* as:

$$g = O(f) : \iff \exists c > 0 : g(n) \leq cf(n),$$

where $n > n_0$ for some constant $n_0 \in \mathbb{N}$.

If ln denotes the natural logarithm (i.e. the logarithm to the base e), we have the following important definition.

Definition I.1.4. For an even positive integer $n \in \mathbb{N}$, we let $\gamma \in \mathbb{R}$ with $0 \leq \gamma \leq 1$, and $c > 0$ be a positive constant. We define

$$L_n(\gamma; c) := O\left(e^{c\left((\ln n)^{\gamma}(\ln \ln n)^{1-\gamma}\right)}\right).$$

If an algorithm, when applied to an input of (bit-)length at most $\log_2 n$, needs $L_n(\gamma; c)$ bit operations for some $c > 0$, then it is called an $L(\gamma)$-*algorithm*.

Certainly, we have

$$L_n(1; c) = O(e^{c \ln n}) = O(n^c) \text{ and } L_n(0; c) = O(e^{c \ln \ln n}) = O((\ln n)^c).$$

Now, we are in a position to define the different types of complexities.

Definition I.1.5.

1. An $L(0)$-algorithm has *polynomial complexity* (or runs in *polynomial time*).
2. An $L(1)$-algorithm has *exponential complexity* (or runs in *exponential time*).
3. An $L(\gamma)$-algorithm, with $\gamma < 1$, has *subexponential complexity* (or runs in *subexponential time*).

Discrete Logarithm Systems with Bilinear Structure

The groups associated to (hyper-)elliptic curves that we have mentioned before, have an additional property, which we want to discuss here very briefly. More details can be found in chapters VI and VII.

Assume that we are given two DL systems $(G, +, P)$ and $(G', +', P')$ (additively written), in which the arithmetic can be done equally fast (this is meant in terms of definition I.1.5). Both groups G and G' have prime order m. Moreover, let $(H, \cdot, Q)$ (multiplicatively written) be another DL system, and suppose that we have a mapping

$$e : G \times G' \to H,$$

which satisfies the following properties:

1. e is *bilinear*: For all $a, b \in \mathbb{N}$, we have

$$e([a]P, [b]P') = e(P, P')^{ab}.$$

2. e is *strongly non-degenerate*: For all $a, b \in \mathbb{N}$, we have

$$e([a]P, P') = e([b]P, P') \iff a \equiv b \pmod{m}.$$

3. e is *efficiently computable*, i.e. it exists an algorithm of polynomial complexity that computes e.

Definition I.1.6. In the above situation, we call (G, e) a *DL system with bilinear structure*.

This bilinear structure on G can be used to construct new cyptographic protocols, as we will discuss in the next section. Unfortunately, it can also be used in a destructive manner, namely by "transferring" a DLP in G to a DLP in H, where it might be easier to solve. Obviously, this can only work, if we can find a $b \in \mathbb{N}$ such that the map $a \mapsto e([a]P, [b]P')$ is injective (this ensures that we can tranfer the solution in H back to a solution in G). How this works in a very explicit situation will be explained in chapter VII.

I.1.2 Protocols

We want to give some examples of how the introduced DL systems can be used in public-key cryptography. To this end, we start by explaining how two people A and B can exchange a secret key. We will then use a DL system with a bilinear structure to generalize this method to three persons. Also, we would like to introduce a very easy way to encrypt messages by using the so called *ElGamal encryption*, which is based on the DLP in some DL system.

Diffie-Hellman Key Exchange

We want to present a protocol for two parties to exchange a secret key. Diffie and Hellman were the first who described it in [DH76], which is the reason why it is called the *Diffie-Hellman* protocol. Assume that A and B want to exchange a secret key in such a way that an eavesdropper E is unable to retrieve their secret key by just listening to their conversation.

A and B take off with a DL system $(G, +, P)$, which is public knowledge and in which the DLP should be hard to solve. The secret key they want to exchange should be an element of G. Now, A and B secretly choose random positive integers a and b (their private keys) and compute $P_A = [a]P$ and $P_B = [b]P$ (their public keys), respectively. Then, they publicly exchange their public keys P_A and P_B, and since the DLP in G is hard, an eavesdropper E is unable to obtain the private keys a or b from P_A or P_B, respectively. In this situation, A and B can respectively compute the elements $[a]P_B$ and $[b]P_A$, which are the same, since

$$[a]P_B = [ab]P = [b]P_A.$$

That way, they are both in possession of the common secret $[ab]P$, which can now be used as a key in some symmetric-key encryption scheme. The eavesdropper E would be left with the *computational Diffie-Hellman problem (CDHP)*, i.e. the problem of computing $[ab]P$ given P_A and P_B.

Assume that E has some special information telling her that $[c]P$ is the secret key, which A and B exchanged. She would then be left with the *decision Diffie-Hellman*

problem (DDHP), i.e. the problem of distinguishing $[ab]P$ from $[c]P$. This problem is certainly not harder than the CDHP.

At this point, it should be noted that the Diffie-Hellman protocol, as we presented it here, is not intended for use in practice. The eavesdropper E could easily attack the protocol by using the so called *man-in-the-middle* attack, i.e. E would pretend to be B for A and A for B. That way, B would (unknowingly) share a secret with E and E with A. Now, E could decrypt messages from B, read them, and then encrypt them again using the common key with A, and vice versa. Clearly, A and B would not notice the presence of E in this way.

As a closing note, we would like to refer the reader to chapter 30 of [ACD+06] concerning the generation of random numbers.

Tripartite Key Exchange

We want to generalize the Diffie-Hellman protocol to three parties by using a DL system (G, e) with bilinear structure (see section I.1.1 for notations). Assume that $G' = G$.

The protocol works as follows: Suppose that Alice (A), Bob (B) and Charlie (C) want to agree on a common secret key, which will be a group element of H. All participants secretly choose random positive integers a, b and c (their private keys) and compute $P_A = [a]P, P_B = [b]P$ and $P_C = [c]P$ (their public keys), respectively. Then, they publicly exchange their public keys P_A, P_B and P_C. Each of the participants can now compute the common secret

$$e(P, P)^{abc} = e(P_B, P_C)^a = e(P_A, P_C)^b = e(P_A, P_B)^c,$$

by using the bilinearity of e. Recall that $e(P, P)$ is non-trivial by the non-degeneracy of e, which is important to have a non-trivial common secret. An eavesdropper E would be left with the *computational bilinear Diffie-Hellman problem (CBDHP)*, i.e. the problem of computing $e(P, P)^{abc}$ given P_A, P_B and P_C. Similarly to the bipartite Diffie-Hellman protocol, there is also the *decision bilinear Diffie-Hellman problem (DBDHP)*, i.e. the problem of distinguishing $e(P, P)^{abc}$ from $e(P, P)^r$ for some given positive integer r.

Again, it should be noted that this protocol is not secure against a man-in-the-middle attack.

Before we proceed to the ElGamal encryption, we would like to stress that a cryptographic protocol on a DL system (G, e) with bilinear structure as above, should never rely on the DDHP in G. The reason for this is the following: Assume that we would like to decide whether $[ab]P = [c]P$ in G. Then, we could easily compute the values

$$e([a]P, [b]P) \text{ and } e([c]P, P).$$

If those two values are equal, we end up with $c \equiv ab \pmod{m}$ by using the non-degeneracy of e, since in this case, it holds:

$$e([c]P, P) = e([a]P, [b]P) = e([ab]P, P).$$

In other words, we know that $[c]P$ indeed is the same as the secret $[ab]P$.

ElGamal Encryption

Let us assume that A and B publicly agreed on a DL system $(G, +, P)$ in which the DLP is hard to solve. Moreover, suppose that they have already generated their pairs of public and private keys in G; say $(a, P_A := [a]P)$ is A's pair and $(b, P_B := [b]P)$ is B's, where a and b are random positive integers, as usual. In the following, we want to describe ElGamal's encryption method in a somewhat loose form (for details, we refer the reader to [MvOV96]).

Let $\mathcal{M}$ denote the set of all possible messages that A and B can communicate. Assume that A and B know some way to represent their messages as elements of the group G, i.e. we have a mapping

$$\varphi : \mathcal{M} \to G,$$

which should be invertible, so that they can transform elements of G back to messages. Now, if B wants to encrypt a message $m \in \mathcal{M}$ for A, he may use the *ElGamal encryption*:

First of all, B chooses a random number $k \in \mathbb{N}$ and computes the two values $[k]P$ and $[k]P_A$ by using A's public key P_A. The encrypted message then is the tuple $([k]P, R) \in G^2$, where $R := [k]P_A + \varphi(m)$.

A can now decrypt this message by using her private key a: Firstly, she computes

$$[a]([k]P) = [ak]P = [k]P_A.$$

Since φ is invertible, she can retrieve the original message by computing

$$\varphi^{-1}(R - [k]P_A) = \varphi^{-1}(\varphi(m)) = m.$$

I.2 Outline and Results

As the title of this diploma thesis suggests, we want to study the arithmetic of elliptic and hyperelliptic curves, while focusing on pairings on certain groups associated to these types of curves. In fact, the title is a bit of an understatement, since we will introduce curves in all their generality. Therefore, we start in chapter II by giving an extensive introduction to algebraic varieties, and to curves as special cases of these. Unlike the common literature on algebraic geometry proposes, we will work over *non*-algebraically closed, but perfect fields. This seems reasonable, as we need to work over finite fields in chapter VII for cryptographic applications. In current research on curves, most arithmetical properties are described in terms of algebraic function field theory. Consequently, the relations between algebraic curves and function fields lie at the heart of chapter II. We will show that function fields and nonsingular projective curves are the "same" (in a certain sense, see corollary II.7.18). Along the way, we give a very

intuitive introduction to morphisms of affine algebraic sets, and give new approaches and proofs to many results on the theory of algebraic curves. For a complete list of the author's contributions, the reader is refered to the introduction of chapter II.

Knowing that we can describe a nonsingular curve C defined over a perfect field k in terms of its function field $k(C)$, we recall many definitions and results from the theory of algebraic function fields of one variable in chapter III. As a particular delicacy, we prove a correspondence between places of $k(C)$ and Galois orbits of points on C in proposition III.4.1. Although rarely treated in the common literature, we introduce Chebotarev's density theorem in section III.6 in order to prove the non-degeneracy of the Tate-Lichtenbaum pairing in chapter VI.

Chapters IV and V finally discuss the theory of elliptic and hyperelliptic curves. While chapter IV has only very few new proofs, chapter V has a lot to offer. It gives a very general introduction to hyperelliptic curves together with a complete derivation of the group law in the Jacobian of such a curve. In addition, it intends to give new approaches and proofs to many results on hyperelliptic curves. Also, we explain how the group law can be performed by an algorithm, called Cantor's algorithm.

Chapter VI certainly is the jewel of this thesis. Not only has it the most to offer, but also needs all the theory from its preceding chapters. It presents a new approach to the Weil pairing by looking at the more general ϕ-Weil pairing, and also offers proofs of all of its properties. Besides this, it gives a complete proof of the properties of the Tate-Lichtenbaum pairing, whereas the proof of the non-degeneracy deserves particular attention. An algorithm to compute these two pairings is then given in section VI.5. Since we need very special pairings in cryptographic applications, we introduce the notions of distortion maps and modified pairings in section VI.6, which will make the pairings more useful.

In chapter VII, we give both constructive and destructive ways to use pairings in cryptography. We start by explaining a tripartite key exchange protocol that uses only one round of communication, and discuss ways to use pairings in identity-based encryption. After that, we show how to attack the DLP on certain elliptic curves by using either the Weil or the Tate-Lichtenbaum pairing. Not surprisingly, there are elliptic curves that are more suited for pairings than others, which we will see in section VII.4.

At the end of this short summary of results, we would like to point out that all the proofs in this document are the author's own work (unless stated otherwise). Also, it should be noted that we will give complete summaries of the author's own contributions at the beginning of each chapter. Last but not least, we want to mention the appendix on Galois cohomology, which is needed to understand section II.8. This appendix has been included for the convenience of the reader.

I.3 Notations

Although, we will introduce each notation, when we first make use of it, we want to list some standard notations in the following table.

Symbol	Meaning
$\|M\|$	number of elements in the set M. Equals ∞, if M is infinite
k	usually denotes a perfect (or finite) field
k^*	multiplicative group of the field k
K	usually denotes a fixed algebraic closure of k
μ_m	group of m-th roots of unity in K
l	usually denotes an intermediate field between k and K
$\mathbb{F}_q$	finite field with q elements, where q is some prime power p^a
$\mathrm{char}(k)$	characteristic of the field k
$N_{l/k}$	norm map of the finite field extension l/k
$\mathrm{Tr}_{l/k}$	trace map of the finite field extension l/k
$G_{l/k}$	Galois group of the field extension l/k
$G_{K/l} \cdot P$	Galois orbit of the point P on some variety
$\mathrm{tr}_k(l)$	transcendence degree of the field extension l/k
$\mathrm{Stab}_G(x)$	stabilizer group of an element x in the group G
$\langle a_1, \ldots, a_r \rangle$	group generated by $a_1, \ldots, a_r$
$\mathrm{Spec}(R)$	spectrum of the ring R
$\mathrm{Max}(R)$	set of all maximal ideals of the ring R
$\mathrm{Reg}(R)$	regular locus of the ring R
$\mathrm{Quot}(R)$	field of fractions of the integral domain R
$(x_1, \ldots, x_m)$	usually an m-tupel, sometimes the ideal generated by $x_1, \ldots, x_m$
$\mathrm{ht}(I)$	height of the prime ideal I
$R_{\mathfrak{p}}$	localization at the prime ideal $\mathfrak{p}$ of the ring R
$\sqrt{I}$	radical of the ideal I
$\dim(R)$	Krull dimension of the integral domain R
$\dim(V)$	("Zariski") dimension of the algebraic set V
$\mathcal{O}_P$	local ring of the point P on the variety V
$\mathbb{P}_{F/k}$	set of places of the function field F/k
$\mathfrak{O}_P$	discr. val. ring of function field F/k corresponding to $P \in \mathbb{P}_{F/k}$
v_P	discr. val. of function field F/k corresponding to $P \in \mathbb{P}_{F/k}$
F_P	the residue class field of the place $P \in \mathbb{P}_{F/k}$
$\mathfrak{p}_\infty$	infinite place of a rational function field
$\mathfrak{O}_S$	holomorphy ring for the subset $\emptyset \neq S \subsetneq \mathbb{P}_{F/k}$
$E[\phi]$	kernel of the isogeny $\phi : E \to E'$ on elliptic curves E, E'
$[m]x$	$x + \cdots + x$ (m-times), where x is an element of some group

Chapter II

Algebraic Curves

This chapter gives the necessary background on algebraic geometry in order to understand the main elements of this thesis, namely *curves*, geometrically. It intends to give a slightly general, but short introduction to "classical" algebraic geometry (over non-algebraically closed ground fields), emphasizing on affine geometry as this is more intuitive than the projective case. The main results are about the relations between algebraic curves and algebraic function fields, which allow us to use the theory of algebraic functions in one variable to study nonsingular projective curves. Since there seems to be a gap in the literature concerning the relationships between algebraic curves and function fields over *non*-algebraically closed fields, this chapter tries to fill this void.

We will start in sections II.1-II.3 with the basic notions in affine geometry, while proceeding very quickly to the most important question (II.2) of this chapter, concerning a possible one-to-one correspondence between curves and function fields. As it turns out, we have to introduce some results about projective varieties in sections II.4-II.6, in order to answer question (II.2) in section II.7. After that, we want to consider algebraic curves over extensions of the ground field in section II.8. To this end, we will need some results from Galois cohomology, which we have summarized in appendix A for the convenience of the reader.

Although, all the proofs given in this chapter originate from the author's own work (unless stated otherwise), we would like to draw the reader's attention to the following highlights/author's own contributions:

- Proofs of many topological results that are missing/unproved in [Har77]. See example II.1.4, lemmas II.3.2, II.3.8, II.5.3 and II.7.11, and proposition II.1.14.
- A very intuitive introduction to morphisms of affine algebraic sets in section II.2. Here, the highlights include new proofs of the properties of morphisms in proposition II.2.3 and, most importantly, theorem II.2.5.
- Proof that a variety V is absolutely irreducible if and only if the ground field is algebraically closed in the function field of V (see proposition II.6.6).
- Adaptation of certain proofs in [Har77] to work over non-algebraically closed fields (see corollary II.7.8, lemma II.7.7, and propositions II.6.5 and II.7.14), resulting

in corollary II.7.18, which basically says that nonsingular projective curves and function fields are the "same" (in a certain sense).

- Proofs of two results on rational points that seem to be missing in the literature. See propositions II.8.1 and II.8.3.

At this point, we should make clear that this chapter assumes the reader to have met "classical" algebraic geometry over algebraically closed ground fields before. And we would like to refer the reader to the books [AM69, Har77, Kun85, Mat80, ZS75, ZS76], since these form the basis of this text.

Throughout, we consider a fixed field k, which is required to be perfect. Also, we fix an algebraic closure K of k.

II.1 Affine Varieties

In this section, we want to introduce the most basic definitions of "affine geometry" and explain a first relation between algebraic curves and algebraic function fields. We start with the basic notion of an *affine algebraic set* and regard some of its properties. For this, let $n \in \mathbb{N}$ be a positive integer.

Definition II.1.1. The *n-dimensional affine space (over k)* is defined as

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

By its *k-rational points* we mean the set

$$\mathbb{A}^n(k) := \{P = (x_1, \ldots, x_n) \in \mathbb{A}^n \mid \text{ all } x_i \in k\}.$$

Now, for a subset $U \subseteq k[X_1, \ldots, X_n]$ we call

$$V_U := V_I := \{P \in \mathbb{A}^n \mid f(P) = 0 \text{ for all } f \in I\}$$

an *affine algebraic set (over k)* where $I := (U)$ is the ideal of $k[X_1, \ldots, X_n]$ generated by the elements of U. For a subset $E \subseteq \mathbb{A}^n$ the set

$$I(E/k) := \{f \in k[X_1, \ldots, X_n] \mid f(P) = 0 \text{ for all } P \in E\}$$

is called *the ideal of E (over k)*. One easily verifies that $I(E/k)$ is indeed an ideal of $k[X_1, \ldots, X_n]$. Sometimes, we simply write $I(E)$ instead of $I(E/k)$ if the context is clear.

One of the most important theorems about the ideal of an affine algebraic set is *Hilbert's Nullstellensatz*:

Theorem II.1.2. Let $V = V_I$ be an affine algebraic set defined by an ideal $I \subseteq k[X_1, \ldots, X_n]$. Then:

$$I(V) = \sqrt{I}, \text{ the radical of } I.$$

Proof. See [ZS76, Ch. VII, Theorem 14, p. 164]. □

Corollary II.1.3. The map $V \mapsto I(V)$ defines a one-to-one correspondence between the set of all algebraic sets V and the set of all radical ideals $I \subseteq k[X_1, \ldots, X_n]$.

Proof. This is [Kun85, Ch. I, proposition 3.7, p. 18]. □

Recall the topological notion of "irreducibility": A subset V of a topological space T is called *irreducible*, if $V = T_1 \cup T_2$, for some closed sets $T_1, T_2 \subseteq T$, implies that $V = T_1$ or $V = T_2$. The empty set is *reducible* by convention.

Example II.1.4. Let V be an infinite topological space such that the closed sets are defined as the finite subsets of V, including $\emptyset$ and V itself (this defines a topology on V!). Then, V is irreducible.

Proof. Let $V = T_1 \cup T_2$ for some closed sets $T_1, T_2 \subseteq V$. If one of these is empty or the whole space, we are done. Otherwise, they are both finite sets. But V is infinite which is a contradiction. □

By considering the affine algebraic subsets of $\mathbb{A}^n$ as *closed sets*, $\mathbb{A}^n$ becomes a topological space. The topology is called *the Zariski topology.* This method indeed defines a topology because of (3) and (5) of the following proposition.

Proposition II.1.5. Let I, J and I_i (i lies in some set of indices) be ideals of $k[X_1, \ldots, X_n]$ and let V, V_i be subsets of $\mathbb{A}^n$. Then:

1. $I \subseteq J \Rightarrow V_J \subseteq V_I$.
2. $V \subseteq W \Rightarrow I(W) \subseteq I(V)$.
3. $V_{\sum_i I_i} = \bigcap_i V_{I_i}$.
4. $I\left(\bigcup_i V_i\right) = \bigcap_i I(V_i)$.
5. $V_{I \cap J} = V_{IJ} = V_I \cup V_J$.
6. $V \subseteq V_{I(V)}$.
7. $I \subseteq I(V_I)$.
8. $V_{I(V)} = V \iff V$ is an affine algebraic set.
9. $I(V_I) = I \iff I = I(W)$ for some $W \subseteq \mathbb{A}^n$.
10. $\sqrt{I(V)} = I(V)$.

Proof. All relations are self-evident, except (3), (5), (8) and (9) which are proved in [ZS76, Ch. VII, p. 160]. □

An affine algebraic set V is called an *affine variety* if it is irreducible in the Zariski topology. There is a very useful characterization of this:

Lemma II.1.6. An algebraic set V (over k) is irreducible if and only if $I(V/k)$ is a prime ideal of $k[X_1, \ldots, X_n]$.

Proof. Cf. [ZS76, Ch. VII, Theorem 12, p. 162]. □

Remark II.1.7. It is well-known that the extension of a prime ideal of $k[X_1, \ldots, X_n]$ to $K[X_1, \ldots, X_n]$ does not have to be prime anymore (cf. [AM69, Ch. 1, p. 10]). So it makes sense to give affine varieties V with the property that the extension of $I(V/k)$ is prime in $K[X_1, \ldots, X_n]$ a special name: An affine variety V (defined over k) is called *absolutely irreducible*, if it is irreducible as a closed set with respect to the Zariski topology of the corresponding spaces over K. In fact, we have the following obvious relation:

An affine variety V (over K) is *defined over* k (i.e. given by polynomials in $k[X_1, \ldots, X_n]$) if and only if $I(V/K) = I(V/k) \cdot K[X_1, \ldots, X_n]$.

Obviously, a variety (over K) that is defined over k, is the same as a variety (over k). In this case, we denote the fact that V is defined over k by V/k.

Remark II.1.8. The proof of lemma II.1.6 can be done exactly in the same way for closed sets in the affine space over K. This yields:

An affine variety V (over k) is absolutely irreducible if and only if the extension $I(V/K)$ of $I(V/k)$ to $K[X_1, \ldots, X_n]$ is prime.

Remark II.1.9. Having the notion of a variety, corollary II.1.3 tells us that affine varieties correspond to prime ideals and points correspond to maximal ideals.

Now we define *the affine coordinate ring (over k)* of an affine algebraic set V by

$$k[V] := \frac{k[X_1, \ldots, X_n]}{I(V/k)}.$$

If V is a variety then $I(V)$ is a prime ideal, i.e. $k[V]$ is an integral domain. In this case, we define $k(V) := \mathrm{Quot}(k[V])$ as *the function field of V (over k)*.

We now come to the most important varieties in the context of this text: *curves*. But before we are able to define these objects, we need the concept of dimension. Let V be an affine algebraic set. By the *dimension* of V, we mean

$$\dim(V) := \sup\{r \mid S_0 \supsetneqq S_1 \supsetneqq \cdots \supsetneqq S_r \text{ chain of irred. closed subsets of } V\}.$$

An affine variety of dimension 1 is called an affine *curve*.

The next few results are necessary to explain the relation between affine curves and *algebraic function fields F/k of transcendence degree 1*, i.e. field extensions $F \supseteq k$ such that F is a finite extension of $k(x)$ for some element $x \in F$, which is transcendental over k.

First of all, we need *Noether's normalization theorem*:

Theorem II.1.10. Let k be an arbitrary field and A an integral domain which is a finitely generated k-algebra. Then:

$$\dim(A) = \mathrm{tr}_k(\mathrm{Quot}(A)),$$

where $\dim(A)$ means the *Krull dimension* of the ring A and $\mathrm{tr}_k(\mathrm{Quot}(A))$ the transcendence degree of the field extension $\mathrm{Quot}(A)/k$.

Proof. See [Mat80, Ch. 5, §14.G, Corollary 1, p. 91]. □

The next result gives a relation of this to affine algebraic sets:

Lemma II.1.11. Let V be an affine algebraic set. Then:

$$\dim(V) = \dim(k[V]).$$

Proof. This is [Har77, Ch. I, Proposition 1.7, p. 6]. There, the ground field k is algebraically closed but the proof is the same for any field. □

Therefore, we have for an affine variety V:

$$\dim(V) = \dim(k[V]) = \mathrm{tr}_k(k(V)). \tag{II.1}$$

This equality is the key ingredient for the following proposition:

Proposition II.1.12. Let $n \in \mathbb{Z}_{>0}$.

1. If $V \subseteq \mathbb{A}^n$ is an affine variety, then $k(V)/k$ is a field extension of k generated by n elements with $\mathrm{tr}_k(k(V)) = \dim(V)$.
2. If F/k is a field extension of k generated by n elements, then it exists an affine variety $V \subseteq \mathbb{A}^n$ with $\dim(V) = \mathrm{tr}_k(F)$ and $F \cong k(V)$.

Proof. We prove the following lemma:

Lemma II.1.13. Let B be a k-algebra and $n \in \mathbb{Z}_{>0}$. Then the following are equivalent:

1. $B \cong k[V]$ for some algebraic set $V \subseteq \mathbb{A}^n$.
2. B is reduced and generated by n elements.

Proof. Let $\emptyset \neq V \subseteq \mathbb{A}^n$ be an affine algebraic set with $k[V] \cong B$. The kernel of the restriction of the natural map $k[X_1, \ldots, X_n] \twoheadrightarrow k[V]$ to k is precisely $k \cap I(V) = \{0\}$, i.e. $k \subseteq k[V]$ (w.r.t. this monomorphism). Together with the fact that k and $k[V]$ are commutative, we see that $k[V] \cong B$ is a finitely generated k-algebra (generated by n elements). If $\bar{f}^m = \bar{0}$ for some $m \in \mathbb{N}$ and $\bar{f} \in k[V]$, then $f^m \in I(V)$, i.e.

$$f \in \sqrt{I(V)} = I(V)$$

by using Proposition II.1.5(10). This in turn means that $\bar{f} = \bar{0}$, i.e. $k[V] \cong B$ is reduced.

Conversely, let B be reduced and generated by n elements. By definition, we have an epimorphism $\phi : k[X_1, \ldots, X_n] \twoheadrightarrow B$. Then, $V := V_I \subseteq \mathbb{A}^n$ is an affine algebraic set, where $I := \ker \phi$. But $I(V) = \sqrt{I}$ by theorem II.1.2 which in turn equals I since B is reduced. So

$$k[V] = \frac{k[X_1, \ldots, X_n]}{I} \cong B.$$

□

Now, let $V \subseteq \mathbb{A}^n$ be an affine variety. By the lemma, $k[V]$ is generated by n elements and is an integral domain, i.e. $k(V)/k$ is generated by n elements with $\mathrm{tr}_k(k(V)) = \dim(V)$ by (II.1).

Conversely, let F/k be a field extension generated by $t_1, \ldots, t_n$. Then $B := k[t_1, \ldots, t_n]$ is a finitely generated reduced k-subalgebra of F (it is reduced because it is an integral domain). We are done by using the lemma and II.1. □

The following question arises immediately:

Are there any restrictions we can apply to V such that proposition II.1.12 becomes a one-to-one correspondence? (II.2)

To answer this question we need some machinery that will be introduced in the sequel of this chapter.

At the end of this section we want to prove a very important result on the Zariski topology and give a further proposition on the dimension of an affine coordinate ring:

Proposition II.1.14. 1. Every descending chain of closed subsets of an affine algebraic set $V \subseteq \mathbb{A}^n$ eventually becomes constant, i.e. V is *Noetherian*.

2. Every Noetherian topological space V is compact. In particular, every affine algebraic set $V \subseteq \mathbb{A}^n$ is compact (in the Zariski topology).

Proof. 1. Let $V_1 \supseteq V_2 \supseteq \cdots$ be a descending chain of closed subsets of V (with respect to the induced topology). Then $I(V_1) \subseteq I(V_2) \subseteq \cdots$ is an ascending chain of ideals in $k[X_1, \ldots, X_n]$ by proposition II.1.5(2). This chain becomes constant since $k[X_1, \ldots, X_n]$ is Noetherian by Hilbert's basis theorem (e.g. [Bos04, Kap. 3.9, Satz 2, p. 131]). Therefore, $V_1 \supseteq V_2 \supseteq \cdots$ becomes constant because if $I(V_i) = I(V_j)$, then $V_i = V_j$.

2. Let $V = \bigcup_{i \in I} U_i$ be an open covering of V where I is some set of indices. Choose an $i_0 \in I$. If $U_{i_0} \neq V$ (otherwise we are done), then it exists $i_1 \in I$ such that $U_{i_0} \subsetneqq U_{i_0} \cup U_{i_1}$. If $U_{i_0} \cup U_{i_1} \neq V$ (otherwise we are done), then it exists $i_2 \in I$ such that $U_{i_0} \subsetneqq U_{i_0} \cup U_{i_1} \subsetneqq U_{i_0} \cup U_{i_1} \cup U_{i_2}$. This process either stops at some point or it gives us a strictly ascending chain of open subsets of V, which becomes constant since V is Noetherian.

□

Proposition II.1.15. Let A be a finitely generated k-algebra, which is an integral domain. Then we have for a prime ideal $\mathfrak{a} \subseteq A$:

$$\mathrm{ht}(\mathfrak{a}) + \dim(A/\mathfrak{a}) = \dim(A).$$

Proof. See [Mat80, Ch. 5, §14.H, Corollary 3, p. 92]. □

II.2 Morphisms of Affine Algebraic Sets

We want to relate affine algebraic sets with respect to their Zariski topologies in terms of continuous mappings. Such mappings will be called morphisms and will have the property that two algebraic sets are "isomorphic" if and only if their corresponding coordinate rings are "isomorphic" (cf. theorem II.2.5). So it seems to be a good idea to investigate the elements of the coordinate ring of an algebraic set in more detail, than we did before.

Let $V \subseteq \mathbb{A}^n$ be an affine algebraic set (over k), $\phi \in k[V]$ and $f \in k[X_1, \ldots, X_n]$ with $\bar{f} = \phi$, where $\bar{f}$ denotes the residue class of f modulo $I(V)$. We define the map

$$\pi_\phi : V \to \mathbb{A}^1 \text{ by } P \mapsto f(P). \tag{II.3}$$

It is well-defined, as for $g \in k[X_1, \ldots, X_n]$ with $\bar{g} = \phi = \bar{f}$ we have $f - g \in I(V)$, i.e. $f(P) = g(P)$ for all $P \in V$.

Now, let $m \in \mathbb{N}$. We call a map

$$\psi : V \to \mathbb{A}^m \text{ with } P \mapsto (\pi_{\phi_1}(P), \ldots, \pi_{\phi_m}(P)) \text{ for } \phi_i \in k[V]$$

a *morphism from V to $\mathbb{A}^m$ (over k).* If $W \subseteq \mathbb{A}^m$ is another algebraic set (over k) and the image of ψ is contained in W, then we call ψ a *morphism from V to W (over k).* The set of all such morphisms is denoted by $\mathrm{Mor}_k(V, W)$. Clearly, $\mathrm{Mor}_k(V, \mathbb{A}^1)$ becomes a k-algebra by adding and multiplying values. In this case, we have a k-algebra isomorphism $\mathrm{Mor}_k(V, \mathbb{A}^1) \cong k[V]$ given by $\psi = \pi_\phi \mapsto \phi$ which allows us to write $\phi(P)$ when we actually mean $\pi_\phi(P)$ and vice versa. Also, we can identify $\phi \in k[V]$ with one of its defining elements $f \in k[X_1, \ldots, X_n]$ because of (II.3).

A morphism $\psi : V \to W$ of affine algebraic sets induces a homomorphism of k-algebras

$$\psi^* : k[W] \to k[V] \text{ given by } f \mapsto f\psi := f \circ \psi,$$

which is called *the coordinate-pullback of ψ*. The proof of this is straightforward.

The next step is to prove the continuity of a morphism that we mentioned above. For this, we need the help of the following lemma:

Lemma II.2.1. For an affine algebraic set $V \subseteq \mathbb{A}^n$ we have the following order-preserving one-to-one correspondence

$$\{\text{ideals of } k[V]\} \overset{1:1}{\longleftrightarrow} \{\text{ideals of } k[X_1, \ldots, X_n] \text{ containing } I(V)\}$$

given by the canonical map $\zeta_V : k[X_1, \ldots, X_n] \twoheadrightarrow k[V]$. In particular, this means that $k[V]$ is Noetherian.

Under this bijection, radical, prime and maximal ideals correspond to radical, prime and maximal ideals, respectively.

Proof. The proof is very easy and can be found in [AM69, Ch. 1, Proposition 1.1, p. 2]. □

Let $Z \subseteq V \subseteq \mathbb{A}^n$ be a closed subset of an affine algebraic set V with respect to the induced topology, i.e. $Z = V_{I(Z)} \cap V = V_{I(Z)}$ since Z is also closed in $\mathbb{A}^n$. We define

$$I_V(Z) := \{\phi \in k[V] \mid \phi(P) = 0 \text{ for all } P \in Z\}.$$

By definition we have $I_V(Z) = \zeta_V(I(Z))$ and by theorem II.1.2 and lemma II.2.1, it is a radical ideal of $k[V]$.

On the other hand, we define for an ideal $\mathfrak{a} \subseteq k[V]$

$$V_{\mathfrak{a}}(V) := \{P \in V \mid \phi(P) = 0 \text{ for any } \phi \in \mathfrak{a}\}.$$

It is easy to see that $V_{\mathfrak{a}}(V) = V_{\zeta_V^{-1}(\mathfrak{a})}$, i.e. $Z := V_{\mathfrak{a}}(V)$ is a closed subset of V. If $\mathfrak{a}$ is radical, then we further have $I(Z) = \zeta_V^{-1}(\mathfrak{a})$, again by theorem II.1.2 and lemma II.2.1. We have shown:

Lemma II.2.2. For a closed subset $V \subseteq \mathbb{A}^n$ we have an order-reversing one-to-one correspondence

$$\{\text{closed subsets } Z \subseteq V\} \overset{1:1}{\longleftrightarrow} \{\text{radical ideals } \mathfrak{a} \subseteq k[V]\}$$

given by the map $Z \mapsto I_V(Z)$. Furthermore, we have:

$$\text{A closed subset } Z \subseteq V \text{ is irreducible } \iff I_V(Z) \text{ is a prime ideal of } k[V].$$

Proposition II.2.3. Let $\psi : V \to W$ be a morphism of two algebraic set $V \subseteq \mathbb{A}^n$ and $W \subseteq \mathbb{A}^m$. Then:

1. ψ is continuous with respect to the Zariski topologies on each algebraic set.
2. ψ maps closed sets to closed sets.
3. ψ maps varieties to varieties.

Proof. 1. Suppose $Z \subseteq W$ is a closed subset, i.e. $Z = V_{\mathfrak{a}}(W)$ for some radical ideal $\mathfrak{a} \subseteq k[W]$ (by the previous lemma). For $P \in V$ we have

$$P \in \psi^{-1}(Z) \iff \psi(P) \in Z \iff \psi^*(f)(P) = 0 \text{ for all } f \in \mathfrak{a},$$

which implies that $\psi^{-1}(Z) = V_{\{\psi^*(f)\}_{f \in \mathfrak{a}}}(V)$ is closed in V by what we have done above.

2. For an arbitrary subset $E \subseteq W$ we can define the ideal $I_W(E)$ and prove that it conincides with $\zeta(I(E))$, exactly as we did in the proof of the previous lemma. So for a closed subset $Z \subseteq V$ we have:

$$I_W(\psi(Z)) = \zeta_W(I(\psi(Z))).$$

But $I(\psi(Z))$ is a radical ideal by proposition II.1.5(10), and so $I_W(\psi(Z))$ must be too, by lemma II.2.1. This, however, means that $\psi(Z)$ is a closed subset of W by lemma II.2.2.

3. The following will give us another proof of part (2). For any closed subset $Z \subseteq V$ we can show by a direct (and very easy) calculation that

$$I_W(\psi(Z)) = (\psi^*)^{-1}(I_V(Z)). \tag{II.4}$$

Since $I_V(Z)$ is a radical by lemma II.2.2, $I_W(\psi(Z))$ is also a radical (cf. [AM69, Ch. 1, p. 10]), and $\psi(Z)$ is closed in W (which is (2)). If Z is irreducible, then $I_V(Z)$ is a prime ideal of $k[V]$ by lemma II.2.2, and so $I_W(\psi(Z))$ is a prime ideal by (II.4), which implies that $\psi(Z)$ is irreducible.

□

We say that a morphism $\psi : V \to W$ between two algebraic sets (over k) is an *isomorphism (over k)*, if it exists a morphism $\eta : W \to V$ such that $\psi\eta = \mathrm{id}_W$ and $\eta\psi = \mathrm{id}_V$. In this case, V and W are called *isomorphic (over k)*. Before we characterize isomorphic algebraic sets, we should say something about the *closure* of a subset $W \subseteq \mathbb{A}^m$:

Lemma II.2.4. The closure of a subset $W \subseteq \mathbb{A}^m$ in $\mathbb{A}^m$ with respect to the Zariski topology (denoted by $\overline{W}$) is $V_{I(W)}$.

Proof. Let $V = V_I \subseteq \mathbb{A}^m$ be an affine algebraic set containing W (for some ideal $I \subseteq k[X_1, \ldots, X_m]$). We have $I \subseteq I(V) \subseteq I(W)$, which in turn means $V_{I(W)} \subseteq V_{I(V)} \subseteq V_I = V$. So $V_{I(W)}$ is the smallest algebraic set containing W. □

Theorem II.2.5. Let $\psi : V \to W$ be a morphism of affine algebraic sets $V \subseteq \mathbb{A}^n$ and $W \subseteq \mathbb{A}^m$. Then:

1. ψ^* is injective $\iff \overline{\psi(V)} = W$ (i.e. $\psi(V)$ is dense in W).

2. ψ^* is surjective $\implies \psi$ is injective.

3. ψ^* is an isomorphism $\iff \psi$ is an isomorphism.

Proof. 1. Assume that ψ^* is injective and that $\psi(V)$ is *not* dense in W, i.e. $Z := \overline{\psi(V)} \subsetneq W$ is a proper closed subset of W containing $\psi(V)$. So it exists an $f \in k[W]$ such that $Z \subseteq V_f(W) \subsetneq W$, which implies $\psi^*(f) = f\psi = 0$ as $\psi(V) \subseteq Z$. But ψ^* is injective, so $f = 0$, which is a contradiction to $V_f(W) \subsetneq W$.

Conversely, let $\overline{\psi(V)} = W$ and let $f \in k[W]$ such that $\psi^*(f) = 0$. The latter implies that $\psi(V) \subseteq V_f(W)$, which in turn means $V \subseteq \psi^{-1}(V_f(W)) \subseteq V$, hence they are equal. Since $\psi(V)$ is dense in W and $V_f(W)$ is closed we have $W = \overline{\psi(V)} \subseteq V_f(W) \subseteq W$, which is only possible if $f = 0$ by definition. So ψ^* is injective.

2. Suppose that ψ^* is surjective and let $X_1, \ldots, X_n$ denote the variables in $\mathbb{A}^n$. Clearly, $X_i \in \mathrm{Mor}_k(V, \mathbb{A}^1) \cong k[V]$, so it exists an element $g_i \in k[W]$ such that $\psi^*(g_i) = X_i$ for every $i \in \{1, \ldots, n\}$. For $P, Q \in V$ with $\psi(P) = \psi(Q)$ we therefore have:

$$P = (g_1(\psi(P)), \ldots, g_n(\psi(P))) = (g_1(\psi(Q)), \ldots, g_n(\psi(Q))) = Q.$$

This means that ψ is injective.

3. Suppose that ψ^* is an isomorphism. By (1) together with proposition II.2.3(2) we see that ψ is surjective and by (2) it is also injective. As in the proof of (2) we let $X_1, \ldots, X_n$ denote the variables in $\mathbb{A}^n$ and consider the elements $g_i \in k[W]$ with $X_i = \psi^*(g_i)$ for every $i \in \{1, \ldots, n\}$. Then, we define $\eta := (g_1, \ldots, g_n) \in \mathrm{Mor}_k(W, \mathbb{A}^n)$ and put $\varphi := (\psi^*)^{-1}$. If $f \in I(V)$ and $Q = (y_1, \ldots, y_m) \in W$, then we have:

$$f(\eta(Q)) = f(\varphi(X_1)(Q), \ldots, \varphi(X_n)(Q)) = \varphi(f(X_1, \ldots, X_n))(Q) = 0,$$

since $f \in I(V)$ and φ is a k-algebra homomorphism. This means that η is in fact an element of $\mathrm{Mor}_k(W, V)$. We know that ψ is bijective, so it exists a unique $P \in V$ with $\psi(P) = Q$. This yields

$$\psi(\eta(Q)) = \psi(g_1(\psi(P)), \ldots, g_n(\psi(P))) = \psi(P) = Q.$$

On the other hand, we have for an arbitrary $P = (x_1, \ldots, x_n) \in V$, which corresponds to a unique $Q \in W$ as ψ is bijective:

$$\eta(\psi(P)) = \eta(Q) = P$$

by the same calculation we did before. So ψ is an isomorphism.

Conversely, let ψ be an isomorphism. In particular this means that ψ is bijective and (1) shows that ψ^* is injective. On the other hand, we know that it exists a morphism $\varphi : W \to V$ such that $\varphi\psi = \mathrm{id}_V$ and $\psi\varphi = \mathrm{id}_W$. Let $f \in k[V]$ and put $g := f \circ \varphi = \varphi^*(f) \in k[W]$. We then have for every $P \in V$:

$$\psi^*(g)(P) = f(\varphi(\psi(P))) = f(P),$$

which simply means $\psi^*(g) = f$ by definition, i.e. ψ^* is surjective.

□

Remark II.2.6. In situation (1) of the above theorem we call ψ a *dominant* morphism and in situation (2) it is called an *embedding of V into W* (because in this case, $\psi : V \to \psi(V)$ is an isomorphism).

To illustrate the notion of morphisms, we give an example which is crucial for cryptographic applications.

Example II.2.7. Suppose that $\mathrm{char}(k) = p > 0$. The mapping $\phi_p : k \to k$ with $x \mapsto x^p$ is an injective endomorphism, which is proved in [Lan02, Ch. IV, §2, p. 179]. Since k is assumed to be perfect, ϕ_p is even surjective, i.e. an automorphism. It is called *the (absolute) Frobenius automorphism of k*. Indeed, if ϕ_p would not be surjective, then it would exist $a \in k$ such that $g := X^p - a \in k[X]$ is a polynomial with no roots in k. But, $g = (X-b)^p$ for some element b of the splitting field of g, which is a contradiction to separability.

Now, ϕ_p induces an injective morphism from $\mathbb{A}^n$ to itself which is also denoted by ϕ_p:

$$\phi_p : \mathbb{A}^n \to \mathbb{A}^n, \phi_p := (X_1^p, \ldots, X_n^p).$$

The restriction to an affine algebraic set $V \subseteq \mathbb{A}^n$ is, by the previous theorem, a bijective morphism from V to $\phi_p(V)$, called *the Frobenius morphism of V*, again denoted by ϕ_p, i.e. $\phi_p \in \mathrm{Mor}_k(V, \phi_p(V))$. We note without proof that ϕ_p is bijective and bicontinuous but *not* an isomorphism.

II.3 Rational Maps of Affine Varieties

Let V be an affine variety (over k) and let $\phi = \overline{f} \in k[V]$ for some $f \in k[X_1, \ldots, X_n]$. To shorten our usual notation, we write

$$V_\phi := V_\phi(V) \text{ and } U_\phi := V \setminus V_\phi.$$

The following equivalences are immediate by definition:

$$V_\phi = V \iff U_\phi = \emptyset \iff f \in I(V).$$

So, for $f \notin I(V)$ (i.e. $\phi \neq 0$) it makes sense to define

$$\frac{1}{\phi}(P) := f(P)^{-1} \in K \text{ for all } P \in U_\phi.$$

Such a map is called "rational" and we define the more general case as follows:

Definition II.3.1. Let $\emptyset \neq U \subseteq V$ be open in V. A map

$$r_U : U \to \mathbb{A}^1, \quad P \mapsto \left(\frac{\psi}{\phi}\right)(P) \text{ for } \psi, \phi \in k[V] \text{ with } U \subseteq U_\phi$$

is called a *rational map from V to $\mathbb{A}^1$ (over k)* with *definition set U*.

We need the following topological result:

Lemma II.3.2. If U is a nonempty open subset of an irreducible topological space V, then U is dense in V.

Proof. Since $U \subseteq \overline{U}$, we have

$$V = \overline{U} \cup (V \setminus \overline{U}) \subseteq \overline{U} \cup (V \setminus U) \subseteq V,$$

i.e. all inclusions are equalities. But V is irreducible which implies

$$V = \overline{U} \text{ or } V = V \setminus U$$

as $V \setminus U$ is closed in V. The latter cannot be true since U is nonempty. □

With the help of this lemma we can prove the following *identity theorem*:

Proposition II.3.3. Let U, U' be nonempty open subsets of the affine variety V and let r_U and $r'_{U'}$ be rational maps from V to $\mathbb{A}^1$. Then:

$$\text{If } r_U = r'_{U'} \text{ on some open subset } W \subseteq U \cap U' \Longrightarrow r_U = r'_{U'} \text{ on } U \cap U'.$$

Proof. This is the above lemma together with [Kun85, Ch. III, proposition 2.5, p. 68]. □

This proposition allows us to define an equivalence relation on rational maps:

$$r_U \sim r'_{U'} :\Longleftrightarrow r_U = r'_{U'} \text{ on } U \cap U'.$$

Indeed, "$\sim$" is reflexive and symmetric by definition, and it is transitive by the above proposition.

Definition II.3.4. The equivalence class of a rational map from V to $\mathbb{A}^1$ with respect to $\sim$ is called a *rational function on V (over k)*. The set of all rational functions on V (denoted by $\mathcal{R}(V)$), becomes a field by adding and multiplying values.

We state the following result which gives a nice describtion of rational function:

Proposition II.3.5. We have a field isomorphism: $\mathcal{R}(V) \cong k(V)$.

Proof. See [Kun85, Ch. III, proposition 2.10, p. 69]. □

This explains why $k(V)$ is sometimes called *the field of rational functions on V*. Note that a rational function $f \in k(V)$ is not necessarily a "function" on the whole of V as we usually understand it, since it is not always defined on every point $P \in V$. Therefore, we define the following:

Definition II.3.6. Let $f \in \mathcal{R}(V)$ be a rational function. If f has a representative $\tilde{f}$ with definition set U containing a point $P \in V$, then we call f *regular at P*.

We denote the set of all rational functions that are regular on some open set $U \subseteq V$ by $\mathcal{O}_V(U)$ (or $\mathcal{O}(U)$ if there is no ambiguity).

In this case, $\tilde{f}|_U = \frac{\psi}{\phi}$ on U for some $\psi, \phi \in k[V]$ with $P \in U \subseteq U_\phi$. So we can define

$$f(P) := \frac{\psi(P)}{\phi(P)}$$

and say that f *is defined at* P.

Similarly to the case of morphisms, we extend the notion of rational maps to the general case:

Definition II.3.7. Let $V \subseteq \mathbb{A}^n$ and $W \subseteq \mathbb{A}^m$ be affine varieties (over k). For rational functions $r_1, \ldots, r_m \in \mathcal{R}(V)$ with representatives $R_1, \ldots, R_m$ (with respect to $\sim$) defined on a nonempty open set $U \subseteq V$ such that $R(U) := (R_1(U), \ldots, R_m(U)) \subseteq W$, we call the m-tuple $r := (r_1, \ldots, r_m)$ a *rational map from* V *to* W *(over* k*)* and denote this situation by the symbol

$$r : V \dashrightarrow W.$$

If $R(U)$ is dense in W then r is called *dominant*.

It is not clear, why there exists a nonempty open set U with $R_1, \ldots, R_m$ defined on it, as used in the definition above. This follows from the following topological result:

Lemma II.3.8. If $U_1, \ldots, U_m$ are nonempty open subsets of an irreducible topological space V, then $\bigcap_{i=1}^m U_i$ is nonempty and open in V.

Proof. Assume that the intersection of the U_i is empty, so $V = \bigcup_{i=1}^m V \setminus U_i$ by one of De Morgan's laws. Now the irreducibility of V implies that $V = V \setminus U_i$ for some $i \in \{1, \ldots, m\}$. This means that $U_i = \emptyset$, which is a contradiction. The rest of the lemma is true by the definition of a topology. □

Let $r = (r_1, \ldots, r_m) : V \dashrightarrow W$ and $r' = (r'_1, \ldots, r'_p) : W \dashrightarrow Z \subseteq \mathbb{A}^p$ be dominant rational maps given by $R_1, \ldots, R_m$ on $U \subseteq V$, respectively $R'_1, \ldots, R'_p$ on $U' \subseteq W$. Because r is dominant, we see that $R^{-1}(U') \subseteq U$ is a nonempty open subset. Now, $R'_1 \circ R, \ldots, R'_p \circ R$ are rational maps defined on the nonempty open set $\tilde{U} := R^{-1}(U') \cap U$ with $R'(\tilde{U}) \subseteq Z$. They form a rational map from V to Z, which we define as the *composition* $r' \circ r$. Since r' is assumed to be dominant, one immediately sees that this is also true for $r' \circ r$.

Definition II.3.9. Let r be as in definition II.3.7.

1. We call r *birational*, if it is dominant and it exists a dominant rational map $r' : W \dashrightarrow V$ such that

   $$r' \circ r \sim \mathrm{id}_V \text{ and } r \circ r' \sim \mathrm{id}_W.$$

   In this case, V are W are said to be *birationally equivalent*.

2. We call r *regular at a point* $P \in V$, if it exists a nonempty open subset U of V containing P such that $r|_U$ is given by an m-tuple of rational maps defined on U.

Again, it makes sense to say that r *is defined at* P in case (2) of the definition, and we define

$$r(P) := (r_1(P), \ldots, r_m(P)).$$

A dominant rational map r from V to W induces a homomorphism of k-algebras

$$r^* : k[W] \longrightarrow k(V) \text{ given by } \phi = \overline{f} \mapsto f \circ r \text{ with } f \in k[X_1, \ldots, X_n].$$

This map is defined since $k(V)$ is a field and r is given by elements $r_1, \ldots, r_m \in k(V)$, i.e. $f \circ r$ is a rational function on V again. It is well-defined, for when $f, g \in k[X_1, \ldots, X_n]$ with $\overline{f} = \overline{g} = \phi$ we have $f - g \in I(W)$, which implies that $f \circ r = g \circ r$ (as rational maps in the sense of definition II.3.1) for some nonempty open subset $U \subseteq V$ by definition, i.e. $f \circ r = g \circ r$ (as rational functions). The fact that r^* is a homomorphism of k-algebras is trivial.

If $0 = r^*(\phi) = f \circ r$ then $f \circ r = 0$ (as rational maps in the sense of definition II.3.1) for some nonempty open subset $U \subseteq V$, i.e. $f \in I(R(U))$ with the notation of definition II.3.7. So $\phi = 0$ on $R(U)$. But ϕ is a morphism and so $\phi^{-1}(\{0\})$ is a closed subset of W by proposition II.2.3, which contains $R(U)$. Due to our assumption on the density of $R(U)$ we see that $\phi = 0 \in k[W]$. This means that r^* is an injective homomorphism, and the embedding can be extended to the field of fractions of $k[W]$:

$$r^* : k(W) \longrightarrow k(V), \frac{\phi}{\psi} = \frac{\overline{f}}{\overline{g}} \mapsto \frac{f \circ r}{g \circ r} \text{ with } f, g \in k[X_1, \ldots, X_n].$$

We have shown that r^* is a monomorphism of k-algebras. We call it the *function-pullback of* r (or the *dual of* r).

For two dominant rational maps $r : V \dashrightarrow W$ and $r' : W \dashrightarrow Z$ we have:

$$(r' \circ r)^* \left(\frac{\phi}{\psi}\right) = \frac{f \circ r' \circ r}{g \circ r' \circ r} = r^* \left(\frac{f \circ r'}{g \circ r'}\right) = (r^* \circ r'^*) \left(\frac{\phi}{\psi}\right), \text{ i.e.}$$

$$(r' \circ r)^* = r^* \circ r'^*. \tag{II.5}$$

Finally, we can prove the main result of this section.

Theorem II.3.10. If $r : V \dashrightarrow W$ is a dominant rational map of varieties (over k), then:

$$r \text{ is birational} \iff r^* \text{ is an isomorphism.}$$

Proof. The proof is very similiar to the one of theorem II.2.5. By considering the coordinate functions $X_1, \ldots, X_n$ we can establish a one-to-one correspondence

$$\{\text{rational map } r : V \dashrightarrow W\} \overset{1:1}{\longleftrightarrow} \{k\text{-algebra homom. } \psi : k(W) \to k(V)\}$$

via $r \mapsto r^*$. The rest follows easily because of (II.5). □

II.4 Projective Varieties

There are several reasons why it is useful to consider the so called *projective geometry*. One of them is, for instance, to be able to grasp the "well-known" phenomenon that two affine lines (algebraic sets given by linear equations) intersect at "infinity" (cf. [Kun85, Ch. I, proposition 5.2, p. 30]). As in the affine case, we want to define the *n-dimensional projective space (over k)*

$$\mathbb{P}^n := \mathbb{P}^n(K) := \{P = (y_0 : \cdots : y_n) \mid y_i \in K, \text{ at least one } y_i \text{ is nonzero}\},$$

where $(y_0 : \cdots : y_n)$ denotes the equivalence class of the following equivalence relation:

$$(y_0 : \cdots : y_n) \sim (z_0 : \cdots : z_n) : \iff \exists \lambda \in K \text{ such that } \forall i : y_i = \lambda z_i.$$

By its *k-rational points* we mean the set

$$\mathbb{P}^n(k) := \{P = (y_0 : \cdots : y_n) \in \mathbb{P}^n \mid \exists \lambda \in K \text{ such that } \forall i : \lambda y_i \in k\}.$$

Recall that a polynomial $F \in k[Y_0, \ldots, Y_n]$ is called *homogeneous of degree d*, if it is the sum of monomials of the same degree d, which is equivalent to saying that

$$F(\lambda Y_0, \ldots, \lambda Y_n) = \lambda^d F(Y_0, \ldots, Y_n) \text{ for all } \lambda \in K.$$

In particular, it makes sense to speak of a *zero* $P = (y_0 : \cdots : y_n) \in \mathbb{P}^n$ of a homogeneous polynomial F of degree d:

$$F(P) = 0 : \iff F(y_0, \ldots, y_n) = 0.$$

This expression is well-defined. An ideal $I \subseteq k[Y_0, \ldots, Y_n]$ is *homogeneous*, if it is generated by homogeneous polynomials. Now, for a homogeneous ideal $I \subseteq k[Y_0, \ldots, Y_n]$, we call

$$V_I := \{P \in \mathbb{P}^n \mid F(P) = 0 \text{ for all } F \in I\}$$

a *projective algebraic set (over k)*. For such an algebraic set V, we define $I(V/k)$ as the homogeneous ideal of $k[Y_0, \ldots, Y_n]$ generated by

$$\{F \in k[Y_0, \ldots, Y_n] \mid F \text{ is homogeneous and } F(P) = 0 \text{ for all } P \in V\},$$

called the *(homogeneous) ideal of V (over k)*. Sometimes, we write $I(V)$ instead of $I(V/k)$, if the context is clear.

Similarly to the affine case, we have the *projective Nullstellensatz*:

Theorem II.4.1. The map $V \mapsto I(V)$ induces an inclusion-reversing one-to-one correspondence between the set of all projective algebraic sets V and the set of all homogeneous radical ideals $I \subseteq k[Y_0, \ldots, Y_n]$ that are contained in $(Y_0, \ldots, Y_n)$. The inverse mapping is given by the formation of the zero set. Furthermore, for any homogeneous

ideal $I \neq k[Y_0, \ldots, Y_n]$ we have

$$I(V_I) = \sqrt{I}.$$

Projective varieties correspond to homogeneous prime ideals and projective points correspond to homogeneous maximal ideals.

Proof. This is [Kun85, Ch. I, proposition 5.9, p. 34]. □

One gets a natural topology on $\mathbb{P}^n$, again called the *Zariski topology* (over k), by considering the projective algebraic sets as closed. A projective algebraic set is called a *projective variety*, if it is irreducible in the Zariski topology. Proposition II.1.5 and lemma II.1.6 can easily be proven in the projective case. The *dimension* and the *coordinate ring* of a projective algebraic set are defined as in the affine case. But these are not the only relations there are between the projective and the affine geometry. We want to establish one with respect to polynomials:

Let $f \in k[X_1, \ldots, X_n]$ be of degree d. We define its *homogenization with respect to* Y_i (for an $i \in \{0, \ldots, n\}$) by

$$f_i^* := Y_i^d f(\frac{Y_0}{Y_i}, \ldots, \frac{Y_{i-1}}{Y_i}, \frac{Y_{i+1}}{Y_i}, \ldots, \frac{Y_n}{Y_i}).$$

This is clearly a homogeneous polynomial of degree d in $k[Y_0, \ldots, Y_n]$.

Conversely, let $F \in k[Y_0, \ldots, Y_n]$ be homogeneous of degree d. We define its *dehomogenization with respect to* Y_i by

$$F_*^i := F(X_1, \ldots, X_i, 1, X_{i+1}, \ldots, X_n).$$

This is clearly a polynomial in $k[X_1, \ldots, X_n]$.

It is immediately seen that those two processes are inverses of each other. Put $H_i := V_{(Y_i)}$ and consider the open sets $U_i := \mathbb{P}^n \setminus H_i$ for every $i = 0, \ldots, n$. The homogenization process induces the map

$$\varphi_i : U_i \to \mathbb{A}^n, (y_0 : \ldots : y_n) \mapsto (\frac{y_0}{y_i}, \ldots, \frac{y_{i-1}}{y_i}, \frac{y_{i+1}}{y_i}, \ldots, \frac{y_n}{y_i}). \tag{II.6}$$

Proposition II.4.2. φ_i is a homeomorphism of U_i (with its induced topology) to $\mathbb{A}^n$ (with its Zariski topology). Its inverse map is denoted by ϕ_i and is explicitly given by

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

Proof. The proof can be found in [Har77, Ch. I, proposition 2.2, p. 10]. There, the ground field k is algebraically closed, but this restriction is not needed in the proof. □

Since the sets $U_0, \ldots, U_n$ are sort of natural and cover the whole projective space $\mathbb{P}^n$, we call the covering *standard*. Furthermore, we denote $\varphi_i(V \cap U_i)$ by V_i for a projective closed set V (we often simply write $V \cap \mathbb{A}^n$ for V_i and a fixed i in mind). It is a closed affine set and its ideal consists of all dehomogenized elements (with respect to Y_i) of the ideal of V. Conversely, let V_I be an affine closed set. We can then speak of the

projective closure $\overline{V_I}$ *of* V_I as the closed projective set defined by the ideal $\overline{I}$ genereated by $\{f_i^* \mid f \in I\}$ for a fixed embedding ϕ_i of V_I into $\mathbb{P}^n$.

Proposition II.4.3. 1. If V is an affine variety, then $\overline{V}$ is a projective variety with

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

2. If V is a projective variety, then $V \cap \mathbb{A}^n$ is an affine variety and

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

There is at least one i such that $V \cap U_i$ is nonempty. We call it a *nonempty affine part of* V and denote it by V_a (with a fixed i in mind).

Proof. This is [Sil86, Ch. I, proposition 2.6, p. 13]. □

Let V be a projective variety and let $V_a \in \mathbb{A}^n$ be a nonempty affine part of V. We define

$$k(V) := k(V_a) \tag{II.7}$$

as *the function field of* V *(over* k*).* By proposition II.4.3(2) we have that $\overline{V_a} = V$ and the following proposition tells us that $k(V)$ is well-defined.

Proposition II.4.4. Let $\overline{V}$ be the projective closure of a nonempty affine variety V. Then there is a k-algebra isomorphism $k(V) \cong k(\overline{V})$. In particular, $k(\overline{V})$ is a finitely generated extension field of k of transcendence degree $\dim(\overline{V}) = \dim(V)$.

Proof. See [Kun85, Ch. III, proposition 2.13, p. 70]. □

The last part of this proposition turns out to be quite useful, in the case where V is given by a principal prime ideal, as we have the following criterion for V to be absolutely irreducible (cf. proposition II.1.12):

Proposition II.4.5. 1. If $V = V_f$ is an affine algebraic set, given by $f \in k[X_1, \ldots, X_n]$, then:

$$V \text{ is absolutely irreducible} \iff k \text{ is algebraically closed in } k(V).$$

2. If $V = V_F$ is a projective algebraic set, given by a homogeneous polynomial $F \in k[Y_0, \ldots, Y_n]$, then:

$$V \text{ is absolutely irreducible} \iff k \text{ is algebraically closed in } k(V).$$

Proof. 1. By remark II.1.8 and the fact that $I(V/K)$ is just $f \cdot K[X_1, \ldots, X_n]$ we have:

$$V \text{ is absolutely irreducible} \iff f \text{ is } \textit{absolutely irreducible},$$

i.e. irreducible over K. The proposition then is simply [Sti93, Ch. III, Corollary 6.7, p. 108].

2. Similarly to (1). Note that remark II.1.8 obviously holds in the projective case as well. □

Our next aim is to generalize the notions of morphisms, rational maps and regular maps of affine algebraic sets to projective algebraic sets.

Definition II.4.6. Let φ_i be the map defined in (II.6) with inverse $\varphi_i^{-1} = \phi_i$ for every $i = 0, \ldots, n$. We call the map $r^{ij} := \varphi_j \circ \phi_i : \mathbb{A}^n \to \mathbb{A}^n$ the (i,j)-*transition map*. Its inverse is r^{ji}.

Definition II.4.7. Let $V \subseteq \mathbb{P}^n$ and $W \subseteq \mathbb{P}^m$ be projective algebraic sets. Let $\psi : V \to W$ be a mapping such that

1. $V = \bigcup_{i=1}^n V_i$ where V_i are the affine parts of V.
2. $\psi_i := \psi|_{V_i}$ is an affine morphism of V_i to an affine part W_i of W (say $\psi_i = (f_1^i, \ldots, f_m^i)$ for $f_k^i \in k[V_i]$ for every affine part V_i).
3. $r^{ij}(f_1^i(P), \ldots, f_m^i(P)) = (f_1^j(P), \ldots, f_m^j(P)) \in W_j$.

Then ψ is called *a (projective) morphism from V to W (over k)*. The set of all such morphisms is denoted by $\mathrm{Mor}_k(V, W)$.

Example II.4.8. By the above definition of projective morphisms it is immediate that the homeomorphism φ_i defined in (II.6) is in fact an isomorphism in the sense of definition II.4.7. Consider the following result on the dimension of a projective variety V:

Proposition II.4.9. Let $V \subseteq \mathbb{P}^n$ be a projective variety and let $V_a \subseteq \mathbb{A}^n$ be a nonempty affine part of V. Then:

$$\dim V = \dim V_a.$$

Proof. This is [Kun85, Ch. II, proposition 4.1, p. 59]. □

Clearly, $\mathbb{A}^n$ is a nonempty affine part of $\mathbb{P}^n$ and so

$$\dim \mathbb{P}^n = \dim \mathbb{A}^n = \dim(k[X_1, \ldots, X_n]) = \mathrm{tr}_k(k(X_1, \ldots, X_n)) = n$$

by proposition II.2.3 together with (II.1). So $\mathbb{P}^n$ has dimension n.

A *(projective) rational map* from a projective variety $V \subseteq \mathbb{P}^n$ to $\mathbb{A}^1$ is defined as the equivalence class of a rational map defined on the affine parts of V compatible with the transition maps on intersections of standard affine pieces U_i. The generalization to rational maps that map to projective varieties is then done in the same way as in section II.3. A rational map from V to $\mathbb{P}^1$ is called a *rational function of V*.

Let $P \in \mathbb{P}^n$ be a point, V a projective variety and V_i an affine part of it containing P. A rational map r from V to $W \subseteq \mathbb{P}^m$ is called *regular at P*, if there exists an open neighborhood U of P in V_i such that $r|_{V_i}$ is defined on U.

With those definitions, it is easy to see that versions of the results in sections II.2 and II.3 also hold in the projective case. We refer to [Kun85] for details and would like to note that our definition of morphisms (in the affine and in the projective case) is equivalent to the following (see [Kun85]):

Definition II.4.10. Let V and W be two nonempty affine or projective algebraic sets. A mapping $\psi : V \to W$ is called a *morphism (over k)*, if it is continuous (in the Zariski topology) and if for every open subset $U \subseteq W$ with $\psi^{-1}(U) \neq \emptyset$ we have: if $f \in \mathcal{O}_W(U)$ then $f \circ \psi \in \mathcal{O}_V(\psi^{-1}(U))$.

We already proved that this definition follows from our definition. The other direction is not much harder. Also, we can see that our definition of rational maps is equivalent to the following:

Definition II.4.11. A *rational map* $\psi : V \to W$ (over k) between two varieties V, W is an equivalence class of pairs (U, ψ_U) where U is a nonempty open subset of V, ψ_U is a morphism of U to W and where (U, ψ_U) and $(U', \psi_{U'})$ are *equivalent*, if ψ_U and $\psi_{U'}$ agree on $U \cap U'$.

Clearly, the notion of dominance is then the same as to say that the image of ψ_U is dense in W.

II.5 Nonsingular Varieties

Let V be an affine or projective variety and $W \subseteq V$ a nonempty irreducible subset (not necessarily closed). The set of all open subsets $U \subseteq V$ with $U \cap W \neq \emptyset$ is denoted by $\mathcal{U}(W)$. Lemma II.3.8 together with the fact that W is irreducible, yield that if $U_1, U_2 \in \mathcal{U}(W)$, then $U_1 \cap U_2 \in \mathcal{U}(W)$.

Definition II.5.1. Let $U_1, U_2 \in \mathcal{U}(W)$ and $r_1 \in \mathcal{O}(U_1), r_2 \in \mathcal{O}(U_2)$. r_1 and r_2 are called *equivalent in W*, if $r_1|_U = r_2|_U$ for some $U \in \mathcal{U}(W)$ with $U \subseteq U_1 \cap U_2$.

This defines an equivalence relation on $\bigcup_{U \in \mathcal{U}(W)} \mathcal{O}(U)$ by the note above the definition, and we denote the set of all equivalence classes with respect to this relation by $\mathcal{O}_{V,W}$. Since constant functions are regular, we have an inclusion $k \hookrightarrow \mathcal{O}_{V,W}$. Addition and multiplication on $\mathcal{O}_{V,W}$ can be defined by adding and multiplying the representatives.

Proposition II.5.2. $\mathcal{O}_{V,W}$ is a local k-algebra with maximal ideal $\mathfrak{m}_{V,W} := \{\rho = \overline{r} \in \mathcal{O}_{V,W} \mid r \text{ vanishes on some nonempty open subset of } W\}$.

Proof. See [Kun85, Ch. III, remark 2.15, p. 71]. □

We are interested in the special case, where W consists of a single point P. In this case, we simply write $\mathcal{O}_P$ resp. $\mathfrak{m}_P$ instead of $\mathcal{O}_{V,\{P\}}$ resp. $\mathfrak{m}_{V,\{P\}}$ and call it the *local ring of P on V*. $\mathcal{O}_P/\mathfrak{m}_P$ is then called the *residue field of P*. By [Kun85, Ch. III, p. 71] we have for an affine variety V and its projective closure $\overline{V}$ that $\mathcal{O}_{V,W} \cong \mathcal{O}_{\overline{V},W}$, which

implies that we do not have to treat the affine and projective cases separately and can simply work in affine geometry. Also, $\mathcal{O}_{V,W} \cong \mathcal{O}_{V_a,W}$ for all nonempty affine part V_a of a projective variety V. It should be noted that we have a k-algebra monomorphism $\mathcal{O}_{V,W} \hookrightarrow k(V)$ by assigning to an element $\rho \in \mathcal{O}_{V,W}$ the uniquely determined rational function that represents it.

If V is an affine variety and $W \subseteq V$ a nonempty irreducible subset, then $\mathfrak{p}_W := I_V(\overline{W})$ is a prime ideal of $k[V]$ by lemma II.2.2 and the following result:

Lemma II.5.3. If $W \subseteq V$ is a nonempty irreducible subset of a topological space V, then its closure (in V) $\overline{W}$ is also irreducible.

Proof. Let $\overline{W} = T_1 \cup T_2$, where T_1, T_2 are closed subsets of $\overline{W}$ (so closed in V), then $S_i := T_i \cap W$ is closed in W for $i = 1, 2$ by definition of the induced topology. But $W = \overline{W} \cap W = S_1 \cup S_2$, so by irreducibility of W we have $W = S_1$ or $W = S_2$. This implies that $\overline{W} = \overline{T_1 \cap W} \subseteq T_1 \subseteq \overline{W}$ or $\overline{W} = \overline{T_2 \cap W} \subseteq T_2 \subseteq \overline{W}$ by definition, i.e. $\overline{W} = T_1$ or $\overline{W} = T_2$. □

Proposition II.5.4. Let $W \subseteq V$ be a nonempty irreducible subset of an affine variety V. Then:

$$\mathcal{O}_{V,W} \cong k[V]_{\mathfrak{p}_W} \text{ (as } k\text{-algebras)},$$

where $k[V]_{\mathfrak{p}_W}$ denotes the localization of $k[V]$ at the prime ideal $\mathfrak{p}_W$.

Proof. This is [Kun85, Ch. III, proposition 3.6, p. 77]. The isomorphism is induced by the k-algebra homomorphism

$$j : k[V] \longrightarrow \mathcal{O}_{V,W} \text{ with } \phi \mapsto \overline{\phi}.$$

□

In particular, the last result means

1. $\mathcal{O}_P \cong k[V]_{\mathfrak{p}_P}$, where $\mathfrak{p}_P = \{\phi \in k[V] \mid \phi(P) = 0\}$.
2. $\mathcal{O}_V := \mathcal{O}_{V,V} \cong k(V)$, since $\mathfrak{p}_V = I_V(V) = \zeta_V(I(V)) = (0)$ for the canonical map $\zeta_V : k[X_1, \ldots, X_n] \twoheadrightarrow k[V]$.

Definition II.5.5. Let $P \in V$ be a point on a projective (or affine) variety V. P is called a *nonsingular point* if the local ring $\mathcal{O}_P$ of P on V is integrally closed in $k(V)$. Otherwise, it is called a *singular point*. The variety V is called *nonsingular* (or *smooth*), if all of its points $P \in V$ are nonsingular.

From this point onwards, we concentrate on curves. Recall the following result from commutative algebra:

Proposition II.5.6. Let A be a Noetherian local domain of (Krull) dimension 1 with maximal ideal $\mathfrak{m}$, $k := A/\mathfrak{m}$. The following are equivalent:

1. A is a discrete valuation ring.

2. A is integrally closed.

3. $\mathfrak{m}$ is a principal ideal.

4. $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$ (in this case, A is called *regular*).

5. Every non-zero ideal is a power of $\mathfrak{m}$.

6. There exists $x \in A$ such that every non-zero ideal is of the form $(x^l), l \geq 0$.

Proof. This is [AM69, Ch. 9, proposition 9.2, p. 94]. □

Remark II.5.7. $\mathfrak{m}^2 \subseteq \mathfrak{m}$ are certainly A-modules, since they are ideals in A and therefore, $M := \mathfrak{m}/\mathfrak{m}^2$ is also an A-module. We know that the *annihilator* of M, denoted by $\mathrm{Ann}(M)$, is an ideal of A. Now, for $x \in \mathfrak{m} \subseteq A$ and $\overline{m} \in M$ with $m \in \mathfrak{m}$ we have:

$$xm \in \mathfrak{m}^2 \Rightarrow x\overline{m} = \overline{xm} = 0 \Rightarrow x\overline{m} \in \mathrm{Ann}(M), \text{ i.e. } \mathfrak{m} \subseteq \mathrm{Ann}(M).$$

If $\overline{x} \in k = A/\mathfrak{m}$ is represented by $x \in A$, we define for $m \in M$: $\overline{x}m := xm \in M$. This definition is independent of the choice of the representative x of $\overline{x}$, since $\mathfrak{m}M = 0$. So, M can be regarded as a k-vector space.

Let C be a projective curve and $P \in C$ a point on C. We already know from lemma II.2.1 that $k[C]$ is a Noetherian integral domain (and so is $k[C]_{\mathfrak{p}_P}$, e.g. by [AM69, Ch. 7, corollary 7.4, p.80]) and by lemma II.1.11 we have $1 = \dim C = \dim k[C]$. Now, since $k[Y_0, \ldots, Y_n]$ is a finitely generated k-algebra, $k[C]$ is one too. Then, by proposition II.1.15 we have: $\mathrm{ht}(\mathfrak{p}_P) = \dim k[C] - \dim k[C]/\mathfrak{p}_P$ but $\dim k[C]/\mathfrak{p}_P = \mathrm{tr}_k(\mathrm{Quot}(k[C]/\mathfrak{p}_P)) \leq \mathrm{tr}_k K = 0$ by theorem II.1.10 (note that $\ker(k[C] \to K, \phi \mapsto \phi(P)) = \mathfrak{p}_P$) and has therefore dimension 0, i.e. $\mathrm{ht}(\mathfrak{p}_P) = 1$. This means, by the following lemma, that $\dim k[C]_{\mathfrak{p}_P} = 1$.

Lemma II.5.8. If $\mathfrak{m}$ is a prime ideal of a ring A, the prime ideals of the local ring $A_{\mathfrak{m}}$ are in one-to-one correspondence with the prime ideals of A contained in $\mathfrak{m}$.

In particular, $\mathrm{ht}(\mathfrak{m}) = \dim A_{\mathfrak{m}}$.

Proof. See [AM69, Ch. 3, corollary 3.13, p. 42]. □

We have seen: $\mathcal{O}_P$ is a Noetherian local domain of dimension 1. Now, proposition II.5.6 tells us that P is a nonsingular point if and only if $\mathcal{O}_P$ is regular, i.e. a discrete valuation ring. The above fact that $\dim k[C]/\mathfrak{p}_P = 0$ can be proved alternatively with the following lemma which shows that $\mathfrak{p}_P$ is a maximal ideal.

Lemma II.5.9. Let $P \in C$ be a point on an affine curve C. The map $P \mapsto \mathfrak{p}_P$ gives a one-to-one correspondence between the points of C and the maximal ideals of $k[C]$.

Proof. By lemma II.1.9 we have a 1-1 correspondence between the points P of C and the maximal ideals of $k[X_1, \ldots, X_n]$ containing $I(C)$. Passing to the quotient by $I(C)$, these correspond to the maximal ideals of $k[C]$, which are therefore $\mathfrak{p}_P = I(\{P\})/I(C)$ since $I(\{P\}) = \{f \in k[X_1, \ldots, X_n] \mid f(P) = 0\}$ (cf. lemma II.2.1). □

Our next aim is to prove a very useful characterization for a point P on a curve C to be nonsingular. For this, we need some definitions.

Definition II.5.10. Let A be a Noetherian ring. We define

1. $\mathrm{Spec}(A) := \{\mathfrak{p} \subseteq A \mid \mathfrak{p} \text{ is a prime ideal of } A\}$ as its *spectrum*.
2. $\mathrm{Reg}(A) := \{\mathfrak{p} \in \mathrm{Spec}(A) \mid A_{\mathfrak{p}} \text{ is a regular local ring}\}$ as its *regular locus*.

In particular, if $A = k[C]$ for some affine curve C, we have seen:

$$\text{A point } P \in C \text{ is nonsingular} \iff \mathfrak{p}_P \in \mathrm{Reg}(k[C]). \tag{II.8}$$

Let C be an affine curve with $I(C) = (f_1, \ldots, f_m) \subseteq k[X_1, \ldots, X_n]$ and let $\mathfrak{p} \in \mathrm{Spec}(k[C])$. Then, $k[C]_{\mathfrak{p}}/\mathfrak{p}k[C]_{\mathfrak{p}} \cong \mathrm{Quot}(k[C]/\mathfrak{p}) \cong k(\xi_1, \ldots, \xi_n)$ where ξ_i is the image of X_i in $k[C]_{\mathfrak{p}}/\mathfrak{p}k[C]_{\mathfrak{p}}$ (e.g. by [AM69, Ch. 3, corollary 3.4, p.39]).

Definition II.5.11. The matrix

$$J(\mathfrak{p}) := \frac{\partial(f_1, \ldots, f_m)}{\partial(\xi_1, \ldots, \xi_n)} = \left(\frac{\partial f_i}{\partial X_k}(\xi_1, \ldots, \xi_n)\right)_{i=1,\ldots,m, k=1,\ldots,n}$$

is called the *Jacobian matrix at* $\mathfrak{p}$.

Now we can state the *Jacobian criterion*.

Theorem II.5.12. Let $P \in C$ be a point on a curve C, where C_a is a nonempty affine part of C with $P \in C_a$. Then:

$$P \text{ is nonsingular} \iff \mathfrak{p}_P \in \mathrm{Reg}(k[C_a]) \iff \mathrm{rank}(J(\mathfrak{p}_P)) = n - 1.$$

Proof. This is [Kun85, Ch. VI, theorem 1.15, p. 171] together with (II.8). □

An easy consequence is the following result:

Corollary II.5.13. The set of smooth points of an affine (or projective) curve C is nonempty and open. Furthermore, C has only finitely many *singularities* (i.e. singular points).

Proof. See [Kun85, Ch. VI, corollary 1.17, p. 173]. □

Example II.5.14. Let $C = \mathbb{P}^1$ be the *projective line*. We want to show that C is an absolutely irreducible nonsingular projective curve. First of all, $C = V_{(0)}$ and by theorem II.4.1 we even have $I(C) = \sqrt{(0)} = (0)$ since (0) is a homogeneous prime ideal of $k[Y_0, Y_1]$. This in turn means that C is absolutely irreducible, as (0) is also a homogeneous prime ideal in $K[Y_0, Y_1]$. Together with example II.4.8 we have shown that C is an absolutely irreducible projective curve and it remains to show that it is nonsingular. Now, by using (II.6) we see that $\mathbb{P}^1 = \mathbb{A}^1 \cup (0:1)$, in our usual notation, where $\mathbb{A}^1$ is isomorphic to U_0. As we have shown above, it is enough to consider one of the nonempty affine parts of C, i.e. $\mathbb{A}^1 = V_{(0)}$. Since all derivatives of 0 are 0, it is

trivial that the Jacobian matrix $J(\mathfrak{p}_P)$ at every point $P \in \mathbb{A}^1$ has rank 0 which means that C is nonsingular by theorem II.5.12.

This example leads us immediately to another very important example.

Example II.5.15. Let C be an absolutely irreducible nonsingular projective curve (over k). Every function $f \in k(C)$ defines a rational map (it is actually a morphism) which we also denote by f, namely

$$f : C \to \mathbb{P}^1, P \mapsto \begin{cases} (f(P) : 1), \text{ if } f \text{ is regular at } P \\ (1 : 0), \text{ if } f \text{ has a pole at } P. \end{cases} \tag{II.9}$$

But since both C and $\mathbb{P}^1$ (with defining variables X and Y) are absolutely irreducible nonsingular projective curves (cf. example II.5.14), we obtain the injective homomorphism

$$f^* : k(X) \to k(C) \text{ (cf. section II.3).}$$

At the end of this section we want to prove a result, which will become very important in section II.7.

Lemma II.5.16. Let $P, Q \in C$ be two points on a projective curve $C \subseteq \mathbb{P}^n$. If $\mathcal{O}_Q \subseteq \mathcal{O}_P$, then $P = Q$.

Proof. We have $k[C_a]_{\mathfrak{p}_Q} = \mathcal{O}_Q \subseteq \mathcal{O}_P = k[C_a]_{\mathfrak{p}_P}$, where C_a is a nonempty affine part of C, so $\mathfrak{p}_P \subseteq \mathfrak{p}_Q$. But $\mathfrak{p}_P$ and $\mathfrak{p}_Q$ are both maximal ideals in $k[C_a]$, i.e. $\mathfrak{p}_P = \mathfrak{p}_Q$. This implies that $P = Q$ in the affine sense by lemma II.5.9, which in particular means that $P = Q$ in the projective sense. □

II.6 Hypersurfaces

The aim of this section is to generalize proposition II.4.5 to arbitrary varieties. This will turn out to be crucial in answering our question (II.2) from the beginning.

Definition II.6.1. Let $f \in k[X_1, \ldots, X_n]$ be an irreducible polynomial. We call the affine variety V_f an affine *hypersurface*.

If $n = 2$, a hypersurface is simply a curve, and if $n = 3$, we call it a *surface*. The definitions in the projective case is analogous. We want to prove that any variety is birational equivalent to a hypersurface. We need some definitions and results from commutative algebra to be able to prove our aim.

Definition II.6.2. A field extension F/k is *separably generated* if there is a transcendence base $\{x_i\}$ for F/k such that F is a separable algebraic extension of $k(\{x_i\})$. Such a transcendence base is called a *separating transcendence base*.

Theorem II.6.3. If k is a perfect field, then any finitely generated field extension F/k is separably generated.

Proof. This is [ZS75, Ch. II, theorem 31, p. 105]. □

We should also recall the *theorem of the primitive element*:

Theorem II.6.4. Let F be a finite separable extension field of a field k. Then there is an element $\alpha \in F$ which generates F as an extension field of k.

Proof. See [ZS75, Ch. II, theorem 19, p. 84]. □

Proposition II.6.5. Any variety V of dimension r is birationally equivalent to a hypersurface H in $\mathbb{P}^{r+1}$.

Proof. We already know that the function field $F := k(V)$ of V is a finitely generated extension field of k (see proposition II.1.12) and since k is assumed to be perfect, F is separably generated over k by theorem II.6.3. So by definition, there exists a transcendence base $x_1, \ldots, x_r \in F$ such that F is a finite separable extension of $k(x_1, \ldots, x_r)$ (the finiteness follows from the fact that it is algebraic and finitely generated). This in turn allows us to choose an algebraic (over $k(x_1, \ldots, x_r)$) element $y \in F$ such that $F = k(x_1, \ldots, x_r, y)$ by theorem II.6.4. Since y is algebraic, there exists a monic irreducible polynomial $g \in k(x_1, \ldots, x_r)[X]$ with $g(y) = 0$. Clearing denominators, we get an irreducible polynomial $f \in k[Z_1, \ldots, Z_{r+1}]$ with $f(x_1, \ldots, x_r, y) = 0$.

Now, $H_a := V_f \subseteq \mathbb{A}^{r+1}$ is an affine hypersurface with function field $k(H_a) = \mathrm{Quot}(k[H_a]) \cong k(x_1, \ldots, x_r)/g \cong F$. By theorem II.3.10 this means that H_a is birationally equivalent to V. By the fact that the homogenization of f stays irreducible together with the definition of the function field of a projective variety, we get that $k(V)$ is isomorphic to $k(H)$, where $H := \overline{H_a}$ is the projective closure of H_a. Then, V is birationally equivalent to H again by theorem II.3.10. □

Remark II.1.8 together with proposition II.4.5 gives us the main result of this section:

Proposition II.6.6. A variety V is absolutely irreducible if and only if k is algebraically closed in $k(V)$.

From now on, we will restrict our attention to *absolutely irreducible curves* C. So we may always assume that k is algebraically closed in $k(C)$.

II.7 Abstract Nonsingular Curves

This section shall be the answer to question (II.2). After giving some basic notions and results we will define an *abstract nonsingular curve* and prove that every nonsingular projective curve is isomorphic to such an abstract nonsingular curve for a given function field of dimension 1 over k. The answer we are looking for is an easy consequence of this.

We will use the following convention:

Convention. By a *function field* F/k we always mean a function field F of transcendence degree one over k such that k is the full constant field of F. From the previous section, we know that this is no restriction for our purposes.

By a *curve* we always mean an absolutely irreducible curve.

At first, we give a summary of results from commutative algebra.

Definition II.7.1. Let $(A, \mathfrak{m}_A)$ and $(B, \mathfrak{m}_B)$ be local rings contained in a field F. If $A \subseteq B$ and $\mathfrak{m}_B \cap A = \mathfrak{m}_A$, we say that B *dominates* A.

Theorem II.7.2. Let R be a local ring contained in a field F. Then:

1. R is a valuation ring of F if and only if R is a maximal element of the set of all local rings contained in F with respect to the relation of domination.
2. R is dominated by some valuation ring of F.

Proof. See [Bou59, Ch. VI, §1, p. 3]. □

Definition II.7.3. Let A be a Noetherian domain of dimension one. A is called a *Dedekind domain*, if it is integrally closed.

Theorem II.7.4. Let A be a Noetherian domain of dimension one. Then the following are equivalent:

1. A is a Dedekind domain.
2. $A_{\mathfrak{p}}$ is a discrete valuation ring for any nonzero prime ideal $\mathfrak{p}$.

Proof. See [AM69, Ch. 9, theorem 9.3, p. 95]. □

Theorem II.7.5. The integral closure of a Dedekind domain in a finite extension field of its quotient field is again a Dedekind domain.

Proof. This is [ZS75, Ch. V, theorem 19, p. 281]. □

Theorem II.7.6. Let A be an integral domain, which is a finitely generated k-algebra and put $L := \mathrm{Quot}(A)$. If F/L is a finite field extension, then the integral closure of A in F is finitely generated as an A-module and as a k-algebra.

Proof. See [ZS75, Ch. V, theorem 9, p. 267]. □

Now, we are able to prove the first step towards our final goal, namely that every discrete valuation ring of a function field F/k is isomorphic to the local ring of a point on some nonsingular affine curve.

Lemma II.7.7. If F/k is a function field and $x \in F$, then the set

$$\{R \in C_F \mid x \notin R\}$$

is finite, where C_F denotes the set of all discrete valuation rings of F/k.

Proof. For $(R, \mathfrak{m}_R) \in C_F$ we know that $k \subseteq R$, i.e. we may assume $x \notin k$. Certainly,

$$x \notin R \iff 0 \neq y := \frac{1}{x} \in \mathfrak{m}_R,$$

which implies that $\{R \in C_F \mid x \notin R\} = \{R \in C_F \mid y \in \mathfrak{m}_R\}$. But k is assumed to be algebraically closed in F, i.e. y is transcendental over k as $y \notin k$. So by definition of a function field, F is a finite field extension of $k(y)$. Clearly, $k[y]$ is a Dedekind domain (e.g. by [AM69, Ch. 9, exm. 1, p. 96]) and so the integral closure of $k[y]$ in F, denoted by B, is a Dedekind domain by theorem II.7.5. Also, by theorem II.7.6, B is a finitely generated k-algebra. This means by lemma II.1.13 together with lemma II.1.11 that B is the affine coordinate ring of an affine curve $C \subseteq \mathbb{A}^n$ for some $n \in \mathbb{N}$ (see also proposition II.6.6). Moreover, C is nonsingular by theorem II.7.4, since $\mathcal{O}_P \cong B_{\mathfrak{p}_P}$ for every point $P \in C$.

On the other hand, $y \in \mathfrak{m}_R$, so $k[y] \subseteq R$, which implies that $B \subseteq R$, as R is integrally closed in F by theorem II.5.6. Clearly, $\mathfrak{n} := \mathfrak{m}_R \cap B \neq 0$ (as $0 \neq y \in \mathfrak{n}$) is a maximal ideal of B, as it is the contraction of a maximal ideal, so we can form $B_{\mathfrak{n}}$, the localization of B at the nonzero prime $\mathfrak{n}$.

Claim. $B_{\mathfrak{n}} = R$. In particular, $\mathrm{Quot}(B) = F$.

Proof. First of all, we have $k \subseteq B \subseteq B_{\mathfrak{n}} \subseteq \mathrm{Quot}(B) \subseteq F$ by definition and the fact that B is an integral domain. We denote the valuation corresponding to R by v_R. If $\frac{a}{b} \in B_{\mathfrak{n}}$, then $v_R(\frac{a}{b}) = v_R(a) - v_R(b) \geq 0$ as $a \in B \subseteq R$ and $b \notin n$ (i.e. $v_R(b) = 0$), showing that $B_{\mathfrak{n}} \subseteq R$. Since $\mathfrak{n}B_{\mathfrak{n}} = \mathfrak{n}_{\mathfrak{n}}$ (see [AM69, Ch. 3, p. 41]) is the unique maximal ideal of $B_{\mathfrak{n}}$, a similiar calculation yields that $\mathfrak{m}_R \cap B_{\mathfrak{n}} = \mathfrak{n}B_{\mathfrak{n}}$, i.e. R dominates $B_{\mathfrak{n}}$.

On the other hand, $B_{\mathfrak{n}}$ is a discrete valuation ring of F/k by theorem II.7.4. But this in turn means by theorem II.7.2(1) that $B_{\mathfrak{n}} = R$. □

Now, by lemma II.5.9 we can choose the unique point P on C corresponding to $\mathfrak{n}$, which means that y, regarded as an element of $k[C]$, vanishes at P.

For different $R \in C_F$ we get different points P on C (recall that C depends only on y) since $R = B_{\mathfrak{p}_P}$ for some point $P \in C$ by the above. But $y \neq 0$, so it vanishes only at a finite set of points, which means that there can only be finitely many $R \in C_F$. □

Corollary II.7.8. Any discrete valuation ring of F/k is isomorphic to the local ring at a point on some nonsingular affine curve.

Proof. Pick $R \in C_F$ and $y \in R \setminus k$. As in the proof of the previous lemma, we can construct a smooth affine curve C such that $k[C] \cong B$, where B denotes the integral closure of $k[y]$ in F. Furthermore, we have seen that it exists a point P on C with $\mathcal{O}_P \cong k[C]_{\mathfrak{p}_P} \cong R$. □

This corollary is the reason why we sometimes call the elements of C_F *points*, and write $P \in C_F$, where P actually means a discrete valuation ring $R_P \in C_F$. The following lemma tells us something about the size of C_F:

Lemma II.7.9. Let V be a nonempty affine variety. Then:

$$\dim V = 0 \iff V \text{ consists of only finitely many points.}$$

Proof. This is [Kun85, Ch. II, proposition 3.11, p. 56]. □

This means that an affine curve always consists of infinitely many points. Together with lemma II.5.16, the corollary implies that C_F is infinite. We can define a topology on C_F by taking $\emptyset$, finite sets and C_F as *closed sets*.

Definition II.7.10. Let $U \subseteq C_F$ be an open subset. We define

$$\mathcal{O}(U) := \bigcap_{P \in U} R_P$$

as *the ring of regular functions on* U. Its elements are called *regular functions*.

Indeed, $f \in \mathcal{O}(U)$ defines a function from U to $\mathbb{A}^1$ by taking $f(P)$ as f modulo $\mathfrak{m}_P$, the maximal ideal of R_P. This is an element in K since

$$R_P/\mathfrak{m}_P \cong k[C]_{\mathfrak{p}_P}/(\mathfrak{p}_P k[C]_{\mathfrak{p}_P}) \cong k[C]/\mathfrak{p}_P \cong k(\xi_1, \ldots, \xi_n),$$

where each ξ_i is the image of X_i in $k[C]_{\mathfrak{p}_P}/(\mathfrak{p}_P k[C]_{\mathfrak{p}_P})$ and is therefore algebraic over k. So we may always think of $R_P/\mathfrak{m}_P$ as embedded in K, and we have the following tower of fields:

$$k \subseteq R_P/\mathfrak{m}_P \subseteq K.$$

Some easy but important consequences can be drawn from the definitions:

Lemma II.7.11. Let F/k be a function field over k. Then:

1. C_F is an irreducible topological space.
2. C_F is Noetherian and therefore compact.
3. In the sense of section II.3, the field $\mathcal{R}(C_F)$ of rational functions of C_F is simply F itself.

Proof.

1. This is example II.1.4.
2. Let $V_1 \supseteq V_2 \supseteq \cdots$ be a descending chain of closed subsets of C_F. If $V_i = C_F$ for all i, we are done. Otherwise, it exists an i such that $V_i \subsetneq C_F$, which implies that V_j is finite for all $j \geq i$. But then it exists a $k \geq j$ such that either $V_k = \emptyset$ or $V_k = V_{k+l}$ for all $l \in \mathbb{N}$. So C_F is Noetherian and compact by proposition II.1.14(2).
3. Let $f, g \in \mathcal{O}(U)$ for some open subset $U \subseteq C_F$ with $f(P) = g(P)$ for all $P \in U$. Then, $f - g \in \mathfrak{m}_P$ for all $P \in U$. But U has infinitely many elements and so, by lemma II.7.7, $f = g$.

The rest follows easily from the fact that every $f \in F/k$ is a regular function on some open set $U \subseteq C_F$. If $f \notin k$ then $f \in \mathfrak{m}_P$ for finitely many $P \in C_F$ by lemma II.7.7 and so f is regular on the complement of the set of those points. If $f \in k$, it is regular on C_F.

□

We can now define what we mean by an *abstract nonsingular curve* and how it fits into our world of varieties.

Definition II.7.12. Let F/k be a function field. An open subset $U \subseteq C_F$, with the induced topology and the induced notion of regular functions on its open subsets, is called an *abstract nonsingular curve*.

By the remark at the end of section II.4 we are now able to include abstract nonsingular curves to our notion of morphisms between varieties as follows:

Definition II.7.13. A *morphism* $\psi : V \to W$ between abstract nonsingular curves or varieties is a continuous mapping such that for every open set $U \subseteq W$, and every regular function $f : U \to \mathbb{A}^1$, $f \circ \psi$ is a regular function on $\psi^{-1}(U)$.

Our next aim is to prove that every nonsingular projective curve is isomorphic to an abstract nonsingular curve.

Proposition II.7.14. Every nonsingular projective curve C is isomorphic to an abstract nonsingular curve.

Proof. Let $F = k(C)$ be the function field of C. We already know that for each point $P \in C$, the local ring $\mathcal{O}_P$ is a discrete valuation ring of F/k by proposition II.5.6. Let $U \subseteq C_F$ be the set of all local rings of C. We define a map $\psi : C \to U$ by $P \mapsto \mathcal{O}_P$. This map is surjective by definition and injective by lemma II.5.16. In order to show that ψ is an isomorphism, we need to show that U is an open subset of C_F (i.e. an abstract nonsingular curve).

The local ring of a projective variety is isomorphic to the local ring of one of its nonempty affine parts (cf. section II.5), so we may assume that C is affine. The coordinate ring $A := k[C]$ of C is a finitely generated k-algebra (say $A = k[x_1, \ldots, x_n]$) by lemma II.1.13, with $\mathrm{Quot}(A) = F$. By what we have done in section II.5, every local ring in U is a localization of A at its maximal ideal and therefore contains A. We have the following equivalence:

$$A \subseteq R_P \iff x_1, \ldots, x_n \in R_P.$$

This implies $U = \bigcap_{i=1}^{n} U_i$ where $U_i := \{P \in C_F \mid x_i \in R_P\}$. But $\{P \in C_F \mid x_i \notin R_P\}$ is a closed set by lemma II.7.7 and so all U_i are open, hence U is open.

ψ is certainly continuous as finite sets are closed in C. Now, let $V \subseteq C$ be an open subset, then we already know that $\mathcal{O}_C(V) = \bigcap_{P \in V} \mathcal{O}_{C,P}$. For an open subset $W \subseteq U$

we have

$$\mathcal{O}_U(W) = \bigcap_{P \in W} R_P = \bigcap_{Q \in \psi^{-1}(W)} \psi(Q) = \bigcap_{Q \in \psi^{-1}(W)} \mathcal{O}_{C,Q} = \mathcal{O}_C(\psi^{-1}(W)).$$

So regular functions on any open set are the same and we have shown that ψ is indeed an isomorphism. □

We want to prove the converse, namely that every abstract nonsingular curve is isomorphic to a nonsingular projective curve. To be able to do so, we need the following result about the unique extension of morphisms from curves to projective varieties.

Proposition II.7.15. Let C be an abstract nonsingular curve, let $P \in C$, let V be a projective variety, and let $\psi : C \setminus P \to V$ be a morphism. Then there exists a unique morphism $\overline{\psi} : C \to V$ extending ψ.

Proof. We have proved every result necessary to understand the proof given in [Har77, Ch. I, proposition 6.8, p. 43]. There, the ground field is assumed to be algebraically closed. This restriction, however, is not needed in the proof by using our vocabulary and results instead of the ones given there. □

This allows us state the main result of this section:

Theorem II.7.16. Let F/k be a function field. Then, the abstract nonsingular curve C_F is isomorphic to a nonsingular projective curve.

Proof. This is [Har77, Ch. I, theorem 6.9, p. 44]. Again, in the proof given there, it is not needed that k is algebraically closed. □

Corollary II.7.17. Every curve is birationally equivalent to a nonsingular projective curve.

Proof. Let C be a curve with function field $F = k(C)$. By the previous result, we know that C_F is a nonsingular projective curve with function field F and so, C is birationally equivalent to C_F by theorem II.3.10. □

Finally, we are able to answer our question (II.2): Proposition II.1.12 becomes a one-to-one correspondence (up to isomorphism) if we restrict ourselves to function fields of transcendence degree 1 over k (k is the full constant field of F) and absolutely irreducible nonsingular projective curves. This follows from the next result:

Corollary II.7.18. There is a one-to-one correspondence (up to isomorphism) between absolutely irreducible nonsingular projective curves C and function fields F/k of transcendence degree 1 over k such that k is the full constant field of F.

Proof. This is [Har77, Ch. I, corollary 6.12, p. 45]. Note that one only needs k to be algebraically closed in F for the proof to work. □

This allows us to work in the theory of algebraic function fields instead of the geometric theory of algebraic curves.

II.8 Base Change and the Action of Galois

In this section, we want to consider varieties over extensions of the ground field k. For this, we let $k \subseteq l \subseteq K$ be an intermediate field and write

$$G_{l/k} := \mathrm{Aut}_k(l) := \{\varphi \in \mathrm{Aut}(l) \mid \varphi(x) = x \text{ for all } x \in k\}$$

for the *Galois group* of the extension l/k (cf. chapter VI of [Lan02] for more on this topic). Similarly to k-rational points on an affine (resp. projective) algebraic set $\subseteq \mathbb{A}^n$ (resp. $\subseteq \mathbb{P}^n$), we can define

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

as the *set of l-rational points* resp. the set

$$\mathbb{P}^n(l) := \{(y_0 : \cdots : y_n) \mid \exists \lambda \in K : \forall i : \lambda y_i \in l\}.$$

It is obvious that the coordinate-wise application of elements of $G_{K/l}$ to points $P \in \mathbb{A}^n$ (resp. $\in \mathbb{P}^n$) defines an action of $G_{K/l}$ on the set of affine (resp. projective) l-rational points. Clearly, this allows us to write $\mathbb{A}^n(l)$ in terms of this action, i.e.

$$\mathbb{A}^n(l) = \{P \in \mathbb{A}^n \mid \sigma(P) = P \text{ for all } \sigma \in G_{K/l}\}.$$

This is also possible for the projective l-rational points of $\mathbb{P}^n(l)$, but it is a bit harder to see:

Proposition II.8.1.

$$\mathbb{P}^n(l) = \{P \in \mathbb{P}^n \mid \sigma(P) = P \text{ for all } \sigma \in G_{K/l}\}.$$

Proof. Let $P = (y_0 : \cdots : y_n) \in \mathbb{P}^n(l)$, i.e. it exists $\lambda \in K^*$ such that

$$P = (\lambda y_0 : \cdots : \lambda y_n) \text{ with } \lambda y_i \in l \text{ for all } i = 0, \ldots, n.$$

This immediately implies that $\sigma(P) = P$ for all $\sigma \in G_{K/l}$.

Conversely, let $P \in \mathbb{P}^n(K)$ with $\sigma(P) = P$ for all $\sigma \in G_{K/l}$, i.e.

$$\forall \sigma \in G_{K/l} \exists \lambda_\sigma \in K^* : \sigma(y_i) = \lambda_\sigma y_i \text{ for all } i = 0, \ldots, n.$$

This enables us to define a map $\xi : G_{K/l} \to K^*$ by $\sigma \mapsto \lambda_\sigma$, since there is at least one index j such that $y_j \neq 0$, which implies that $\lambda_\sigma = \frac{\sigma(y_j)}{y_j}$ is uniquely determined. Furthermore, we have for $\sigma, \tau \in G_{K/l}$:

$$\lambda_{\sigma\circ\tau} y_i = \sigma(\lambda_\tau y_i) = \sigma(\lambda_\tau)\lambda_\sigma y_i,$$

i.e. $\xi \in Z^1(G_{K/l}, K^*)$ (cf. definition A.0.7). But by Hilbert's theorem 90 (cf. proposition A.0.8), we know that $H^1(G_{K/l}, K^*)$ is trivial and so, ξ is actually a 1-coboundary

and therefore automatically continuous. On the other hand, $B^1(G_{K/l}, K^*)$ is a group and so the inverse of ξ, namely $\sigma \mapsto \lambda_\sigma^{-1}$, is also a 1-coboundary. This means that it exists $\alpha \in K^*$ such that $\lambda_\sigma^{-1} \cdot \alpha = \sigma(\alpha)$ for all $\sigma \in G_{K/l}$. In addition, we have

$$\sigma(\alpha y_i) = \lambda_\sigma^{-1} \cdot \alpha \cdot \lambda_\sigma \cdot y_i = \alpha \cdot y_i \text{ for all } \sigma \in G_{K/l}.$$

Now, with Galois theory (cf. lemma VI.2.2), this implies that $\alpha y_i \in l^*$ for all $i = 0, \ldots, n$, i.e. $P \in \mathbb{P}^n(l)$. □

Definition II.8.2. Let $P \in \mathbb{P}^n$. We define the *field of definition of* P as the smallest extension field, denoted by $k(P)$, of k such that $P \in \mathbb{P}^n(k(P))$.

For $P \in \mathbb{P}^n$, let $G_{K/l} \cdot P$ denote the set $\{\sigma(P) \mid \sigma \in G_{K/l}\}$. By the proposition, we know that $P \in \mathbb{P}^n(l)$ if and only if $G_{K/l} \cdot P = P$. This implies that

$$k(P) = \bigcap_{G_{K/l} \cdot P = P} l, \text{ where } l \text{ runs through all intermediate fields } k \subseteq l \subseteq K.$$

By the definition of the set of l-rational points on an (affine or projective) algebraic set V, it is now clear that we have

$$V(l) = \{P \in V \mid \sigma(P) = P \text{ for all } \sigma \in G_{K/l}\}.$$

Our next aim is to define the action of the Galois group on $K[V]$ for an affine variety $V \subseteq \mathbb{A}^n$ defined over l. To this end, let $\bar{f} \in K[V]$ be given by $f \in K[X_1, \ldots, X_n]$. Now, for all $\sigma \in G_{K/l}$, we define

$$\sigma(\bar{f}) := \overline{\sigma(f)},$$

where σ acts on f by acting on its coefficients. This clearly defines an action of $G_{K/l}$ on $K[V]$ since $G_{K/l}$ takes $I(V) = I(V/K)$ to itself. Furthermore, if $P \in V$, we have

$$\sigma(\bar{f})(\sigma(P)) = \overline{\sigma(f)}(\sigma(P)) = \sigma(f)(\sigma(P)) = \sigma(f(P)) = \sigma(\bar{f}(P)),$$

since we defined $\bar{f}(P)$ as $f(P)$ (cf. (II.3)).

Since $K(V)$ is defined as the quotient field of $K[V]$, the action on $K[V]$ naturally extends to $K(V)$ as follows: If $f = \frac{g}{h} \in K(V)$, we define

$$\sigma(f) := \frac{\sigma(g)}{\sigma(h)} \in K(V).$$

One easily verifies that this indeed defines an action of $G_{K/l}$ on $K(V)$.

Proposition II.8.3. If V/l is an affine variety defined over l, then

$$l[V] = \{\bar{f} \in K[V] \mid \sigma(\bar{f}) = \bar{f} \text{ for all } \sigma \in G_{K/l}\}$$

and consequently,

$$l(V) = \{\varphi \in K(V) \mid \sigma(\varphi) = \varphi \text{ for all } \sigma \in G_{K/l}\}.$$

Proof. If $\bar{f} \in l[V](\hookrightarrow K[V])$ then $\sigma(\bar{f}) = \overline{\sigma(f)} = \bar{f}$ as the coefficients of f all lie in l.

Conversely, let $\bar{f} \in K[V]$ with $\sigma(\bar{f}) = \bar{f}$ for all $\sigma \in G_{K/l}$. By example A.0.5(2), we know that $I(V)$ is a $G_{K/l}$-module and since $\sigma(f) - f \in I(V)$, we can define a map

$$\xi : G_{K/l} \to I(V) \text{ by } \sigma \mapsto \sigma(f) - f.$$

Now, the argumentation is exactly the same as in the proof of proposition II.8.1. Firstly, we prove that ξ is a 1-cocycle. We have

$$\sigma(\tau(f)) - f = \sigma(\tau(f)) - \sigma(f) + \sigma(f) - f = \sigma(\tau(f) - f) + (\sigma(f) - f)$$

which already means that $\xi \in Z^1(G_{K/l}, I(V))$. Now by proposition A.0.8(2) this means that ξ is a 1-coboundary and so the inverse of xi, namely $\sigma \mapsto f - \sigma(f)$, is also a 1-coboundary, i.e. it exists $g \in I(V)$ such that

$$\sigma(f + g) = f + g \text{ for all } \sigma \in G_{K/l}.$$

With Galois theory, it follows that $f + g \in l[X_1, \ldots, X_n]$, i.e. $\bar{f} = \overline{f + g}$ has a representative in $l[X_1, \ldots, X_n]$, so $\bar{f} \in l[V](\hookrightarrow K[V])$. □

Since the function field of a projective variety $V \subseteq \mathbb{P}^n$ defined over l is defined via a nonempty affine part V_a (cf. definition II.7), the proposition states in this case:

$$l(V) = \{\varphi \in K(V) \mid \sigma(\varphi) = \varphi \text{ for all } \sigma \in G_{K/l}\}.$$

Let $C/k \subseteq \mathbb{A}^n$ be an absolutely irreducible nonsingular affine curve defined over k given by some polynomials $f_1, \ldots, f_r \in k[X_1, \ldots, X_n]$. We want to define what is usually meant by a *base change* from k to l.

First of all, it is obvious that C regarded in the Zariski topology over l is a closed set (this holds also for non-absolutely irreducible curves). Now, since C is absolutely irreducible, we know that the ideal of C in $k[X_1, \ldots, X_n]$, $I(C/k) = (f_1, \ldots, f_r) \cdot k[X_1, \ldots, X_n]$, is prime and that its extension $I(C/k) \cdot l[X_1, \ldots, X_n]$ to $l[X_1, \ldots, X_n]$ is also prime (cf. remark II.1.8). But C is defined over k, which means that $I(C/l) = I(C/k) \cdot l[X_1, \ldots, X_n]$, since $I(C/k) = I(V/l) \cap k[X_1, \ldots, X_n]$. This implies that

$$l[C] = k[C] \cdot l, \text{ and immediately implies } l(C) = k(C) \cdot l. \tag{II.10}$$

Let $C/k \subseteq \mathbb{P}^n$ be an absolutely irreducible nonsingular projective curve defined over k given by some homogenous polynomials $F_1, \ldots, F_r \in k[Y_0, \ldots, Y_n]$. Since C is absolutely irreducible, we know that the ideal $I(C/k) = (F_1, \ldots, F_r)$ of C is prime and that its extension to $l[Y_0, \ldots, Y_n]$ is also prime (cf. remark II.1.8). By proposition II.4.3 we

know that a nonempty affine part C_a of C is also absolutely irreducible, which implies

$$l(C) = l(C_a) = k(C_a) \cdot l = k(C) \cdot l \tag{II.11}$$

by (II.10).

The process of regarding the (affine or projective) curve C/k over the field extension l is called a *base change from k to l* and we denote the curve regarded over l by $C \cdot l$.

Chapter III

Function Fields

The purpose of this chapter is to recall important definitions and results from the theory of algebraic function fields of one variable. To this end, we begin in section III.1 by giving the most basic definitions, such as of places and divisors. We will always try to define things in terms of the curves that are associated to a given function field (cf. chapter II). Very quickly, we will come to the very momentous Riemann-Roch theorem in section III.2, which is of fundamental importance in the sequel of this thesis. Similarly to the base change we may perform on algebraic curves (see section II.8 of the previous chapter), we want to discuss algebraic extensions of function fields in section III.3. From this, we can prove an interesting result that relates the points on a given curve to the places of the associated function field in section III.4 (the proof is the author's own work, see proposition III.4.1). After this short introduction, we want to study some properties of divisors in a little more detail in section III.5, where the famous Weil reciprocity law lies in the focus. The last section will be section III.6, which might seem to be taken a bit out of context, but it will become most important in chapter VI.

Before we start, we would like to refer the reader to Stichtenoth's excellent book [Sti93], which gives a complete introduction to the theory of algebraic function fields, and from which we took most of the definitions and results. A more advanced treatment of this theory can be found in [Sal06], which we mostly rely on in section III.6.

III.1 Places and Divisors

III.1.1 Definitions and First Properties

Let k be a perfect field with a fixed algebraic closure K. Furthermore, let F/k be a function field of transcendence degree one over k such that k is the full constant field of F/k, i.e. a field extension F/k such that F is a finite extension of $k(x)$ for some transcendental element $x \in F$ over k such that k is algebraically closed in F. Recall from chapter II that such function fields always occur as the function field of some absolutely irreducible curve. In fact, we have proven in section II.7 that there is a one-to-one correspondence between such function fields and absolutely irreducible

nonsingular projective curves (up to isomorphism).

Definition III.1.1. A *place* P of F/k is the maximal ideal of some discrete valuation ring $\mathfrak{O}$ of F/k. An element $t \in P$ with $P = t\mathfrak{O}$ is called a *uniformizer for* $\mathfrak{O}$ *at* P.

Note that by [Sti93, Ch. I, theorem I.1.12], places, valuation rings and discrete valuations of F/k essentially amount to the same thing. So to every place P belongs a unique discrete valuation of F/k which we denote by v_P, and a unique discrete valuation ring, which we denote by $\mathfrak{O}_P$. With this notation, an element $t \in F$ is a uniformizer at P if and only if $v_P(t) = 1$. If we denote the set of all places P of F/k by $\mathbb{P}_{F/k}$, we have the following result.

Proposition III.1.2. For every function field F/k, the set $\mathbb{P}_{F/k}$ of all places is infinite.

Proof. See [Sti93, Ch. I, corollary 3.2, p. 12]. □

The field $F_P := \mathfrak{O}_P/P$ is called the *residue class field of* P and we define the *degree of* P as $\deg P := [F_P : k]$, which is a finite number by [Sti93, Ch. I, proposition I.1.14, p. 6].

Let C/k be an absolutely irreducible curve (affine or projective) (defined over k). We already know that $k(C)$ is a function field of transcendence degree 1 over k with full constant field k. To prevent a massive notational overload, we will always consider F as the function field $k(C)$ of C.

Definition III.1.3. The *divisor group* $\mathrm{Div}(F)$ (or $\mathrm{Div}_k(C)$) of F/k (or C) is defined as the (formal) free abelian group (additively written) generated by the symbols (P) for places P of F/k. An element $D \in \mathrm{Div}(F)$ is called a *divisor* of F/k and is representable as the formal sum

$$D = \sum_{P \in \mathbb{P}_{F/k}} n_P(P) \text{ with } n_P \in \mathbb{Z} \text{ and } n_P = 0 \text{ for almost all } P.$$

The *support of* D, denoted by $\mathrm{supp}(D)$, is the set of all places P for which n_P is nonzero. If the supports of two divisors D and E are disjoint, we say that D and E are *coprime*. In addition, if $k = K$ is algebraically closed, we simply write $\mathrm{Div}(C)$ for $\mathrm{Div}_K(C)$.

If a divisor $D \in \mathrm{Div}(F)$ has the form $D = (P)$ for some $P \in \mathbb{P}_{F/k}$, it is called a *prime divisor*. For $Q \in \mathbb{P}_{F/k}$ and a divisor $D = \sum n_P(P) \in \mathrm{Div}(F)$, we define $v_Q(D) := n_Q$. D is called *effective*, denoted by $D \geq 0$, if $v_P(D) \geq 0$ for all $P \in \mathbb{P}_{F/k}$. By $W \geq D$, we mean that $W - D$ is effective for two divisors D, W. The definition of the degree of a place P can be extended to divisors: We define the following map

$$\deg : \mathrm{Div}(F) \to \mathbb{Z} \text{ by } \sum_{P \in \mathbb{P}_{F/k}} n_P(P) \mapsto \sum_{P \in \mathbb{P}_{F/k}} n_P \cdot \deg(P).$$

The *degree* of a divisor $D \in \mathrm{Div}(F)$ is then defined as the image of D under deg. We put

$$D_0 := \sum_{P \in \mathbb{P}_{F/k}, n_P \geq 0} n_P(P) \text{ and } D_\infty := \sum_{P \in \mathbb{P}_{F/k}, n_P \leq 0} -n_P(P),$$

thus $D = D_0 - D_\infty$.

For an element $f \in F^* := F \setminus \{0\}$ we define the *principal divisor of* f as $\operatorname{div}(f) := \sum_{P \in \mathbb{P}_{F/k}} v_P(f)(P)$. To avoid ambiguity, we sometimes write $\operatorname{div}_F(f)$ instead of just $\operatorname{div}(f)$. The set of all principal divisors forms a subgroup of $\operatorname{Div}(F)$, denoted by $\operatorname{Princ}(F)$. We call the points $P \in \operatorname{supp}(\operatorname{div}(f)_0)$ (resp. $P \in \operatorname{supp}(\operatorname{div}(f)_\infty)$) the *zeros* (resp. *poles*) of f.

Proposition III.1.4. Let C/k be an absolutely irreducible curve (affine or projective) defined over k with function field $F = k(C)$, and let $f \in k(C)^*$. Then:

1. $\operatorname{div}(f)_0 = \operatorname{div}(f^{-1})_\infty$.
2. If $f \notin k$, then $[k(C) : k(f)] = \deg(\operatorname{div}(f)_\infty) = \deg(\operatorname{div}(f)_0)$.
3. $\deg(\operatorname{div}(f)_0) = 0 \iff f \in k^*$.
4. $\deg(\operatorname{div}(f)) = 0$.

Proof. 1. This follows immediately from the properties of the valuations v_P.

2. See [Sti93, Ch. I, theorem I.4.11, p. 18].

3. If $f \in k^*$, then $v_P(f) = 0$ for all $P \in \mathbb{P}_{F/k}$, i.e. $\deg(\operatorname{div}(f)_0) = \deg(0) = 0$.

   Conversely, let $\deg(\operatorname{div}(f)_0) = 0$ and assume that $f \notin k$. This contradicts (2).

4. If $f \notin k$, this follows from (2), since $\operatorname{div}(f) = \operatorname{div}(f)_0 - \operatorname{div}(f)_\infty$. If $f \in k^*$, we have $\deg(\operatorname{div}(f)_0) = 0$ by (3). But $v_P(f) = 0$ for all $P \in \mathbb{P}_{F/k}$, so $\operatorname{div}(f)_\infty = 0$ which gives the result.

□

Corollary III.1.5. Let $f, g \in k(C)^*$ for some absolutely irreducible nonsingular projective curve C. We have:

$$\operatorname{div}(f) = \operatorname{div}(g) \iff f = c \cdot g \text{ for some nonzero constant } c \in k^*.$$

Proof. We have $\operatorname{div}(\frac{f}{g}) = 0$, which particularly means that $\deg(\operatorname{div}(\frac{f}{g})_0) = 0$ and so by part (3) of the last proposition: $c := \frac{f}{g} \in k^*$. This implies that $f = \frac{f}{g} g = cg$. The converse is obvious, as $\operatorname{div}(c) = 0$. □

By $\operatorname{Div}^0(F)$ we denote the set of all degree zero divisors. This is obviously a subgroup of $\operatorname{Div}(F)$, since addition is coefficientwise, the zero divisor has degree 0 and $\deg(-D) = -\deg(D) = 0$ for $D \in \operatorname{Div}^0(F)$. The previous proposition shows in particular that $\operatorname{Princ}(F) \subseteq \operatorname{Div}^0(F)$. This leads us to the following definition.

Definition III.1.6. We define the *divisor class group* of F (resp. C) as the quotient

$$\operatorname{Pic}(F) := \operatorname{Div}(F)/\operatorname{Princ}(F)$$

and the *Picard group* or *Jacobian* of F (resp. C) as

$$\mathrm{Pic}^0(F) := \mathrm{Div}^0(F)/\mathrm{Princ}(F).$$

For a divisor $D \in \mathrm{Div}^0(F)$ (resp. $\mathrm{Div}(F)$), we denote its residue class in $\mathrm{Pic}^0(F)$ (resp. $\mathrm{Pic}(F)$) by $[D]$. Two divisors $D_1, D_2 \in \mathrm{Div}^0(F)$ (resp. $\mathrm{Div}(F)$) lie in the same class if it exists an element $f \in F^*$ such that $D_1 - D_2 = \mathrm{div}(f)$.

III.1.2 The Genus of a Curve

We want to define a very important invariant of an absolutely irreducible curve C/k with function field $F = k(C)$, called its *genus*. Before we are able to do so, we need some preliminaries.

Definition III.1.7. Let $D \in \mathrm{Div}(F)$. Define

$$L(D) := \{f \in F^* \mid \mathrm{div}(f) \geq -D\} \cup \{0\}.$$

$L(D)$ is a finite dimensional k-vector space (see [Sti93, Ch. I, lemma I.4.6, p. 17] and [Sti93, Ch. I, proposition I.4.9, p. 18]), and we define $\ell(D) := \dim_k(L(D))$ as its dimension. We have the following result, which gives a relation between $\ell(D)$ and $\deg(D)$:

Lemma III.1.8. It exists a constant $\gamma \in \mathbb{Z}$ such that

$$\deg(D) - \ell(D) \leq \gamma \text{ for all divisors } D \in \mathrm{Div}(F).$$

Proof. This is [Sti93, Ch. I, proposition I.4.14, p. 20]. □

Since this γ is independent of the divisors D, the following maximum exists.

Definition III.1.9. The non-negative integer

$$g(C) := g(F) := g := \max\{\deg(D) - \ell(D) + 1 \mid D \in \mathrm{Div}(F)\}$$

is called the *genus* of F (resp. C).

III.1.3 The Rational Function Field

As we have seen in example II.5.14, the projective line $\mathbb{P}^1$ is an absolutely irreducible nonsingular projective curve with corresponding function field

$$k(\mathbb{P}^1) = k(\mathbb{A}^1) = k(x)$$

for some transcendental element x over k. The function field $F := k(x)$ over k is called *rational*. For this particular case, we can describe its valuations explicitly.

Let $p(x) \in k[x]$ be a monic, irreducible polynomial. Then the ring

$$\mathfrak{O}_{p(x)} := \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in k[x], p(x) \nmid g(x) \right\}$$

with maximal ideal

$$\mathfrak{p}_{p(x)} := \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in k[x], p(x) \mid f(x), p(x) \nmid g(x) \right\} \tag{III.1}$$

defines a valuation ring. Places of the type $\mathfrak{p}_{p(x)}$ are called *finite*.

There is another valuation ring of $k(x)/k$, namely

$$\mathfrak{O}_\infty := \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in k[x], \deg(f(x)) \leq \deg(g(x)) \right\}$$

with maximal ideal

$$\mathfrak{p}_\infty := \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in k[x], \deg(f(x)) < \deg(g(x)) \right\}. \tag{III.2}$$

The place $\mathfrak{p}_\infty$ is called the *infinite* place of $k(x)$.

These are already all the places of $k(x)/k$ as the following theorem yields:

Theorem III.1.10. Let $F = k(x)$ be the rational function field over k.

1. If $\mathfrak{p} = \mathfrak{p}_{p(x)}$ is a finite place of F/k as in (III.1), then $p(x)$ is a uniformizer at $\mathfrak{p}$, $\deg(\mathfrak{p}) = \deg(p(x))$ and we have an isomorphism

   $$k[x]/(p(x)) \cong F_\mathfrak{p}.$$

   For $z \in F^*$ of the form $z = p(x)^n \cdot (f(x)/g(x))$ with $n \in \mathbb{Z}, f(x), g(x) \in k[x], p(x) \nmid f(x)$ and $p(x) \nmid g(x)$, we have $v_\mathfrak{p}(z) = n$.

2. If $\mathfrak{p} = \mathfrak{p}_\infty$ is the infinite place of F/k as in (III.2), then $1/x$ is a uniformizer at $\mathfrak{p}$ and $\deg(\mathfrak{p}) = 1$. For $z = f(x)/g(x) \in F^*$ we have $v_\mathfrak{p}(z) = \deg(g(x)) - \deg(f(x))$.

3. There are no places of F/k other than the places $\mathfrak{p}_{p(x)}$ and $\mathfrak{p}_\infty$, defined by (III.1) and (III.2).

Proof. (1) and (2) are [Sti93, Ch. I, proposition 2.1, p. 9]. (3) is [Sti93, Ch. I, theorem 2.2, p. 10]. □

The subring $k \subsetneqq k[x] \subsetneqq F := k(x)$ is of a special type:

Definition III.1.11. For $\emptyset \neq S \subsetneqq \mathbb{P}_{F/k}$ let

$$\mathfrak{O}_S := \{z \in F \mid v_\mathfrak{p}(z) \geq 0 \text{ for all } \mathfrak{p} \in S\}$$

be the intersection of all valuation rings $\mathfrak{O}_\mathfrak{p}$ with $\mathfrak{p} \in S$. Any ring of this form is called a *holomorphy ring* of F/k.

Lemma III.1.12. Let $F = k(x)$ be a rational function field over k. Then,

$$k[x] = \bigcap_{\mathfrak{p}_\infty \neq \mathfrak{p} \in \mathbb{P}_{F/k}} \mathfrak{O}_\mathfrak{p},$$

i.e. $k[x] = \mathfrak{O}_S$ for $S := \{P \in \mathbb{P}_{F/k} \mid \mathfrak{p} \neq \mathfrak{p}_\infty\}$ is a holomorphy ring of F/k.

Proof. Let $z = f(x) \in k[x]$. By part (1) of the theorem, it is clear that $v_\mathfrak{p}(z) \geq 0$ for all finite places $\mathfrak{p}$ of F/k. Conversely, let z be an element of the intersection of all $\mathfrak{O}_\mathfrak{p}$ ($\mathfrak{p}$ runs through all finite places of F/k). Suppose that $z \in k(x) \setminus k[x]$, i.e. $z = f(x)/g(x)$ with $f(x), g(x) \in k[x]$ coprime and $\deg(g(x)) > 0$. Let $p(x) \in k[x]$ be a monic irreducible polynomial with $p(x) \mid g(x)$. Since $f(x)$ and $g(x)$ are coprime, this implies $p(x) \nmid f(x)$ and we have by part (1) of the theorem that $v_\mathfrak{p}(z) < 0$ for the finite place $\mathfrak{p} = \mathfrak{p}_{p(x)}$. This in turn means $z \notin \mathfrak{O}_\mathfrak{p}$, which is a contradiction. □

There is the following useful result on holomorphy rings in arbitrary function fields F/k:

Theorem III.1.13. Let R be a subring of F/k and let

$$S(R) := \{P \in \mathbb{P}_{F/k} \mid R \subseteq \mathfrak{O}_P\}.$$

Then the following holds:

1. $\emptyset \neq S(R) \subsetneqq \mathbb{P}_{F/k}$.
2. The integral closure of R in F is $\mathfrak{O}_{S(R)}$, which has F as its quotient field.

Proof. This is [Sti93, Ch. III, theorem 2.6, p. 69]. □

III.2 The Riemann-Roch Theorem

In this section we want to give the most important theorem in the theory of function fields, namely the *Riemann-Roch theorem*. Let C/k be an absolutely irreducible curve over k with function field $F = k(C)$. For any divisor $D \in \mathrm{Div}(F)$, it gives a relation between $\ell(D)$ and $\deg(D)$ via the genus of C. Also, some important consequences of this shall be considered. We will need some results on *Weil differentials* and *adeles*. These two notions shall be defined, firstly.

Definition III.2.1. We define

$$\mathcal{A}_C := \mathcal{A}_F := \{\alpha = (\alpha_P)_{P \in \mathbb{P}_{F/k}} \subseteq F \mid \alpha_P \in R_P \text{ for almost all } P \in \mathbb{P}_{F/k}\}$$

as the *adele space* of F (resp. C). Its elements α are called *adeles*.

This becomes a k-vector space by adding and scalar-multiplying elements componentwise. Then, we can define a k-subspace of $\mathcal{A}_F$ for every divisor $D \in \mathrm{Div}(F)$:

$$\mathcal{A}_C(D) := \mathcal{A}_F(D) := \{\alpha \in \mathcal{A}_F \mid v_P(\alpha) \geq -v_P(D) \text{ for all } P \in \mathbb{P}_{F/k}\}.$$

Now, a k-linear map $\omega : \mathcal{A}_F \to k$ that vanishes on $\mathcal{A}_F(D) + F$ for some divisor $D \in \mathrm{Div}(F)$ is called a *Weil differential* of F/k (resp. C). The set

$$\Omega_C := \Omega_D := \{\omega \mid \omega \text{ is a Weil differential of } F/k\}$$

is called the *module of Weil differentials* of F/k (resp. C).

Having defined these notions, we can define special divisors of C, namely *canonical divisors*. The zero-divisor, for instance, is such a canonical divisor. For a nonzero Weil differential ω, we have the following result for which we define

$$M(\omega) := \{D \in \mathrm{Div}(F) \mid \omega \text{ vanishes on } \mathcal{A}_F(D) + F\}.$$

Lemma III.2.2. Let $0 \neq \omega \in \Omega_C$. Then there is a uniquely determined divisor $W \in M(\omega)$ such that $D \leq W$ for any $D \in M(\omega)$. W is called *the divisor of* ω and is denoted by $\mathrm{div}(\omega)$.

Proof. See [Sti93, Ch. I, lemma I.5.10, p. 27]. □

Definition III.2.3. A divisor $D \in \mathrm{Div}(F)$ is called a *canonical divisor* of F (or C), if $D = \mathrm{div}(\omega)$ for some $\omega \in \Omega_F$.

Finally, we are able to state the Riemann-Roch theorem.

Theorem III.2.4. Let C/k be an absolutely irreducible curve with function field $F = k(C)$. Then, for any $D \in \mathrm{Div}(F)$, we have

1. If $W \in \mathrm{Div}(F)$ is a canonical divisor then:

$$\ell(D) = \deg(D) + 1 - g + \ell(W - D)$$

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

3. If $\deg(D) \geq 2g - 1$, then $\ell(D) = \deg(D) + 1 - g$.

Proof. 1. See [Sti93, Ch. I, theorem I.5.15, p. 28].

2. This is an immediate consequence of the first part.

3. Cf. [Sti93, Ch. I, theorem I.5.17, p. 29].

□

As a very important consequence of this, we have the following result that ensures the existence of functions with prescribed poles and zeros of particular order.

Corollary III.2.5. If $D = \sum n_P(P) \in \mathrm{Div}(F)$ is a divisor of degree $\geq g$, then there is a function $f \in F$, which has poles of order at most n_P (hence zeros of order at least $-n_P$ if $n_P < 0$) at the places $P \in \mathrm{supp}(D)$ and no poles elsewhere.

Proof. Let $D = \sum_{P \in \mathbb{P}_{F/k}} n_P(P) \in \mathrm{Div}(F)$ be a divisor of degree $\geq g$. By theorem III.2.4(2), we have $\ell(D) \geq \deg(D) + 1 - g \geq 1$, so $L(D) \neq \{0\}$. We can pick a nonzero element $f \in L(D)$, i.e. $\mathrm{div}(f) \geq -D$. For $P \in \mathbb{P}_{F/k}$ with $n_P > 0$, this means that f has a pole at P of order at most n_P as $-v_P(f) \leq n_P$. Similarly, if $n_P < 0$ for a place $P \in \mathbb{P}_{F/k}$, f has a zero at P of order at least $-n_P$ as $v_P(f) \geq -n_P$. For all places $P \in \mathbb{P}_{F/k}$ with $n_P = 0$ we have $v_P(f) \geq 0$, so f has no pole at P (it might have a zero though). □

Another consequence of the Riemann-Roch theorem concerns the Picard group $\mathrm{Pic}^0(F)$ for an absolutely irreducible curve C/k defined over a finite field k with function field $F = k(C)$.

Corollary III.2.6. Let $k = \mathbb{F}_q$ be a finite field with q elements and let C/k be an absolutely irreducible curve over k with function field $F = k(C)$. Then, the Picard group $\mathrm{Pic}^0(F)$ is a finite group and its order $h = h_F = h_C$ is called *the class number* of F (or C).

Proof. This is [Sti93, Ch. V, proposition 1.3, p. 159]. □

We want to give another two applications of the Riemann-Roch theorem, starting with the so called *strong approximation theorem.*

Corollary III.2.7. Let $S \subsetneq \mathbb{P}_{F/k}$ be a proper subset and let $P_1, \ldots, P_r \in S$, $r \in \mathbb{N}$. Suppose there are given $x_1, \ldots, x_r \in F$ and $n_1, \ldots, n_r \in \mathbb{Z}$. Then there exists an element $x \in F$ such that

$$v_{P_i}(x - x_i) = n_i \text{ for all } i = 1, \ldots, r, \text{ and}$$

$$v_P(x) \geq 0 \text{ for all } P \in S \setminus \{P_1, \ldots, P_r\}.$$

Proof. See [Sti93, Ch. I, theorem 6.4, p. 31]. □

The second application is *Clifford's theorem*:

Theorem III.2.8. Let F/k be a function field with full constant field k. Then, for any divisor D with $0 \leq \deg(D) \leq 2g - 2$ we have that

$$\ell(D) \leq 1 + \frac{1}{2} \cdot \deg(D).$$

Proof. This is [Sti93, Ch. I, theorem 6.11, p. 34]. □

III.3 Algebraic Extensions of Function Fields

As usual, we let C/k be an absolutely irreducible curve over k with function field $F = k(C)$. Moreover, let C'/k' be another absolutely irreducible curve over an extension field $k' \supseteq k$ with function field $F' = k'(C')$ such that F'/F is an algebraic extension. We assume that $F \subseteq F'$ are both contained in a common algebraic closure Φ. In this situation, F'/k' is called an *algebraic extension of* F/k.

Definition III.3.1. 1. If $F' = Fk'$ (= smallest field that contains both F and k'), then F'/k' is called a *constant field extension of* F/k.

2. If $[F' : F] < \infty$, then F'/k' is called a *finite extension of* F/k.

3. If F'/F is a finite Galois extension, then F'/k is called a *Galois extension of* F/k.

The next proposition summarizes some important properties of general algebraic extensions of function fields.

Proposition III.3.2. Let F'/k' be an algebraic extension of F/k.

1. k'/k is an algebraic extension with $F \cap k' = k$, and $[F' : F] < \infty$ if and only if $[k' : k] < \infty$.

2. For a place P (resp. P') of F/k (resp. F'/k') with corresponding valuation ring $\mathfrak{O}_P$ (resp. $\mathfrak{O}'_{P'}$) and discrete valuation v_P (resp. $v'_{P'}$), we have:

$$P \subseteq P' \iff \mathfrak{O}_P \subseteq \mathfrak{O}'_{P'} \iff \exists e \in \mathbb{Z}_{\geq 1} \forall x \in F : v'_{P'}(x) = e \cdot v_P(x).$$

In this case, we say that P' *lies over* P (denoted by $P' \mid P$) and we have

$$P = P' \cap F \text{ and } \mathfrak{O}_P = \mathfrak{O}'_{P'} \cap F.$$

Moreover, $e(P'|P) := e$ is called the *ramification index of* P' *over* P, whereas $P'|P$ is *ramified*, if $e(P'|P) > 1$, and *unramified*, if $e(P'|P) = 1$.

3. Any place P' of F'/k' lies over exactly one place P of F/k, namely $P = P' \cap F$. Conversely, any place P of F/k has at least one, but only finitely many, extensions $P' \in \mathbb{P}_{F'/k'}$.

Proof. 1. This is [Sti93, Ch. III, lemma 1.2, p. 60].

2. See [Sti93, Ch. III, proposition 1.4, p. 60].

3. See [Sti93, Ch. III, proposition 1.7, p. 62].

□

Definition III.3.3. Let P' be a place of an algebraic extension F'/k' of F/k lying over a place P of F/k. We call the number $f(P'|P) := [F'_{P'} : F_P]$ the *inertia index of* P' *over* P.

Proposition III.3.4. Let F'/k' be an algebraic extension of F/k and let $P' \in \mathbb{P}_{F'/k'}$ and $P \in \mathbb{P}_{F/k}$ with $P'|P$. Then

1. $f(P'|P) < \infty \iff [F' : F] < \infty$.

2. If F''/k'' is an algebraic extension of F'/k' and $P'' \in \mathbb{P}_{F''/k''}$ an extension of P', then

$$e(P''|P) = e(P''|P') \cdot e(P'|P) \text{ and } f(P''|P) = f(P''|P') \cdot f(P'|P).$$

Proof. This is [Sti93, Ch. III, proposition 1.6, p. 62]. □

III.3.1 The Conorm

Definition III.3.5. Let F'/k' be an algebraic extension of F/k and let P be a place of F/k. We define the *conorm of P (with respect to F'/F)* by

$$\mathrm{Con}_{F'/F}(P) := \sum_{\substack{P'|P, \\ P' \in \mathbb{P}_{F'/k'}}} e(P'|P)(P') \in \mathrm{Div}(F').$$

This definition can be $\mathbb{Z}$-linearly extended to $\mathrm{Div}(F)$ and yields an injective group homomorphism

$$\mathrm{Con}_{F'/F} : \mathrm{Div}(F) \hookrightarrow \mathrm{Div}(F'), \sum n_P(P) \mapsto \sum n_P \cdot \mathrm{Con}_{F'/F}(P).$$

We summarize some important properties of the conorm of a divisor:

Proposition III.3.6. Let F'/k' be an algebraic extension of F/k. Then:

1. For all $x \in F^*$, we have

$$\mathrm{Con}_{F'/F}(\mathrm{div}_F(x)_0) = \mathrm{div}_{F'}(x)_0, \mathrm{Con}_{F'/F}(\mathrm{div}_F(x)_\infty) = \mathrm{div}_{F'}(x)_\infty$$

and

$$\mathrm{Con}_{F'/F}(\mathrm{div}_F(x)) = \mathrm{div}_{F'}(x).$$

2. If F''/k'' is an algebraic extension of F'/k', we have

$$\mathrm{Con}_{F''/F}(D) = \mathrm{Con}_{F''/F'}(\mathrm{Con}_{F'/F}(D)) \text{ for all } D \in \mathrm{Div}(F).$$

Proof. See [Sti93, Ch. III, proposition 1.9, p. 63]. □

By part (1) of this proposition, the conorm induces a homomorphism of divisor class groups

$$\mathrm{Con}_{F'/F} : \mathrm{Pic}(F) \to \mathrm{Pic}(F').$$

III.3.2 Constant Field Extensions and the Action of Galois

This section is the function field theoretic version of section II.8 of chapter II. Let k'/k be an algebraic extension of a perfect field k and let F/k be a function field with full constant field k. By [Sti93, Ch. III, proposition 6.1, p. 101], k' is the full constant field of $F' := Fk'$ and so, F'/k' is a constant field extension of F/k. We summarize the most important properties of such extensions in the following proposition.

Proposition III.3.7. Let $F' = Fk'$ be a constant field extension of F/k. Then:

1. F'/F is unramified, i.e. $e(P'|P) = 1$ for all $P \in \mathbb{P}_{F/k}$ and all $P' \in \mathbb{P}_{F'/k'}$ with $P'|P$.

2. F'/k' has the same genus as F/k.

3. $\deg(\mathrm{Con}_{F'/F}(D)) = \deg(D)$ for any $D \in \mathrm{Div}(F)$.

4. The conorm map $\mathrm{Con}_{F'/F} : \mathrm{Pic}(F) \to \mathrm{Pic}(F')$ is injective.

5. The residue class field $F'_{P'}$ of any place $P' \in \mathbb{P}_{F'/k'}$ is the compositum $F_P k'$, whereas $P = P' \cap F$.

Proof. This is [Sti93, Ch. III, theorem 6.3, p. 103]. □

Example III.3.8. Let k be a finite field, $k' = K$ a fixed algebraic closure of k, $F = k(C)$ the function field of an absolutely irreducible curve C/k defined over k, and $F' = K(C)$. We show that $K(C)/K$ is a constant field extension of $k(C)/k$. To this end, it suffices to show that $K(C) = k(C) \cdot K$, the compositum of $k(C)$ and K. But this, we have already shown in section II.8, namely in (II.10) and (II.11). An immediate consequence of parts (1) and (3) of the proposition is that

$$\mathrm{Con}_{K(C)/k(C)}(P) = P'_1 + \ldots + P'_r,$$

for $P \in \mathbb{P}_{k(C)/k}$ of degree r and pairwise distinct places $P'_i \in \mathbb{P}_{K(C)/K}$.

Also, we know by the proposition, that $\mathrm{Pic}(k(C))$ is a subgroup of $\mathrm{Pic}(K(C))$ in terms of the injective conorm map.

Before we proceed to the next section, we would like to give one result on the action of the Galois group on place extensions.

Proposition III.3.9. Let F'/k' be an extension of F/k (not necessarily constant), and let P' be a place of F' extending a place P of F. Consider an element $\sigma \in G_{F'/F}$ of the Galois group $G_{F'/F}$. Then $\sigma(P') := \{\sigma(z) \mid z \in P'\}$ is a place of F', and we have

1. $v_{\sigma(P')}(y) = v_{P'}(\sigma^{-1}(y))$ for all $y \in F'$.

2. $\sigma(P') \mid P$.

3. $e(\sigma(P')|P) = e(P'|P)$ and $f(\sigma(P')|P) = f(P'|P)$.

Proof. This is [Sti93, Ch. III, lemma 5.2, p. 89]. □

III.3.3 Galois Extensions

Let F'/k' be a Galois extension of F/k. We let $G_{F'/F}$ act on the set of all extensions $\{P' \in \mathbb{P}_{F'/k'} \mid P' \text{ lies over } P\}$ by defining

$$\sigma(P') := \{\sigma(x) \mid x \in P'\}.$$

One easily checks that this is indeed an action.

Lemma III.3.10. Let F'/k' be a Galois extension of F/k and let P be a place of F. Then, the Galois group $G_{F'/F}$ acts transitively on the set of extensions of P, i.e.

$$\forall P_1, P_2 \in \mathbb{P}_{F'/k'} \text{ with } P_1|P, P_2|P : \sigma(P_1) = P_2 \text{ for some } \sigma \in G_{F'/F}.$$

Proof. This is [Sti93, Ch. III, theorem 7.1, p. 109]. □

We have the following important corollary from this.

Corollary III.3.11. Let F'/k' be a Galois extension of F/k and let P be a place of F. If $P_1, \ldots, P_r$ are all the places of F'/k' lying above P, then we have for all $i, j = 1, \ldots, r$:

$$e(P_i|P) = e(P_j|P) \text{ and } f(P_i|P) = f(P_j|P).$$

We call $e(P) := e(P_i|P)$ the *ramification index* of P, and $f(P) := f(P_i|P)$ the *inertia degree* of P. In addition, we have $e(P) \cdot f(P) \cdot r = [F' : F]$.

Proof. See [Sti93, Ch. III, corollary 7.2, p. 110]. □

III.3.4 Finite Separable Extensions

There are many different types of function field extensions that we will need in later chapters. Here, we want to take a closer look at finite separable extensions. Therefore, let F'/k' be a finite separable extension of F/k, where k (resp. k') is the full constant field of F (resp. F'). We start with the following proposition.

Proposition III.3.12. Assume that the finite separable extension F'/F is of degree n. Let P' be a place of F'/k' lying above a place P of F/k. We denote the discrete valuation ring corresponding to P' (resp. P) by $\mathfrak{O}'_{P'}$ (resp. $\mathfrak{O}_P$). Then, the integral closure $\overline{\mathfrak{O}_P}$ of $\mathfrak{O}_P$ in F' is

$$\overline{\mathfrak{O}_P} = \bigcap_{P'|P} \mathfrak{O}'_{P'}.$$

There exists a F-basis $\{u_1, \ldots, u_n\}$ of F'/F such that

$$\overline{\mathfrak{O}_P} = \sum_{i=1}^{n} \mathfrak{O}_P \cdot u_i.$$

Proof. This is [Sti93, Ch. III, corollary 3.5, p. 75]. □

Such F-bases of F'/F have a special name.

Definition III.3.13. A basis $\{u_1, \ldots, u_n\}$ of F'/F as in the previous proposition is called a *local integral basis* of F'/F at P.

There is a very important result, due to Kummer, that can often be used to determine all extensions of a given place $P \in \mathbb{P}_{F/k}$ in F'. The result is often referred to as *Kummer's theorem.*

Theorem III.3.14. Let P be a place of F/k. Assume that $F' = F(y)$ with $y \in F'$ is integral over $\mathfrak{O}_P$. Let $\varphi(X) = \sum c_i X^i \in \mathfrak{O}_P[X]$ denote the minimal polynomial of y over F, and set $\bar{\varphi} := \sum \bar{c}_i X^i \in F_P[X]$. Moreover, suppose that

$$\bar{\varphi}(X) = \prod_{i=1}^{r} \gamma_i(X)^{\epsilon_i}$$

is the factorization of $\bar{\varphi}(X)$ over F_P.

If at least one of the following conditions

1. $\epsilon_i = 1$ for all $i = 1, \ldots, r$, or
2. $\{1, y, \ldots, y^{n-1}\}$ is a local integral basis at P

is satisfied, then there exists, for $1 \leq i \leq r$, exactly one place $P_i \in \mathbb{P}_{F'/k'}$ with $P_i|P$. The places $P_1, \ldots, P_r$ are all the places of F' lying above P, and we have

$$\mathrm{Con}_{F'/F}(P) = \sum_{i=1}^{r} \epsilon_i(P_i),$$

i.e. $\epsilon_i = e(P_i|P)$. The residue class field $F'_{P_i} = \mathfrak{O}'_{P_i}/P_i$ is isomorphic to $F_P[X]/(\gamma_i(X))$, hence $f(P_i|P) = \deg \gamma_i(X)$.

Proof. This is [Sti93, Ch. III, theorem 3.7, p. 76]. □

III.4 Points and Places

Let C/k be an absolutely irreducible nonsingular curve over k. Recall the surjective map

$$C \to C_{k(C)}, P \mapsto \mathcal{O}_P \tag{III.3}$$

from the proof of proposition II.7.14. There we saw that, if k is algebraically closed, then this is actually a bijection. But the $\mathcal{O}_P$'s are discrete valuation rings and so example III.3.8 yields the bijection

$$C \to \mathbb{P}_{K(C)/K} \text{ given by } P \mapsto \mathfrak{m}_P(K),$$

where $\mathfrak{m}_P(K)$ is the unique maximal ideal of $\mathcal{O}_P$. So each point on C is a place of $K(C)/K$ and vice versa.

Over k, this situation looks a bit different:

Proposition III.4.1. Let C/k be an absolutely irreducible nonsingular curve over k. Then there is a one-to-one correspondence between the Galois orbits $G_{K/k} \cdot P$ of points $P \in C$ and places of $k(C)/k$.

Proof. Let $\mathfrak{p} \in \mathbb{P}_{k(C)/k}$ be a place of degree r, and let $\mathfrak{P}_1, \ldots, \mathfrak{P}_r \in \mathbb{P}_{K(C)/K}$ be the r distinct places of $K(C)/K$ that lie over $\mathfrak{p}$ (recall that $K(C)/k(C)$ is a constant field extension). These correspond to points $P_1, \ldots, P_r \in C$. We want to show that these

points form a Galois orbit. Now by (III.3), we have that $\mathfrak{p} = \mathfrak{m}_P(k)$ for some $P \in C$, where $\mathfrak{m}_P(k)$ is the unique maximal ideal of $\mathcal{O}_P$. Clearly, we have that $\mathfrak{m}_{P_i}(k) = \mathfrak{p}$ for all $i = 1, \ldots, r$, and since $\mathfrak{m}_P(K)$ lies over $\mathfrak{p}$, we have that $P = P_j$ for some $j \in \{1, \ldots, r\}$. Then, since $\mathcal{O}_P = k[C_a]_{\mathfrak{p}_P}$ (cf. section II.5), we only have to show:

1. $\mathfrak{p}_{\sigma(P)} = \mathfrak{p}_P$ for all $\sigma \in G_{K/k}$.
2. $|G_{K/k} \cdot P| = r$.

The first statement ensures that $\sigma(P) \in \{P_1, \ldots, P_r\}$, while the second implies that $G_{K/k} \cdot P = \{P_1, \ldots, P_r\}$. We prove 1.: First of all, we know from the definition that

$$\mathfrak{p}_{\sigma(P)} = \{\phi \in k[C_a] \mid \phi(\sigma(P)) = 0\}.$$

By proposition II.8.3, this means that

$$\mathfrak{p}_{\sigma(P)} = \{\phi \in K[C_a] \mid \tau(\phi) = \phi \text{ for all } \tau \in G_{K/k}, \text{ and } \phi(\sigma(P)) = 0\}.$$

On the other hand, we have for $\phi \in k[C_a]$:

$$0 = \phi(\sigma(P)) = \sigma(\phi)(\sigma(P)) = \sigma(\phi(P)) \iff \phi(P) = 0.$$

But this in turn means $\mathfrak{p}_{\sigma(P)} = \mathfrak{p}_P$ by definition.

Let us prove 2.: We have that

$$[K : k] = [K : k(P)] \cdot [k(P) : k] = [K : k(P)] \cdot r,$$

i.e. $[G_{K/k} : G_{K/k(P)}] = r$, where $k(P)$ denotes the field of definition of P. But the stabilizer subgroup $\mathrm{Stab}_{G_{K/k}}(P)$ of P in $G_{K/k}$ equals $G_{K/k(P)}$ by definition. So, by the orbit-stabilizer theorem (cf. [Bos04, Ch. 5, Bem. 1.5, p. 241]), we have:

$$|G_{K/k} \cdot P| = [G_{K/k} : G_{K/k(P)}] = r,$$

which proves the proposition. □

Recall, that a point $P \in C$ is k-rational if and only if $|G_{K/k} \cdot P| = 1$, as we have shown in section II.8 (in the paragraph after definition II.8.2). So we have the following corollary.

Corollary III.4.2. Let C/k be an absolutely irreducible nonsingular curve over k. There is a one-to-one correspondence between the k-rational points $P \in C(k)$ and the places $\mathfrak{P} \in \mathbb{P}_{k(C)/k}$ of degree 1.

Let C/k be an absolutely irreducible nonsingular curve over k. We know that over the algebraic closure K of k, each point $P \in C$ is a place $\mathfrak{P} \in \mathbb{P}_{K(C)/K}$. This means that we can write a divisor $D = \sum_{\mathfrak{P} \in \mathbb{P}_{K(C)/K}} n_{\mathfrak{P}}(\mathfrak{P}) \in \mathrm{Div}_K(C)$ in the form

$$D = \sum_{P \in C} n_P(P),$$

and we can $\mathbb{Z}$-linearly extend the action of $G_{K/k}$ on the points $P \in C$ to divisors. This immediately gives us the following corollary from the above proposition.

Corollary III.4.3. Let C/k be an absolutely irreducible nonsingular curve over k, and let $k \subseteq l \subseteq K$ be an intermediate field. Then

$$\mathrm{Div}_l(C) = \{D \in \mathrm{Div}_K(C) \mid \sigma(D) = D \text{ for all } \sigma \in G_{K/l}\}.$$

Therefore, we sometimes say that the divisors in $\mathrm{Div}_l(C)$ are *defined over* l.

On principal divisors, the Galois group acts as follows (see [Sti93, Ch. III, lemma 5.2, p. 89]): If $f \in k(C)^*$, then

$$\sigma(\mathrm{div}(f)) = \sum v_P(f)(\sigma(P)) = \sum v_{\sigma^{-1}(P)}(f)(P) = \mathrm{div}(\sigma(f)) \text{ f. a. } \sigma \in G_{K/k}.$$

At the end of this section, we would like to state the *Hasse-Weil bound*, which gives an estimate on the number of k-rational point on an absolutely irreducible nonsingular curve over k, if k is a finite field.

Theorem III.4.4. Let $k = \mathbb{F}_q$ be a finite field with q elements. Moreover, let C/k be an absolutely irreducible nonsingular curve over k of genus g with function field $F = k(C)$. Then:

$$(q+1) - 2\sqrt{q}g \leq |C(k)| \leq (q+1) + 2\sqrt{q}g.$$

By corollary III.4.2, the same bound also holds for the places of F/k of degree 1.

Proof. See [Sti93, Ch. V, theorem 2.3, p. 170]. □

III.5 The Weil Reciprocity Law

Let C/k be an absolutely irreducible nonsingular curve over k with function field $F = k(C)$. We want to study principal divisors in a bit more detail. They have some nice properties, and this section is devoted to the *Weil reciprocity law*, which gives such a property.

As in section II.7, we can regard the elements $f \in F$ as functions on the places $P \in \mathbb{P}_{F/k}$, where f has no pole (i.e. where $f \in \mathfrak{O}_P$) into the residue class field F_P by defining $f(P)$ as f modulo P. If we add the special symbol "∞", we can define

$$f : \mathbb{P}_{F/k} \to F_P \cup \{\infty\} \text{ by } P \mapsto \begin{cases} f \pmod P, \text{ if } f \in \mathfrak{O}_P \\ \infty, \text{ if } f \in F \setminus \mathfrak{O}_P \end{cases}.$$

Remark III.5.1. Let $P \in C(k)$ be a k-rational point on C. Recall the isomorphism

$$\mathcal{O}_P/\mathfrak{p}_P\mathcal{O}_P \cong \mathrm{Quot}(k[C_a]/\mathfrak{p}_P) = k[C_a]/\mathfrak{p}_P \cong k(\xi_1, \ldots, \xi_n)$$

from the paragraph above definition II.5.11, where $\mathcal{O}_P$ is the local ring of P on C with unique maximal ideal $\mathfrak{p}_P\mathcal{O}_P$, $\mathfrak{p}_P = \{\phi \in k[C_a] \mid \phi(P) = 0\}$, and C_a a nonempty affine part of C (the ξ_i's are the images of the X_i's in $k[C_a]_{\mathfrak{p}_P}/\mathfrak{p}_P k[C_a]_{\mathfrak{p}_P}$). In other words, this isomorphism means for $f \in \mathcal{O}_P = \mathfrak{O}_{\mathfrak{P}}$:

$$f(P) = f \pmod{\mathfrak{P}} = f(\mathfrak{P}),$$

where $\mathfrak{P}$ is the unique place of $k(C)$ of degree 1 corresponding to the point $P \in C(k)$. If $f \notin \mathcal{O}_P$, we simply define $f(P) := \infty$.

This definition can be extended to certain divisors by using the convention that $\infty^0 := 1 \in k$: Let $D = \sum n_P(P) \in \mathrm{Div}(F)$ and $f \in F$ with $\mathrm{supp}(D) \cap \mathrm{supp}(\mathrm{div}(f)) = \emptyset$. Then, it makes sense to define

$$f(D) := \prod_{P \in \mathbb{P}_{F/k}} N_{F_P/k}(f(P))^{n_P},$$

where $N_{F_P/k} : F_P \to k$ denotes the usual *norm* of the extension F_P/k. Since the norm map is a homomorphism from F_P^* into k^*, it is immediately seen that the evaluation of a rational function f at a divisor D is both a homomorphism in D (for fixed f) and in f (for fixed D).

Remark III.5.2. Let $f \in k^*$ be a constant (i.e. $\mathrm{div}(f) = 0$) and let $D = \sum n_P(P)$ be a divisor of degree 0. Then, $f(D) = 1$.

Proof. Recall that the embedding $k \subseteq F_P$ is meant in terms of the ring homomorphism

$$k \subseteq \mathfrak{O}_P \to \mathfrak{O}_P/P, x \mapsto x \pmod{P}.$$

Therefore, we have

$$f(D) = \prod f^{\deg(P)\cdot n_P} = f^{\sum n_P \deg(P)} = f^{\deg(D)} = 1.$$

□

Remark III.5.3. If $k = K$ is algebraically closed, we know that places of F/K are actually points on C (cf. corollary III.4.2). Together with remark III.5.1, the evaluation of functions at divisors turns into

$$f(D) = \prod_{P \in C} f(P)^{n_P},$$

where $f \in K(C), D = \sum n_P(P) \in \mathrm{Div}(C)$ such that $\mathrm{supp}(D) \cap \mathrm{supp}(\mathrm{div}(f)) = \emptyset$.

Now, the *Weil reciprocity law* states:

Theorem III.5.4. Let C/k be an absolutely irreducible nonsingular curve over k, and let $f, g \in k(C)^*$ with $\mathrm{supp}(\mathrm{div}(f)) \cap \mathrm{supp}(\mathrm{div}(g)) = \emptyset$. Then:

$$f(\mathrm{div}(g)) = g(\mathrm{div}(f)).$$

Proof. See [Hes04]. □

III.6 The Chebotarev Density Theorem

This section gives a generalization to the case of function fields over finite fields of Dirichlet's theorem on the infinitude of primes in the arithmetic progression $\{a, a+n, a+2n, \ldots\}$, when $\gcd(a,n) = 1$, namely the *Chebotarev density theorem*. We should state the ingredients of this result clearly:

Situation. Let $k = \mathbb{F}_q$ be a finite field with q elements of characteristic $p > 0$, F/k be a function field with full constant field k, and let F' be a finite Galois extension of F. We denote the algebraic closure of k in F' by k', i.e. F'/k' is a function field with full constant field k'.

In order to be able to understand the notations used in the statement of the main result, we need to recall some notions and results from function field theory: Let $P' \in \mathbb{P}_{F'/k'}$ be an extension of a place $P \in \mathbb{P}_{F/k}$. We define the following subgroups of the Galois group $G := G_{F'/F}$ of F' over F:

1. $D := \{\sigma \in G \mid \sigma(P') = P'\}$ is called the *decomposition group* of P' over P.
2. $I := \{\sigma \in G \mid v'_{P'}(\sigma(z) - z) > 0 \text{ for all } z \in \mathfrak{O}'_{P'}\}$ is called the *inertia group* of P' over P.

There is one very important result concerning these two groups, we should recall.

Theorem III.6.1. In the situation of this section, the following statements hold:

1. The decomposition group D has order $e(P'|P) \cdot f(P'|P)$.
2. The inertia group I is normal in D and has order $e(P'|P)$.
3. The residue field extension $F'_{P'}/F_P$ is a Galois extension, and we have an isomorphism
$$G_{F'_{P'}/F_P} \cong D/I. \tag{III.4}$$

Proof. This is [Sti93, Ch. III, theorem 8.2, p. 119]. □

Now, since k is finite, F_P is also a finite field, and so $G_{F'_{P'}/F_P}$ is a cyclic group generated by the Frobenius automorphism (e.g. [Bos04, Ch. 3, Satz 9.6, p. 129])

$$\sigma : F'_{P'} \to F'_{P'}, \quad x \mapsto x^{q^{\deg P}}.$$

Recall that the *norm* of the place P of F, denoted by $N(P)$, is defined as the cardinality of F_P and hence $q^{\deg P} = |F_P| = N(P)$.

By theorem III.6.1, we know that the order of the inertia group is precisely the ramification index $e(P'|P)$. This implies that, if P is unramified (i.e. $e(P'|P) = 1$), then I is trivial which, in turn means in conjunction with (III.4), that D is generated

by the image of the Frobenius automorphism. We denote this element by $\left[\frac{F'/F}{P'}\right]$ and call it the *Frobenius automorphism at* P'. It should be noted that whenever we use the symbol $\left[\frac{F'/F}{P'}\right]$, we will understand that P is unramified.

We want to study what will happen to the Frobenius automorphism at P', when P' runs through all the places over P. Recall that G acts transitively on the set of all extensions $\{P' \in \mathbb{P}_{F'/k'} \mid P' \text{ lies over } P\}$ by lemma III.3.10. Now, by the following result, we see that, when P' runs through all the places over P, the Frobenius automorphism runs through a conjugacy class of G:

Proposition III.6.2. For every $\sigma \in G$ we have:

$$\left[\frac{F'/F}{\sigma(P')}\right] = \sigma \left[\frac{F'/F}{P'}\right] \sigma^{-1}.$$

Proof. This is [Sal06, Ch. 11, proposition 2.3, p. 378]. □

This allows us to define the *Artin symbol*:

Definition III.6.3. Let P' be a place of F' lying over a place P of F such that P is unramified in F'. Then, the *Artin symbol* of P is defined as the conjugacy class

$$\left(\frac{F'/F}{P}\right) = \left\{\sigma \left[\frac{F'/F}{P'}\right] \sigma^{-1} \mid \sigma \in G\right\}.$$

We are almost able to state the main theorem of this section, the only ingredient that is still missing is the following quantitative measure on a subset A of $\mathbb{P}_{F/k}$ which we apply to test its infinitude by a qualitative description.

Definition III.6.4. Let A be a subset of $\mathbb{P}_{F/k}$. Then the limit ($s \in \mathbb{R}, s > 1$)

$$\delta(A) := \lim_{s \to 1^+} \frac{\sum_{P \in A} N(P)^{-s}}{\sum_{P \in \mathbb{P}_{F/k}} N(P)^{-s}},$$

is called the *Dirichlet density of* A, in case the limit exists.

We can finally state the *Chebotarev density theorem*:

Theorem III.6.5. In the situation of this section, let $\mathfrak{C}$ be a conjugacy class of $G_{F'/F}$. Then the Dirichlet density of the set

$$\left\{P \in \mathbb{P}_{F/k} \mid \left(\frac{F'/F}{P}\right) = \mathfrak{C}\right\}$$

exists and is equal to $\frac{|\mathfrak{C}|}{[F':F]}$.

Proof. This is [Sal06, Ch. 11, theorem 2.20, p. 387]. □

We will need this theorem in section VI.3 to prove the non-degeneracy of a pairing that will be defined in that section. In [Sal06], the proof of the above theorem is done in several steps and there is one easy result on the Dirichlet density of a finite set that is of particular interest to us.

Proposition III.6.6. If $A \subseteq \mathbb{P}_{F/k}$ is finite, then $\delta(A) = 0$.

Proof. See [Sal06, Ch. 11, proposition 2.7, p. 379]. □

This means that, if the Dirichlet density of a given set $A \subseteq \mathbb{P}_{F/k}$ is nonzero, the set A has infinitely many places. On the other hand, we have the following bound (which is a consequence of the Hasse-Weil bound, cf. theorem III.4.4) for the number B_d of places of degree d:

Lemma III.6.7. For all $d \geq 1$, we have the estimate

$$|B_d - \frac{q^d}{d}| < (2 + 7g) \cdot \frac{q^{d/2}}{d},$$

where g denotes the genus of F/k.

In particular, there are only finitely many places of a given degree d, and if $d \geq 4g+3$, then $B_d \geq 1$.

Proof. See [Sti93, Ch. V, corollary 2.10, p. 179]. □

Now, let $A \subseteq \mathbb{P}_{F/k}$ be a set of places of F such that $\delta(A) \neq 0$, then the lemma ensures the existence of places in A of degree d for all $d \geq$ some constant. This fact is crucial in the proof of the non-degeneracy of the Tate-Lichtenbaum pairing in section VI.3.

Chapter IV

The Arithmetic of Elliptic Curves

In the sequel of this thesis, we will need two special types of algebraic curves, namely elliptic and hyperelliptic curves. The present chapter deals with the former. It intends to give an overview on the arithmetic of elliptic curves, and will mostly rely on [Sil86]. We will follow our motto (cf. section I.2), and only prove those results that the author could not find in the literature, or for which he wants to present different approaches. For the proofs of all other results, we will refer the reader to an appropriate source.

Starting with the definition of an elliptic curve and its Weierstraß equation in section IV.1.1, we show that the points on an elliptic curve form a group and give explicit formulae to perform the group law in section IV.1.2. Then, in section IV.1.3, we discuss isogenies, which are special morphisms between elliptic curves, and also give a summary of certain properties of them. In particular, we want to give some relations between isogenies and divisors in section IV.1.4. The most important part of this chapter is section IV.2, where we introduce supersingular elliptic curves, which will turn out to be very useful in cryptographic applications in chapter VII. One of the reasons for their usability is the fact that they have an embedding degree less or equal to 6, which we will see in section IV.3.

As we did in introductions of previous chapters, we want to highlight the author's contribution in the present chapter:

- Proof of certain results that are missing/exercises in [Sil86]. See example IV.1.17 and lemma IV.1.16.

- An example of a supersingular elliptic curve over $\mathbb{F}_{11}$ of order 12 with embedding degree 2 (see examples IV.2.7 and IV.3.4).

In what follows, k will denote a perfect field with a fixed algebraic closure K. Moreover, we will always understand an *absolutely irreducible nonsingular projective* curve, when using the term *curve*. Unlike in previous chapters, we will from now on denote a curve over the algebraic closure K simply by C. Recall, that if C is defined over k, we denote this by C/k. These conventions will be carried out until the end.

IV.1 Definitions and Basic Properties

IV.1.1 Definition and Normal Form

We start with the definition of an elliptic curve.

Definition IV.1.1. An *elliptic curve* E is a curve of genus 1, equipped with a special point $\mathcal{O}_E \in E$, called the *point at infinity*. The elliptic curve E is *defined over* k, denoted by E/k (as usual), if it is defined over k as a curve *and* $\mathcal{O}_E \in E(k)$ is k-rational.

Now, the most important result in this section concerns the *Weierstraß equation*. It says that every elliptic curve is isomorphic to a curve given by a Weierstraß equation and vice versa.

Proposition IV.1.2. 1. Every elliptic curve E/k is isomorphic (over k) to a plane curve C/k given by a *Weierstraß equation*

$$C : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

with coefficients $a_1, \ldots, a_6 \in k$, via an isomorphism taking $\mathcal{O}_E$ to $(0 : 1 : 0)$.

2. Conversely, every plane curve C/k given by a Weierstraß equation is an elliptic curve defined over k with point at infinity $\mathcal{O}_E = (0 : 1 : 0)$.

Proof. See [Sil86, Ch. III, proposition 3.1, p. 63]. □

By this proposition, we can always consider an elliptic curve E as a curve $E \subseteq \mathbb{P}^2$ given in Weierstraß form, and it therefore consists of points $P = (x, y) \in \mathbb{A}^2$ that satisfy this equation, together with the point at infinity $\mathcal{O}_E = (0 : 1 : 0)$. In particular, if E is defined over k, then [Sil86, Ch. III, proposition 2.2(f), p. 55] says that

$$E(k) = \{(x, y) \in \mathbb{A}^2(k) \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}_E\}.$$

IV.1.2 Group Law

Elliptic curves have the property that the points on them form a group with a special composition law (denoted by $+$). It is defined as follows.

Lemma IV.1.3. Let E be an elliptic curve in Weierstraß form. Let $P, Q \in E$, L the line connecting P and Q (tangent line to E at P, if $P = Q$), and R the third point of intersection of L with E (this works because of Bezout's theorem, see [Har77, Ch. I, corollary 7.8, p. 54]). Let L' be the line connecting R and $\mathcal{O}_E$. Then $P + Q$ is defined as the third point of intersection of L' with E. This method is called the *chord and tangent process* and makes E into an Abelian group with identity element $\mathcal{O}_E$.

Proof. This is [Sil86, Ch. III, proposition 2.2, p. 55]. □

It is interesting that the group law can also be described via the Picard group of the elliptic curve E.

Proposition IV.1.4. Let E be an elliptic curve. Then, the following map is a group isomorphism:

$$\pi : E \to \mathrm{Pic}^0(E), P \mapsto [(P) - (\mathcal{O}_E)].$$

In particular: If E is defined over k, then $E(k) \cong \mathrm{Pic}^0(k(E))$.

Proof. This is [Sil86, Ch. III, proposition 3.4, p. 66]. The second statement follows by definition of the action of the Galois group $G_{K/k}$ (see also [Sti93, Ch. VI, proposition 1.6, p. 192]). □

This group law can be described in explicit formulae and is perfomed by algorithm 1.

Algorithm 1 Elliptic Curve Group Law Algorithm

INPUT: Two points $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E$.
OUTPUT: The sum $P_3 = P_1 + P_2 \in E$.

if $x_1 = x_2$ and $y_2 = -y_1 - a_1x_2 - a_3$ **then**
  return $\mathcal{O}_E$
else if $x_1 = x_2$ **then**
  $\lambda \leftarrow \frac{3x_1^2+2a_2x_1+a_4-a_1y_1}{2y_1+a_1x_1+a_3}$
  $\nu \leftarrow \frac{-x_1^3+a_4x_1+2a_6-a_3y_1}{2y_1+a_1x_1+a_3}$
else
  $\lambda \leftarrow \frac{y_2-y_1}{x_2-x_1}$
  $\nu \leftarrow \frac{y_1x_2-y_2x_1}{x_2-x_1}$
$x_3 \leftarrow \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$
$y_3 \leftarrow -(\lambda + a_1)x_3 - \nu - a_3$
return (x_3, y_3)

Proof of algorithm 1. See [Sil86, Ch. III, group law algorithm 2.3, p. 58]. □

Remark IV.1.5. If $P_2 \neq -P_1$, then $y = \lambda x - \nu$ is the line through P_1 and P_2, respectively the tangent to E at P_1, if $P_1 = P_2$.

Remark IV.1.6. It is clear that the algorithm runs in polynomial time, since it only consists of the basic operations $+, -, \cdot, /$ in k (cf. [ACD+06, Ch. 11, p. 201]).

Now that we have defined a group law on E, we want to introduce a special notation.

Definition IV.1.7. Let E be an elliptic curve and $P \in E$ a point on it. We define $[0](P) := \mathcal{O}_E$ and let $m \in \mathbb{Z}$. If $m > 0$, we define

$$[m](P) := P + P + \cdots + P \ (m \text{ times})$$

and if $m < 0$, we define $[m](P) = [-m](-P)$. This results in the mapping $[m] : E \to E$ which is called *the multiplication-by-m map.*

Definition IV.1.8. Let E be an elliptic curve. We define the *sum* of a divisor $D = \sum n_P(P) \in \mathrm{Div}(E)$ as

$$\mathrm{sum}(D) := \sum [n_P]P \in E \text{ (addition on } E).$$

Corollary IV.1.9. Let E be an elliptic curve and let $D = \sum n_P(P) \in \mathrm{Div}(E)$. Then:

$$D \text{ is principal } \iff \deg(D) = 0 \text{ and } \mathrm{sum}(D) = \mathcal{O}_E.$$

Proof. See [Sil86, Ch. III, corollary 3.5, p. 67]. □

IV.1.3 Isogenies

Now that we have introduced elliptic curves, it seems to be reasonable to consider morphisms between them that respect the group law.

Definition IV.1.10. Let E and E' be two elliptic curves. A non-constant morphism (cf. definition II.4.10) $\phi : E \to E'$ with the additional property $\phi(\mathcal{O}_E) = \mathcal{O}_{E'}$ is called an *isogeny* between E and E'. In this case, E and E' are said to be *isogenous*.

As a matter of fact (cf. [Har77, Ch. II, proposition 6.8, p. 137]), every isogeny is surjective. We recall the pull-back of a morphism $\phi : E \to E'$ that we have introduced in chapter II:

$$\phi^* : K(E') \to K(E), f \mapsto f \circ \phi.$$

We proved that ϕ^* is a homomorphism of fields and is therefore injective. It is a fact that $K(E)/\phi^*K(E')$ is a finite field extension (see also [Har77, Ch. II, proposition 6.8, p. 137]). This injection allows us to define the *degree of* ϕ as the degree of the field extension $K(E)/\phi^*K(E')$. It also gives us the notion of ϕ being separable: ϕ is called *separable* (inseparable, purely inseparable) if the corresponding field extension has this property. By convention, we let the "constant isogeny", that maps everything to $\mathcal{O}_{E'}$, have degree 0.

Example IV.1.11. [Sil86, Ch. III, theorem 3.6, p. 68] (proof that E is a group variety, cf. lemma IV.2.1) together with [Sil86, Ch. III, proposition 4.2, p. 71] (proof that $[m]$ is non-constant) show that the multiplication-by-m map $[m]$ is an isogeny, if $m \neq 0$.

This example leads us to one of the most important groups in the sequel of this text:

Definition IV.1.12. Let E be an elliptic curve and let $0 \neq m \in \mathbb{Z}$. We define the *m-torsion subgroup of E* as the kernel of the multiplication-by-m isogeny, i.e.

$$E[m] := \{P \in E \mid [m]P = \mathcal{O}_E\}.$$

Consequently, we can define the *torsion subgroup of E* as

$$E_{\mathrm{tors}} = \bigcup_{m=1}^{\infty} E[m].$$

Similarly to this notation, we denote the kernel of an arbitrary isogeny $\phi : E \to E'$ from E to an elliptic curve E' by

$$E[\phi] := \{P \in E \mid \phi(P) = \mathcal{O}_{E'}\}.$$

The multiplication-by-m isogeny is certainly one of the most important isogenies in the theory of elliptic curves, but there is another important map which is "almost" an isogeny:

Example IV.1.13. Let E be an elliptic curve and $Q \in E$ a fixed point on it. We define the following map

$$\tau_Q : E \to E \text{ by } P \mapsto P + Q$$

and call it the *translation-by-Q map*. By writing the map in terms of the explicit addition formulae, we see that τ_Q is a rational map. It has the rational map τ_{-Q} as its inverse and is therefore birational. It is in fact an isomorphism (see [Sil86, Ch. II, proposition 2.1, p. 23]). Clearly, if $Q = \mathcal{O}_E$ then τ_Q is the "constant isogeny", else, it is not an isogeny since $\tau_Q(\mathcal{O}_E) = Q \neq \mathcal{O}_E$.

The notion of the pull-back of an isogeny, we have recalled above, enables us to describe the "ramification" of an isogeny at a point.

Definition IV.1.14. Let $\phi : E \to E'$ be an isogeny of two elliptic curves E and E' and let $P \in E$. We define the *ramification index of ϕ at P* as

$$e_\phi(P) := v_P(\phi^* t_{\phi(P)}),$$

where $t_{\phi(P)} \in K(E')$ is a uniformizer at $\phi(P)$ (in the sense of definition III.1.1) and v_P is the discrete valuation of $K(E')/K$ corresponding to the place P (cf. section III.4). Clearly, $e_\phi(P) \geq 1$. The isogeny ϕ is called *unramified at P* if $e_\phi(P) = 1$; and if it is unramified at any point of E, we simply call it *unramified*.

Similarly to the function-pullback of ϕ, we can define a "divisor-pullback of ϕ":

Definition IV.1.15. Let $\phi : E \to E'$ be an isogeny of two elliptic curves E and E'. Firstly, we define for a place $Q \in \mathrm{Div}(E')$ the mapping

$$(Q) \mapsto \sum_{P \in \phi^{-1}(Q)} e_\phi(P)(P).$$

This map can be $\mathbb{Z}$-linearly extended to $\mathrm{Div}(E')$, yielding the group homomorphism (also denoted by ϕ^*)

$$\phi^* : \mathrm{Div}(E') \to \mathrm{Div}(E), \sum_{Q \in E'} n_Q(Q) \mapsto \sum_{Q \in E'} n_Q \left(\sum_{P \in \phi^{-1}(Q)} e_\phi(P)(P) \right).$$

The next lemma gives a property of this mapping in conjuction with the ramification index of an isogeny:

Lemma IV.1.16. Let $\phi : E \to E'$ be an isogeny of two elliptic curves E and E'.

1. For all $f \in K(E')^*$ and all $P \in E$, we have
$$v_P(\phi^* f) = e_\phi(P) \cdot v_{\phi(P)}(f).$$
2. For all $f \in K(E')^*$, we have
$$\phi^*(\mathrm{div}(f)) = \mathrm{div}(\phi^* f).$$
3. If $\psi : E' \to E''$ is another isogeny from E' to the elliptic curve E'', then:
$$e_{\psi\circ\phi}(P) = e_\phi(P) e_\psi(\phi(P)) \text{ for all } P \in E$$
and
$$(\psi \circ \phi)^* = \phi^* \circ \psi^*.$$

Proof. 1. In section II.5, we proved that the local ring $\mathcal{O}_{\phi(P)}$ of $\phi(P)$ on E' is a discrete valuation ring, i.e. we can write (cf. [Sti93, Ch. I, theorem 1.6, p. 3])
$$f = t_{\phi(P)}^d \cdot f_1 \text{ with } f_1 \in \mathcal{O}_{\phi(P)}^* \text{ and } d := v_{\phi(P)}(f),$$
where $t_{\phi(P)}$ is a uniformizer at $\phi(P)$. This implies
$$v_P(\phi^* f) = v_P(\phi^*(t_{\phi(P)}^d \cdot f_1)) = d \cdot v_P(\phi^* t_{\phi(P)}) + v_P(\phi^* f_1)$$
as ϕ^* is a homomorphism of fields. But $v_P(\phi^* t_{\phi(P)}) = e_\phi(P)$ and $v_P(\phi^* f_1) = v_{\phi(P)}(f_1) = 0$, so
$$v_P(\phi^* f) = d \cdot e_\phi(P).$$

2. We apply the first part:
$$\mathrm{div}(\phi^* f) = \sum_{P\in E} v_P(\phi^* f)(P) = \sum_{P\in E} v_{\phi(P)}(f) e_\phi(P)(P).$$
Since ϕ is surjective, we can write this as
$$\sum_{Q\in E'} \left(v_Q(f) \cdot \sum_{P\in\phi^{-1}(Q)} e_\phi(P)(P) \right) = \sum_{Q\in E'} \left(v_Q(f) \cdot \phi^*((Q)) \right).$$
This in turn equals
$$\phi^* \left(\sum_{Q\in E'} v_Q(f)(Q) \right) = \phi^*(\mathrm{div}(f))$$
by using that ϕ^* is a homomorphism of fields.

3. The first part is simply [Sil86, Ch. II, proposition 2.6(c), p. 28], whereas the second part goes as follows. It is certainly enough to prove the formula for a prime divisor $D = (Q) \in \mathrm{Div}(E'')$ with $Q \in E''$. First of all, we have

$$(\psi \circ \phi)^*((Q)) = \sum_{P \in (\psi\circ\phi)^{-1}(Q)} e_\psi(\phi(P)) e_\phi(P)(P)$$

by using the definition and the previous formula. By exactly the same argumentation as in part (2) of this lemma, this equals

$$\sum_{R \in \psi^{-1}(Q)} \left(e_\psi(R) \sum_{\phi^{-1}(R)} e_\phi(P)(P) \right).$$

Now, by the definition of ϕ^*, ψ^* and the fact that they are homomorphisms, the above term is equal to

$$\phi^* \left(\sum_{R \in \psi^{-1}(Q)} e_\psi(R)(R) \right) = (\phi^* \circ \psi^*)((Q)).$$

□

Example IV.1.17. Let E be an elliptic curve. We want to give two examples of unramified isogenies.

1. The translation-by-Q map τ_Q is unramified for all $Q \in E$.
2. The multiplication-by-(-1) map $[-1]$ is unramified.

Proof. 1. By using part (3) of the lemma, we see that

$$1 = e_{\mathrm{id}}(P) = e_{\tau_{-Q}\circ\tau_Q}(P) = e_{\tau_Q}(P) e_{\tau_{-Q}}(P+Q)$$

for all $P \in E$. But $e_{\tau_Q}(P) \geq 1$ and $e_{\tau_{-Q}}(P+Q) \geq 1$, so both must be equal to 1, i.e. $e_{\tau_Q}(P) = 1$ for all $P \in E$.

2. Same argument as in the first part. Here, $[-1]$ is the inverse to itself, i.e.

$$1 = e_{[-1]}(P) e_{[-1]}(-P) \text{ for all } P \in E.$$

Both ramification indices are ≥ 1 which yields the result.

□

We summarize the results on isogenies that are most important for our purposes in the following theorem:

Theorem IV.1.18. Let $\phi : E \to E'$ be an isogeny of degree m of elliptic curves E and E'. Then:

1. ϕ is a group homomorphism.

2. For every $Q \in E'$ we have

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg(\phi).$$

3. If ϕ is separable, then

$$|\phi^{-1}(Q)| = \deg(\phi) \text{ for all } Q \in E'.$$

   In particular: $|\ker(\phi)| = \deg(\phi)$.

4. There exists a unique isogeny $\hat{\phi} : E' \to E$ such that

$$\hat{\phi} \circ \phi = [m].$$

Proof. 1. See [Sil86, Ch. III, theorem 4.8, p. 75].

2. This is [Sil86, Ch. II, proposition 2.6, p. 28].

3. Cf. [Sil86, Ch. III, theorem 4.10, p. 76].

4. This is [Sil86, Ch. III, theorem 6.1, p. 84].

□

Definition IV.1.19. Let $\phi : E \to E'$ be an isogeny of degree m of elliptic curves E and E'. The unique isogeny of part (4) of the theorem is called the *dual isogeny to* ϕ.

It has some nice properties:

Proposition IV.1.20. Let $\phi : E \to E'$ be an isogeny of degree m of elliptic curves E and E'.

1. We have
$$\hat{\phi} \circ \phi = [m] \text{ on } E \text{ and } \phi \circ \hat{\phi} = [m] \text{ on } E'.$$

2. For all $0 \neq m \in \mathbb{Z}$:
$$\widehat{[m]} = [m] \text{ and } \deg([m]) = m^2.$$

3. $\deg(\hat{\phi}) = \deg(\phi) = m$ and $\hat{\hat{\phi}} = \phi$.

4. As a group homomorphism, $\hat{\phi}$ equals the composition

$$E' \to \mathrm{Div}^0(E') \xrightarrow{\phi^*} \mathrm{Div}^0(E) \xrightarrow{\mathrm{sum}} E$$

   with

$$Q \mapsto (Q) - (\mathcal{O}_{E'}) \mapsto \phi^*((Q) - (\mathcal{O}_{E'})) \mapsto \mathrm{sum}(\phi^*((Q) - (\mathcal{O}_{E'}))).$$

Proof. See [Sil86, Ch. III, theorem 6.2, p. 86] and [Sil86, Ch. III, theorem 6.1, p. 84]. □

IV.1.4 Divisors Revisited

Now that we have the notion of isogenies on elliptic curves, we can prove more relations between these and divisors.

Definition IV.1.21. Let $\phi : E \to E'$ be an isogeny of two elliptic curves. We define

$$\phi_* : K(E) \to K(E') \text{ by } \phi_* := (\phi^*)^{-1} \circ N_{K(E)/\phi^* K(E')},$$

where $N_{K(E)/\phi^* K(E')}$ is the usual norm map of the field extension $K(E)/\phi^* K(E')$. Also, we define this map on the group of divisors of E, namely

$$\phi_* : \mathrm{Div}(K(E)) \to \mathrm{Div}(K(E')), \sum n_P(P) \mapsto \sum n_P(\phi(P)).$$

(Recall that ϕ is a morphism)

The next lemma contains all important relations between ϕ^*, ϕ_* and divisors.

Lemma IV.1.22. Let $\phi : E \to E'$ be an isogeny of two elliptic curves.

1. $\phi^*(\mathrm{div}(f)) = \mathrm{div}(\phi^* f)$ for all $f \in K(E')^*$.
2. $\phi_*(\mathrm{div}(f)) = \mathrm{div}(\phi_* f)$ for all $f \in K(E)^*$.
3. $\deg(\phi^* D) = \deg(\phi) \cdot \deg(D)$ for all $D \in \mathrm{Div}(K(E'))$.
4. $\deg(\phi_* D) = \deg(D)$ for all $D \in \mathrm{Div}(K(E))$.

Proof. 1. This is lemma IV.1.16(2).

2. See [Ser79, Ch. I, proposition 14, p. 17].
3. This is immediate by theorem IV.1.18(2).
4. Clear by definition.

□

IV.2 Supersingular Elliptic Curves

We want to return to the theory of isogenies of elliptic curves E/k by looking at isogenies of the form $\phi : E \to E$ in more detail. For the convenience of the reader, we recall a result on elliptic curves that we have already used in example IV.1.11:

Lemma IV.2.1. Elliptic curves E are *group varieties*, i.e. the group operations

$$[-1] : E \to E, P \mapsto -P \text{ and } + : E \times E \to E, (P, Q) \mapsto P + Q$$

are morphisms of varieties.

Proof. See [Sil86, Ch. III, theorem 3.6, p. 68]. □

As a trivial, but very important consequence, we obtain:

Corollary IV.2.2. Let E and E' be two elliptic curves with isogenies $\phi, \psi : E \to E'$ such that $\psi \neq -\phi$. Then the mapping

$$\phi + \psi : E \to E' \text{ defined by } P \mapsto \phi(P) + \psi(P)$$

is again an isogeny from E to E'.

Proof. By the previous lemma, $\phi + \psi$ is a composition of morphisms, and it certainly maps $\mathcal{O}_E$ to $\mathcal{O}_{E'}$. Since $\psi \neq -\phi$, $\phi + \psi$ is clearly non-constant. □

This lemma allows us to define the group of isogenies for two elliptic curves E and E':

$$\mathrm{Hom}(E, E') := \{\text{isogenies } \phi : E \to E'\} \cup \{\mathcal{O}_{E'}\}$$

where $\mathcal{O}_{E'}$ denotes the "constant isogeny". The commutative group law is simply defined as

$$(\phi + \psi)(P) = \phi(P) + \psi(P) \text{ for all } P \in E,$$

whereas $\mathcal{O}_{E'}$ is the neutral element of that group.

Now assume that $E = E'$, then we know by chapter II that the composition of two morphisms $\phi, \psi \in \mathrm{Hom}(E, E)$ is again a morphism, which is therefore non-constant as ϕ and ψ are surjective. This leads us to the definition of the *endomorphism ring of* E:

$$\mathrm{End}(E) := \mathrm{Hom}(E, E) \cup \{\mathcal{O}_E\},$$

where multiplication is given by composition. Recall that it is indeed a ring by theorem IV.1.18(1).

If E and E' are defined over k, we can restrict our attention to isogenies that are defined over k, and we denote the corresponding groups of isogenies by

$$\mathrm{Hom}_k(E, E') \text{ and } \mathrm{End}_k(E),$$

respectively.

Since isogenies are group homomorphisms, it is obvious that a point $P \in E[m]$ (for an integer m) fulfills

$$\phi(P) \in E[m]$$

for an endomorphism $\phi \in \mathrm{End}(E)$. This allows us to define $\mathrm{End}(E[m])$ as the ring of all endomorphisms restricted to the m-torsion group $E[m]$. Similarly, we define $\mathrm{End}_k(E[m])$.

There are certain elliptic curves for which the endomorphism ring is non-commutative, and we call those curves supersingular. The next proposition leads to a definition of those special curves.

Proposition IV.2.3. Let E/k be an elliptic curve and $0 \neq m \in \mathbb{Z}$. Then:

1. $\deg[m] = m^2$.
2. If $\mathrm{char}(k) = 0$ or if m is coprime to $\mathrm{char}(k)$, then
$$E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \oplus (\mathbb{Z}/m\mathbb{Z}).$$
3. If $\mathrm{char}(k) = p > 0$, then either
$$E[p^e] \cong \{\mathcal{O}_E\} \text{ for all } e = 1, 2, 3, \ldots; \text{ or}$$
$$E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z} \text{ for all } e = 1, 2, 3, \ldots.$$

Proof. See [Sil86, Ch. III, corollary 6.4, p. 89]. □

Definition IV.2.4. If $\mathrm{char}(k) = p > 0$ and $E[p] \cong \{\mathcal{O}_E\}$, we say that the elliptic curve E/k is *supersingular*. Otherwise, it is called *ordinary*.

We have the following interesting characterization of supersingular elliptic curves over finite fields.

Theorem IV.2.5. Assume that $k = \mathbb{F}_q$ is a finite field with q elements that is of characteristic $p > 0$. As usual, we let K denote a fixed algebraic closure of k. If E/k is an elliptic curve defined over k, then the following are equivalent:

1. E is supersingular, i.e. has no points of order p over K.
2. $|E(k)| \equiv 1 \pmod{p}$, i.e. $|E(k)| = q + 1 - t$ for $p \mid t$.
3. The endomorphism ring $\mathrm{End}(E)$ of E over K is non-commutative.

Proof. (1) $\iff$ (2): See [Was03, Ch. 4, propostion 4.31, p. 130].

(1) $\iff$ (3): This is [Sil86, Ch. V, theorem 3.1, p. 137].

□

So we see that the number of k-rational points on an elliptic curve E/k tells us whether E is supersingular or not. The next result, which is due to Waterhouse [Wat69], tells us exactly how many k-rational points exist, when E is supersingular.

Theorem IV.2.6. Let $k = \mathbb{F}_q$ with $q = p^a$ elements, where p is a prime and $a \in \mathbb{N}$. Define
$$T := \{q + 1 - |E(k)| : E/k \text{ an elliptic curve over } k\}.$$
Then T equals the set of all $t \in \mathbb{Z}$ with $|t| \leq 2\sqrt{q}$, which satisfy one of the following conditions:

1. $\gcd(t, p) = 1$.
2. If a is even, then $t = \pm 2\sqrt{q}$.
3. If a is even and $p \not\equiv 1 \pmod{3}$, then $t = \pm\sqrt{q}$.

4. If a is odd and $p = 2, 3$, then $t = \pm\sqrt{qp}$.

5. If (a is odd) or (a is even and $p \not\equiv 1 \pmod 4$), then $t = 0$.

The curves corresponding to condition 1 are ordinary, while the others are supersingular.

Proof. See [Wat69]. □

At the end of this section, we would like to see how the above results work with a particular example.

Example IV.2.7. Let $q = 11$ be a prime number and let $k = \mathbb{F}_{11}$ be a finite field with 11 elements. We fix an algebraic closure K of k and consider the affine curve

$$E : y^2 = x^3 + 3x \text{ over } k.$$

By using the Jacobian criterion (see theorem II.5.12), we see that this is an affine nonsingular curve. Furthermore, it is certainly absolutely irreducible, as one easily verifies (otherwise it would be the affine line). Therefore, E is given by a Weierstraß equation and hence defines an elliptic curve over k by proposition IV.1.2. We want to show that E is supersingular.

First of all, we can use theorem IV.2.6 to see that $|E(k)| = q + 1 = 12$ (this is part 5 of the theorem). This, in turn, means by theorem IV.2.5 that E is supersingular.

Immediately, we find that the k-rational point $(2, 5)$ lies on the curve E. By using the group law on E, we can compute all of its multiples, and see that it is of precise order 12. We get the following table:

Order	Point	Order	Point	Order	Point
1	$\mathcal{O}_E$	4	$(6, 5)$	12	$(2, 5)$
2	$(0, 0)$	4	$(6, 6)$	12	$(2, 6)$
3	$(3, 5)$	6	$(1, 2)$	12	$(7, 1)$
3	$(3, 6)$	6	$(1, 9)$	12	$(7, 10)$

IV.3 The Embedding Degree

Let E/k be an elliptic curve over $k = \mathbb{F}_q$ with an integer $m \mid |E(k)|$, coprime to q. In chapter VI, we will introduce bilinear mappings π (as we have already met in section I.1.1) on $E(\mathbb{F}_{q^s})[m]$, where s is the smallest non-negative integer, depending on E and m, such that π is non-degenerate (at least in those situations we are intersted in). We will now give the precise definition of this integer s and refer the reader to chapter VI for details, and the relation between s and the non-degeneracy of π.

Definition IV.3.1. Let E/k be an elliptic curve over $k = \mathbb{F}_q$ and let $m \in \mathbb{Z}_{\geq 1}$ be coprime to q with $m \mid |E(k)|$. The *embedding degree (of E and m)* is defined as the smallest positive integer $s \geq 1$ such that

$$m \mid (q^s - 1).$$

It seems natural to ask for the embedding degree of certain elliptic curves, like supersingular curves. In fact, supersingular curves always have embedding degree $s \leq 6$, as the next theorem says.

Theorem IV.3.2. The following table lists all possibilities for embedding degree and group structure for supersingular elliptic curves E over $\mathbb{F}_q$:

s	q	$\lvert E(\mathbb{F}_q)\rvert$	Group structure of $E(\mathbb{F}_{q^s})$
1	p^{2b}	$q \pm 2\sqrt{q} + 1$	$(\mathbb{Z}/(\sqrt{q} \pm 1)\mathbb{Z})^2$
2	(5)	$q + 1$	$(\mathbb{Z}/(q+1)\mathbb{Z})^2$
3	(3)	$q + \sqrt{q} + 1$	$(\mathbb{Z}/(q^{3/2} - 1)\mathbb{Z})^2$
3	(3)	$q - \sqrt{q} + 1$	$(\mathbb{Z}/(q^{3/2} + 1)\mathbb{Z})^2$
4	2^{2b+1}	$q \pm \sqrt{2q} + 1$	$(\mathbb{Z}/(q^2+1)\mathbb{Z})^2$
6	3^{2b+1}	$q \pm \sqrt{3q} + 1$	$(\mathbb{Z}/(q^3+1)\mathbb{Z})^2$

The numbers (3) and (5) in the q column correspond to the cases 3 and 5 of theorem IV.2.6.

Proof. See [Men93, Ch. 5, table 5.2, p. 73] or [BSS05, Ch. IX, theorem IX.20, p. 199]. □

We have the following important corollary from this table.

Corollary IV.3.3. Let E/k be a supersingular elliptic curve over k with $m \mid \lvert E(k)\rvert$ for some prime number $m > 4\sqrt{q}$. If s denotes the embedding degree of E, and if m and $l := k(\mu_m)$, then

$$m^2 \mid \lvert E(l)\rvert \text{ but } m^3 \nmid \lvert E(l)\rvert, \text{ and } E(l)[m] \cap mE(l) = \{\mathcal{O}_E\}.$$

In particular, we have an isomorphism

$$E(l)[m] \cong E(l)/mE(l),$$

i.e. $E(l)[m]$ is a system of representatives for $E(l)/mE(l)$.

Proof. This is [BSS05, Ch. IX, theorem IX.22, p. 200]. □

We want to use theorem IV.3.2 to see what the embedding degree of a particular supersingular elliptic curve looks like.

Example IV.3.4. Recall the supersingular elliptic curve

$$E : y^2 = x^3 + 3x \text{ over the finite field } k = \mathbb{F}_{11}$$

from example IV.2.7. We have seen that there are exactly $\lvert E(k)\rvert = 12$ k-rational points on E. By theorem IV.3.2 this means that the embedding degree of E is always $s = 2$.

Chapter V

The Arithmetic of Hyperelliptic Curves

As we have already mentioned in chapter IV, the second type of curves, we are interested in, is the hyperelliptic type, to which the present chapter is devoted. It seems that the theory of these curves is not extensively treated in the literature from a function field theoretic viewpoint. Therefore, we try to give a very general approach to this topic. For instance, we neither restrict our attention to certain characteristics of the ground field, nor do we assume the curves to be imaginary quadratic from the start (e.g. as it is done in the excellent appendix of [Kob99]).

Hyperelliptic curves are a generalization of elliptic curves. Loosely speaking, they are elliptic curves of genus $g > 1$, and we give a precise definition together with a normal form, which looks similar to the Weierstraß equation of elliptic curves, in section V.1. As a special delicacy, section V.1.3 contains a short treatment of the so called Weierstraß points that always exist on hyperelliptic curves over algebraically closed fields. We will discuss their existence over non-algebraically closed fields as well. The main part of this chapter is section V.2. We start in sections V.2.1 and V.2.2 with a very general introduction to fractional ideals and the ideal class group, in order to prove corollary V.2.17 in section V.2.3, saying that the ideal class group is isomorphic to the Jacobian of an imaginary quadratic hyperelliptic curve. It is then the aim of section V.2.4 to prove the existence of so called semireduced divisors in any given ideal class. We will "reduce" those divisors in section V.2.5 to so called reduced divisors, which are unique in the case of imaginary quadratic hyperelliptic curves. Section V.3 forms the last section of this chapter, in which we make all the just described steps explicit and give an efficient algorithm to perform the group law in the Jacobian of an imaginary quadratic hyperelliptic curve.

The author's own contributions include the following highlights:

- A very detailed and complete derivation of the general Weierstraß equation (V.1) of an arbitrary hyperelliptic curve in section V.1.
- A complete introduction to fractional ideals and the ideal class group in sections V.2.1 and V.2.2. Although these two sections are based on [AM69], we give all

the proofs that are missing in that reference, plus some additional results (in particular, see lemma V.2.9 and remark V.2.12).

- Proofs of certain results that seem to be missing in the literature. See corollary V.2.17, lemma V.2.14, and theorem V.2.16.

- An elaboration of results about different representatives of ideal classes is given in section V.2.4. The proofs of theorems V.2.28 and V.2.36 should get the most attention. Many results are based on [Eng00].

- A complete and very detailed proof of the consistency of Cantor's algorithm in section V.3, based on [Eng00].

Unlike in previous chapters, we will from now on assume $k = \mathbb{F}_q$ to be a *finite* field with q elements, and let K denote a fixed algebraic closure of k.

V.1 Definitions and Normal Forms

Definition V.1.1. An absolutely irreducible nonsingular projective curve C defined over 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 $x \in k(C)$ that is transcendental over k.

Since every field extension of degree 2 is normal, the condition on $k(C)$ in the definition is actually equivalent to saying that it exists $x \in k(C)$ transcendental over k such that $k(C)/k(x)$ is a cyclic Galois extension of degree 2. By the usual decomposition law for Galois extensions (cf. corollary III.3.11) we know, for a place $\mathfrak{p}$ of $k(x)$, that $efr = 2$, where r denotes the number of its extensions in $k(C)$, f its inertia degree and e its ramification index. So $\mathfrak{p}$ may be either *(totally) ramified* (i.e. $e = 2$), *(completely) splitting* (i.e. $r = 2$) or *inert* (i.e. $f = 2$). This has an important consequence concerning the k-rational points on C.

If P is a place of $k(C)$ of degree 1, then it exists exactly one place $\mathfrak{p} = P \cap k(x)$ lying under P, which also has to have degree 1 since

$$1 = \deg(P) = [k(C)_P : k] = [k(C)_P : k(x)_\mathfrak{p}][k(x)_\mathfrak{p} : k] = [k(C)_P : k(x)_\mathfrak{p}] \deg(\mathfrak{p}).$$

Now, assume that all places of degree 1 of $k(x)$ are inert and that $\mathfrak{p}$ is such a place. This means that it exists precisely one place P of $k(C)$ extending $\mathfrak{p}$ with $e = e(P|\mathfrak{p}) = 1$ and $f = f(P|\mathfrak{p}) = 2$. We know by theorem III.6.1 that the decomposition group D of P over $\mathfrak{p}$ has order 2, the inertia group of P over $\mathfrak{p}$ is trivial and that the Galois group $G_{k(C)_P/k(x)_\mathfrak{p}}$ of the Galois extension $k(C)_P/k(x)_\mathfrak{p}$ is isomorphic to D, i.e.

$$\deg(P) = [k(C)_P : k] = [k(C)_P : k(x)_\mathfrak{p}] \deg(\mathfrak{p}) = 2.$$

So C has no k-rational points by corollary III.4.2. This degenerate case can be resolved

by the Hasse-Weil bound (see theorem III.4.4), which says that

$$N \geq (q+1) - 2\sqrt{q}g.$$

So if $q \geq 4g^2$, we have that $N \geq (4g^2+1) - 4g^2 = 1$. This means that C does always have k-rational points, if the field k is "big enough", i.e. if $q \geq 4g^2$. Therefore, we will always assume that *k is a field with $q \geq 4g^2$ elements* (this is the case for most cryptographic applications anyway).

Now we know that there exists a place of $k(x)$ that is not inert and for simplicity, *we may assume that this place is the infinite place $\mathfrak{p}_\infty$ of $k(x)$*. Otherwise, we may choose a place $\mathfrak{p} = \mathfrak{p}_p$ of degree 1 of $k(x)$ that is not inert, where p is a monic irreducible polynomial in $k[x]$, which is a uniformizer for $\mathfrak{p}$, i.e. $v_\mathfrak{p}(\frac{1}{p}) = -1$. Since we are considering the rational function field $k(x)$, it is clear that $v_\mathfrak{q}(\frac{1}{p}) = 0$ for all other places $\mathfrak{q}$ of $k(x)$. This means that the pole divisor $\mathrm{div}(\frac{1}{p})_\infty$ of $\frac{1}{p}$ in $k(C)$ can only have the two forms

$$\mathrm{div}(\frac{1}{p})_\infty = \begin{cases} P_1 + P_2, \text{ if } \mathfrak{p} \text{ is ramified} \\ 2P, \text{ else} \end{cases},$$

where P_1, P_2 respectively P are (all) the places of $k(C)$ extending $\mathfrak{p}$ in the corresponding case. By theorem III.1.4 we therefore have

$$[k(C) : k(\frac{1}{p})] = \deg(\mathrm{div}(\frac{1}{p})_\infty) = 2,$$

and $k(C)$ is a cyclic Galois extension of $k(\frac{1}{p})$ of degree 2, in which the infinite place is not inert. So by changing our element x to $\frac{1}{p}$, we may always assume that the infinite place $\mathfrak{p}_\infty$ is not inert. This leads us to the following definition:

Definition V.1.2. A hyperelliptic curve C is called *imaginary quadratic*, if the infinite place $\mathfrak{p}_\infty$ of $k(x)$ is (totally) ramified, and it is called *real quadratic*, if $\mathfrak{p}_\infty$ is (completely) splitting.

In what follows, we will mean an *absolutely irreducible curve*, when we use the term *curve*. As an easy application of the Riemann-Roch theorem, we have the following characterization of a hyperelliptic curve.

Lemma V.1.3. A nonsingular curve C of genus $g > 1$ is hyperelliptic if and only if it exists an effective divisor $D \in \mathrm{Div}(C)$ of degree 2 such that $\ell(D) \geq 2$.

In particular: Every nonsingular curve of genus 2 is hyperelliptic.

Proof. See [Sti93, Ch. VI, lemma 2.2, p. 193]. □

Now, since $g \geq 2$ we see that $\deg(D) = 2 \leq 2(g-1)$ and we can apply theorem III.2.8 to our situation:

$$2 \leq \ell(D) \leq 1 + \frac{1}{2} \cdot \deg(D) = 2, \text{ i.e. } \ell(D) = 2.$$

$1, x \in L(D)$ are obviously linearly independent over k and form a k-basis of $L(D)$ since $L(D)$ is a 2-dimensional k-vector space. By theorem III.2.4(2), we know that

$$\ell(jD) \geq (j-1)\deg(D) + \deg(D) + 1 - g = (j-1)\deg(D) + \ell(D) = 2j$$

for all $1 \leq j \leq g$. For $j \in \{1, \ldots, g\}$ we have

$$\operatorname{div}(x^j) = j \cdot \operatorname{div}(x) \geq -jD, \text{ so } 1, x, \ldots, x^j \in L(jD).$$

These are $\leq 2j$ elements and we claim that they are linearly independent over k. To prove this, we assume that there exist $a_0, \ldots, a_j \in k$ (not all of them are zero) such that

$$a_j x^j + \cdots + a_1 x + a_0 = 0.$$

The number $n := \max\{i \mid a_i \neq 0\}$ is certainly nonzero and we see, by multiplying with $(a_n)^{-1}$, that x is a root of a monic polynomial of degree n in $k[X]$. This is a contradiction as x is assumed to be transcendental over k.

Consider the divisor $(g+1)D$ which is of degree $2g+2 \geq 2g-1$ so $\ell((g+1)D) = 2g+2+1-g = g+3$ by theorem III.2.4(3). This means that there must be a $(g+3)$-th function $y \in L((g+1)D)$ that is independent of the $g+2$ powers of x: $1, x, \ldots, x^{g+1}$. Assume that $y \in k[x]$, i.e. it exist $a_0, \ldots, a_n \in k$ such that

$$y = a_n x^n + \cdots + a_1 x + a_0.$$

Since y is linearly independent of $1, x, \ldots, x^{g+1}$, we see that $n > g+1$. This implies for all places $P \in \mathbb{P}_{k(C)/k}$ that

$$\begin{aligned} v_P(y) &= 0 && \text{if } v_P(x) > 0 \\ v_P(y) &\geq 0 && \text{if } v_P(x) = 0 \\ v_P(y) &= n \cdot v_P(x) < 0 && \text{if } v_P(x) < 0. \end{aligned}$$

Now, x has at least one pole P and we therefore have

$$v_P(y) < 0 < -v_P(x),$$

so $y \notin L(D)$, which is a contradiction, i.e. $y \notin k[x]$. Again by theorem III.2.4(3), we know that the vector space $L(2(g+1)D)$ has dimension $3g+5$ and since $(g+1)D \subseteq 2(g+1)D$, it contains the following $3g+6$ functions

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

This means that one of these functions is a nontrivial k-linear combination of the others, in which y^2 has a nonzero coefficient a, since $y \notin k[x]$. We multiply this combination by a and replace y by $a^{-1}y$. This allows us to assume that $a = 1$, which leads to an

equation

$$y^2 + h(x)y = f(x), \tag{V.1}$$

where $h(x), f(x) \in k[x]$ with $\deg(h) \leq g+1$ and $\deg(f) \leq 2g+2$. We would like to know more about the degrees of the polynomials h, f, and it is in fact possible to determine the exact degrees. This is done in the next section.

V.1.1 Normal Forms

Before, we have seen that a hyperelliptic curve yields an equation

$$y^2 + h(x)y = f(x).$$

In this section, we want to study this equation in more detail. In particular, we want to show that every hyperelliptic curve is birationally equivalent to the affine curve defined by this equation.

First of all, it should be said that the function fields of hyperelliptic curves are also called hyperelliptic.

Definition V.1.4. A *hyperelliptic* function field with full constant field k is a quadratic extension of genus > 1 of a rational function field. The terms *imaginary quadratic* and *real quadratic* are defined as for hyperelliptic curves.

In odd characteristic we have the following result about the precise degrees of h and f.

Theorem V.1.5. Assume that $\mathrm{char}(k) \neq 2$.

1. Let F/k be a hyperelliptic function field of genus $g > 1$. Then, F is the function field of a nonsingular plane affine curve given by an equation

$$y^2 = f(x) \in k[x] \tag{V.2}$$

with a monic square-free (over the algebraic closure) polynomial $f(x)$ of degree m, where m equals $2g+1$ or $2g+2$.

2. Conversely, a nonsingular projective curve C/k that is birationally equivalent to an affine nonsingular curve of type (V.2) (such a curve exists by section II.7) is a hyperelliptic curve of genus

$$g = \begin{cases} (m-1)/2 \text{ if } m \equiv 1 \bmod 2 \\ (m-2)/2 \text{ if } m \equiv 0 \bmod 2. \end{cases}$$

3. For a hyperelliptic curve C/k given by (V.2), we have

$$C \text{ is } \begin{cases} \text{imaginary quadratic, if } \deg(f) = 2g+1 \\ \text{real quadratic, if } \deg(f) = 2g+2. \end{cases}$$

In the first case, the infinite place $\mathfrak{p}_\infty$ of $k(x)$ is ramified and in the second, it is splitting.

Proof. 1. The first part is [Sti93, Ch. VI, proposition 2.3(a), p. 194], whereas the fact that $f(x)$ can be chosen to be monic is [Eng00, Ch. 3, theorem 3.3, p. 40], so it suffices to show that (V.2) defines a nonsingular plane affine curve. Firstly, we want to show that $y^2 - f(x)$ is irreducible in $k(x)[y]$. Assuming that it is reducible, we see that $y^2 - f(x) = (y - \alpha)(y - \beta)$ in $k(x)[y]$, which implies by Gauss that $\alpha, \beta \in k[x]$ (cf. [Bos04, Ch. 2, Korollar 7.6, p. 64]). This in turn means that

$$f(x) = (\alpha + \beta)y - \alpha\beta, \text{ i.e. } -\alpha = \beta \text{ and } \alpha^2 = f(x),$$

which contradicts to the fact that $f(x)$ is square-free in $k[x]$. So $y^2 - f(x)$ is absolutely irreducible since k is the full constant field of F (cf. proposition II.4.5). This implies that it defines an absolutely irreducible plane affine curve C and we are done by showing that it is nonsingular. The proof of the nonsingularity can be found in [Eng00, Ch. 3, theorem 3.3, p. 40].

We should note the following: $f(x)$ is square-free over k by [Sti93, Ch. VI, proposition 2.3(a), p. 194], and so it factorizes into pairwise distinct irreducible polynomials over k. Every such irreducible factor is separable since k is a finite field and so, $f(x)$ itself is separable, i.e. square-free over the algebraic closure.

2. By part (1) it suffices to show that the curve defined by (V.2) is hyperelliptic, which is done in [Sti93, Ch. VI, proposition 2.3(b), p. 194].

3. This is part (c) of [Sti93, Ch. VI, proposition 2.3, p. 194].

□

In even characteristic we have a similar result:

Theorem V.1.6. Assume that $\mathrm{char}(k) = 2$.

1. Let F/k be a hyperelliptic function field of genus $g > 1$. Then, F is the function field of a nonsingular plane affine curve given by an equation

$$y^2 + h(x)y = f(x) \tag{V.3}$$

with a monic nonzero polynomial $h(x) \in k[x]$ of degree $\leq g+1$ and a polynomial $f(x) \in k[x]$ of degree m, where $2g + 1 \leq m \leq 2g + 2$ such that any irreducible polynomial dividing h is a simple divisor of f.

2. Conversely, a nonsingular projective curve C/k that is birationally equivalent to an affine nonsingular curve of type (V.3) is a hyperelliptic curve of genus

$$g = \begin{cases} (m-1)/2 \text{ if } m \equiv 1 \bmod 2 \\ (m-2)/2 \text{ if } m \equiv 0 \bmod 2. \end{cases}$$

3. For a hyperelliptic curve C/k given by (V.3), we have

$$C \text{ is } \begin{cases} \text{imaginary quadratic, if } \deg(f) = 2g+1 \text{ and } \deg(h) \leq g \\ \text{real quadratic, if } \deg(f) \leq 2g+2 \text{ and } \deg(h) = g+1. \end{cases}$$

In the first case, the infinite place $\mathfrak{p}_\infty$ of $k(x)$ is ramified and in the second, it is splitting.

Proof. All 3 parts are proved in [Eng00, Ch. 3, theorem 3.5, p. 42]. □

In the imaginary quadratic situation of the theorem, we can transform (V.3) into the model chosen by Koblitz in [Kob89]. There, $f(x)$ is chosen to be monic. Unfortunately, we will lose our condition that $h(x)$ is monic under this transformation. Let a denote the leading coefficient of $f(x)$. Define $\tilde{f}(\tilde{x}) := a^{\deg(f)-1} f(\tilde{x})$, a polynomial in $\tilde{x} = \frac{x}{a}$ of degree $\deg(f)$ with leading coefficient $a^{\deg(f)+1}$, so $\tilde{f}(\tilde{x}) = f(x)$. Furthermore, define $\tilde{h}(\tilde{x}) := \frac{h(a\tilde{x})}{a^{(\deg(f)+1)/2}}$ a polynomial in $\tilde{x}$ of degree $\deg(h)$ with leading coefficient $a^{\deg(h)-(g+1)}$. We can choose a generator for $k(C)$ over $k(\tilde{x})$, namely $\tilde{y} := \frac{y}{a^{(\deg(f)+1)/2}}$. This yields

$$\tilde{y}^2 + \tilde{h}(\tilde{x})\tilde{y} = \frac{y^2 + \tilde{h}(\tilde{x}) a^{(\deg(f)+1)/2} y}{a^{\deg(f)+1}} = \frac{f(x)}{a^{\deg(f)+1}} = \frac{\tilde{f}(\tilde{x})}{a^{\deg(f)+1}} =: g(\tilde{x}),$$

where $g(\tilde{x})$ is a monic polynomial in $\tilde{x}$. So if we lose the condition that $h(x)$ is monic, we may assume $f(x)$ to be monic.

V.1.2 A Note on the Projective Closure of a Hyperelliptic Curve

Let C/k be an affine hyperelliptic curve given by a *Weierstraß equation* (cf. theorems V.1.5 and V.1.6)

$$y^2 + h(x)y = f(x) \text{ with } h(x) \text{ and } f(x) \in k[x], \tag{V.4}$$

where $2g+1 \leq \deg(f) \leq 2g+2, \deg(h) \leq g+1$ and $h(x)$ is monic. This affine curve is nonsingular by what we have done before. Let $\overline{C}$ be its projective closure in $\mathbb{P}^2$ in the sense of proposition II.4.3. We would like to emphasize that $\overline{C}$ is always singular as we will show below, but we know by section II.7 that there does always exist a nonsingular projective curve, birationally equivalent to $\overline{C}$, which is not contained in $\mathbb{P}^2$. The projective closure $\overline{C} \subseteq \mathbb{P}^2$ is in the focus of this subsection.

Let $P = (a : b : c) \in \mathbb{P}^2(k)$ be a k-rational point on $\overline{C}$ with $c \neq 0$. By definition of the 2-dimensional projective space we can write $P = (\frac{a}{c} : \frac{b}{c} : 1)$. So all k-rational points on $\overline{C}$ of the form $(a : b : c)$ with $c \neq 0$ are in fact "affine" points on C in terms of proposition II.4.2. We call these *finite points*. There is only one other k-rational point on $\overline{C}$, namely $\mathcal{O}_C := (0 : 1 : 0) \in \mathbb{P}^2(k)$, which certainly satisfies (V.4). This unique point $\mathcal{O}_C$ is called the *point at infinity*. Speaking in affine coordinates this means that

the set of all k-rational points has the following form

$$C(k) = \{(a, b) \in k \times k \mid b^2 + h(a)b = f(a)\} \cup \{\mathcal{O}_C\}.$$

It is easy to check that the homogenization to $\mathbb{P}^2$ of the Weierstraß equation (V.4) has a singularity at $\mathcal{O}_C$ by the Jacobian criterion (theorem II.5.12).

V.1.3 Weierstraß Points

Before we talk about a "group law" for hyperelliptic curves in the next section, we want to derive another important property from the fact that $k(C)/k(x)$ is of degree 2. Firstly, it is clear by what we have done before that $k(C) = k(x, y)$. Now, since the Galois group $G_{k(C)/k(x)}$ has order 2, we can choose the nontrivial automorphism in it and denote it by ω. All elements of $k(x)$ are fix under ω and ω is a homomorphism, so to get an explicit description of ω it suffices to calculate $\omega(y)$. For arbitrary characteristic of k, we know that C is given in the general form

$$y^2 + h(x)y = f(x) \text{ for polynomials } h(x), f(x) \in k[x],$$

where $\deg(h) \leq g + 1$ and $2g + 1 \leq \deg(f) \leq 2g + 2$ (recall that $h(x)$ can be assumed to be zero, if $\mathrm{char}(k) \neq 2$). By applying ω to this relation we conclude that

$$(\omega(y)^2 - y^2) + h(x)(\omega(y) - y) = 0,$$

which is equivalent to

$$(\omega(y) - y)(\omega(y) + y + h(x)) = 0.$$

Now, since ω is nontrivial, this is the same as to say

$$\omega(y) = -y - h(x).$$

Furthermore, it is clear that ω is an *involution* (i.e. $\omega^2 = \mathrm{id}$) as the order of $G_{k(C)/k(x)}$ equals 2.

For a k-rational point $P = (a, b) \in k \times k$ on the hyperelliptic curve C we can apply ω element-wise, i.e.

$$\omega(a, b) := (\omega(a), \omega(b)) = (a, -b - h(a))$$

and because of the equivalent steps above, it is immediate that $\omega(P) \in C(k)$, i.e. a k-rational point on C. ω is inverse to itself, so it actually defines a bijection on the k-rational points $C(k)$ of C.

Similarly, this can be done over the algebraic closure K of k. We have that $K(C) = K \cdot k(C)$ since the curve C is defined over k, so

$$K[C] = K[x, y]/\left(g \cdot k[x, y] \cdot K[x, y]\right) = K \cdot k[C]$$

(cf. [Sil86, Ch. I, remark 1.2, p. 6]). This means that $K(C)/k(C)$ is a constant field extension and, by [Sti93, Ch. III, proposition 6.1 + theorem 6.3, p. 101,103], we know that $K(C)/K$ is a hyperelliptic function field with full constant field K, same genus g and same transcendental element x such that $[K(C) : K(x)] = 2$. So, exactly as we have done before, we get an involution ω as above and we can sum up the results in a definition:

Definition V.1.7. Let C/k be a hyperelliptic curve defined over k. Then, there exists a bijective mapping $\omega : C(K) \to C(K)$ defined by $(a, b) \mapsto (a, -b - h(a))$, called *hyperelliptic involution*, that fulfills $\omega(\omega(P)) = P$ for all $P \in C$. The fixed points under this involution are called *Weierstraß points* (over K).

Before we begin to take a closer look at Weierstraß points, we would like to draw the attention to the norm and trace of the quadratic field extension $k(C)/k(x)$:

Remark V.1.8. Since $G_{k(C)/k(x)} = \{\mathrm{id}, \omega\}$, it follows immediately by [Bos04, Ch. 4, Satz 7.4, p. 196] that for $z \in k(C)$, we have

$$\mathrm{Tr}_{k(C)/k(x)}(z) = z + \omega(z) \in k(x) \text{ and } N_{k(C)/k(x)}(z) = z \cdot \omega(z) \in k(x).$$

There are certain results on Weierstraß points that are of particular interest to us:

Proposition V.1.9. Let C/k be a hyperelliptic curve of genus g defined over k and let K denote a fixed algebraic closure of k. We have:

1. The number of Weierstraß points on C is at least 1 and at most $(g-1)g(3g-1)$.
2. The Weierstraß points correspond to the ramified places of $K(C)/K(x)$. So, if C is imaginary quadratic, then *the* place lying over the infinite place $\mathfrak{p}_\infty$ of $K(x)$ is a Weierstraß point.
3. If $\mathrm{char}(k) \neq 2$, then C has precisely $2g + 2$ Weierstraß points.

Proof. 1. This is [Sal06, Ch. 14, corollary 2.52, p. 556].

2. See [Sal06, Ch. 14, corollary 2.72, p. 564].

3. See [Sal06, Ch. 14, corollary 2.74, p. 566].

□

This proposition only deals with Weierstraß points over an algebraic closure of k and the question arises, when Weierstraß points exist that are k-rational. Since we assumed that our ground field k has $q \geq 4g^2$ elements, we have seen that by the Hasse-Weil Bound, there exist (finitely many) places of degree 1 in $k(x)$. If one of those places ramifies in $k(C)$, we get the existence of k-rational Weierstraß points:

Proposition V.1.10. Let C/k be a hyperelliptic curve defined over k. Then, every place lying over a place of degree 1 in $k(x)$ that ramifies in $k(C)$ is a k-rational Weierstraß point.

In particular, if C is imaginary quadratic, then *the* place lying over the infinite place $\mathfrak{p}_\infty$ of $k(x)$ is a k-rational Weierstraß point.

Proof. See [Sal06, Ch. 14, theorem 2.67, p. 562]. □

Corollary V.1.11. Let C/k be an imaginary quadratic hyperelliptic curve defined over k of genus g. If g is even, then g is a *pole number of* $\mathfrak{p}_\infty$, i.e. it exists a function $z \in k(C)^*$ such that $\operatorname{div}(z)_\infty = g(\mathfrak{p}_\infty)$.

Proof. This is [Sal06, Ch. 14, theorem 2.67(iii), p. 562]. □

V.2 The Group Law for Hyperelliptic Curves

In contrast to the case of elliptic curves, where the Jacobian is isomorphic to the curve itself, the Jacobian of a hyperelliptic curve defines something new. And instead of calculating in the set of rational points as in the elliptic case, we need to work in some other group that is isomorphic to the Jacobian. That is what the word "for" in the title of this section tries to suggest. The group law we will define is not *on* the actual curve but *in* some other group that is isomorphic to the Jacobian of the curve.

V.2.1 Fractional Ideals

An essential notion needed to be able to define the mentioned group that should be isomorphic to the Jacobian of a given curve, is the notion of fractional ideals. We will introduce this notion in a more general setting, namely for an arbitrary integral domain $\mathcal{O}$ and its field of fractions F.

Definition V.2.1. An $\mathcal{O}$-submodule $\mathfrak{a}$ of F is called a *fractional ideal* of $\mathcal{O}$, if

$$r\mathfrak{a} \subseteq \mathcal{O} \text{ for some nonzero } r \in \mathcal{O}.$$

By taking $r = 1$ we see that all "ordinary" ideals are fractional ideals, which from now on are called *integral* ideals. Let $z = \frac{r}{s} \in F$, then

$$(z) := \mathcal{O}z \subseteq F$$

defines a fractional ideal since $s \cdot \mathcal{O}z \subseteq \mathcal{O}$, and is called *principal*. Furthermore, we define for a fractional ideal $\mathfrak{a}$ of $\mathcal{O}$:

$$\mathfrak{a}^{-1} := (\mathcal{O} : \mathfrak{a}) := \{z \in F \mid z\mathfrak{a} \subseteq \mathcal{O}\}.$$

Lemma V.2.2. Every finitely generated $\mathcal{O}$-submodule $\mathfrak{a}$ of F is a fractional ideal.

If, moreover, $\mathcal{O}$ is Noetherian, then the converse is also true.

Proof. Let $\mathfrak{a}$ be a finitely generated $\mathcal{O}$-submodule of F, say by $x_1, \ldots, x_n \in F$. For every $1 \leq i \leq n$ we can write $x_i = y_i r^{-1}$ where $y_i, r \in \mathcal{O}$, by extending the x_i's by their greatest common divisor. Then, $r\mathfrak{a} \subseteq \mathcal{O}$, i.e. $\mathfrak{a}$ is a fractional ideal.

Conversely, let $\mathfrak{a}$ be a fractional ideal and let $\mathcal{O}$ be Noetherian, i.e. it exists $0 \neq r \in \mathcal{O}$ such that $r\mathfrak{a} \subseteq \mathcal{O}$, $I := r\mathfrak{a}$ is an integral ideal of $\mathcal{O}$. This implies that we can write $\mathfrak{a} = r^{-1}I$. But since $\mathcal{O}$ is Noetherian, I is finitely generated and so is $\mathfrak{a}$. □

Remark V.2.3. Note that, in the proof of the lemma, we have shown that for every fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ there exists an integral ideal I of $\mathcal{O}$ such that

$$\mathfrak{a} = r^{-1}I \text{ for some nonzero } r \in \mathcal{O}.$$

Conversely, let I be an integral ideal of $\mathcal{O}$ and $0 \neq r \in \mathcal{O}$. Then, it is clear that $r^{-1}I$ is a fractional ideal of $\mathcal{O}$.

Definition V.2.4. An $\mathcal{O}$-submodule $\mathfrak{a}$ of F is called an *invertible ideal*, if there exists an $\mathcal{O}$-submodule $\mathfrak{b}$ of F such that $\mathfrak{ab} = \mathcal{O}$, where the product is defined as

$$\mathfrak{ab} := \left\{ \sum_{\text{finite}} x_i y_i \mid x_i \in \mathfrak{a}, y_i \in \mathfrak{b} \right\} \subseteq F,$$

which is clearly an $\mathcal{O}$-submodule of F.

Lemma V.2.5. Let $\mathfrak{a}$ be an invertible ideal of F with inverse $\mathfrak{b}$. Then, $\mathfrak{a}$ is a fractional ideal of $\mathcal{O}$, $\mathfrak{b}$ is unique and equal to $(\mathcal{O} : \mathfrak{a})$. In particular, it follows that $\mathfrak{b}$ is also invertible and therefore an invertible fractional ideal itself with inverse $\mathfrak{a}$.

Proof. We prove that $\mathfrak{b} = (\mathcal{O} : \mathfrak{a})$ from which the uniqueness of $\mathfrak{b}$ follows. We have

$$\mathfrak{b} \overset{\text{def.}}{\subseteq} (\mathcal{O} : \mathfrak{a}) \overset{\mathcal{O}=\mathfrak{ab}}{=} (\mathcal{O} : \mathfrak{a})\mathfrak{ab} \overset{\text{def.}}{\subseteq} \mathcal{O}\mathfrak{b} = \mathfrak{b}.$$

Now, we prove that $\mathfrak{a}$ is finitely generated. By definition we have that $\mathfrak{a}(\mathcal{O} : \mathfrak{a}) = \mathcal{O}$, so it exist $n \in \mathbb{N}$, $x_i \in \mathfrak{a}$ and $y_i \in (\mathcal{O} : \mathfrak{a})$ for $1 \leq i \leq n$ such that $\sum_i x_i y_i = 1$, i.e.

$$x = \sum_i (y_i x) x_i \text{ for all } x \in \mathfrak{a}.$$

Clearly, $y_i x \in \mathcal{O}$ which implies that $\mathfrak{a}$ is finitely generated, i.e. a fractional ideal by lemma V.2.2. □

Example V.2.6. Let (z) be a nonzero principal fractional ideal of $\mathcal{O}$ for $0 \neq z \in F$. Then (z) is invertible with inverse (z^{-1}) because

$$(z)(z^{-1}) = \left\{ \sum_{\text{finite}} x_i z y_i z^{-1} \mid x_i, y_i \in \mathcal{O} \right\} = \left\{ \sum_{\text{finite}} x \mid x \in \mathcal{O} \right\} = \mathcal{O}.$$

In particular, we see that $(1) = \mathcal{O}$ is an invertible fractional ideal.

With the multiplication defined in definition V.2.4, we can prove that the set of all invertible ideals forms an Abelian group.

Proposition V.2.7. Let $\mathcal{I}$ denote the set of all invertible fractional ideals of F. Then, $\mathcal{I}$ is an Abelian group with respect to multiplication.

Proof. Let $\mathfrak{a}, \mathfrak{b} \in \mathcal{I}$ be two invertible ideals of F, i.e. invertible fractional ideals of $\mathcal{O}$. Then $\mathfrak{ab}$ is an $\mathcal{O}$-submodule of F and it is invertible by the example. Therefore, $\mathfrak{ab}$ is an invertible fractional ideal. The associativity of the multiplication is trivial by definition. By lemma V.2.5, we already know that the inverse of an invertible ideal lies in $\mathcal{I}$. The neutral element of $\mathcal{I}$ is simply $\mathcal{O} = (1)$, which lies in $\mathcal{I}$ because of the example. The following is trivial:

$$\mathcal{O}\mathfrak{a} = \mathfrak{a}\mathcal{O} = \mathfrak{a}.$$

□

The interesting part is, that if $\mathcal{O}$ is a Dedekind domain, then $\mathcal{I}$ is equal to the set of all nonzero fractional ideals of $\mathcal{O}$.

Theorem V.2.8. If $\mathcal{O}$ is a Dedekind domain, then every nonzero fractional ideal of $\mathcal{O}$ is invertible. In particular, the nonzero fractional ideals of $\mathcal{O}$ form a group with respect to multiplication.

Proof. See [AM69, Ch. 9, theorem 9.8, p. 97]. □

V.2.2 The Ideal Class Group

In the tenor of the previous section, we want to continue the more general approach and take F/k as an arbitrary function field extending the rational function field $k(x)$ with full constant field k. We want to relate divisor classes to ideal classes and in order to do so, we firstly need a ring in F in which we have the notion of ideals. We borrow this idea from number theory where the designated ring is the integral closure of $\mathbb{Z}$ in the number field. The analogue of $\mathbb{Z}$ is $k[x]$ and we consider its integral closure $\mathcal{O}$ in F. The following lemma summarizes what we already know about the ring $\mathcal{O}$:

Lemma V.2.9.

1. $\mathcal{O}$ is the intersection of all valuation rings $\mathfrak{O}_P$ of F/k where P is a place of F/k extending some finite place $\mathfrak{p}$ of $k(x)/k$, i.e. $\mathcal{O} = \mathfrak{O}_S$ with $S := \{P \in \mathbb{P}_{F/k} \mid P \nmid \mathfrak{p}_\infty\}$ is a holomorphy ring, where $\mathfrak{p}_\infty$ denotes the infinite place of $k(x)/k$.
2. $\mathrm{Quot}(\mathcal{O}) = F$.
3. $\mathcal{O}$ is a Dedekind domain.
4. Every nonzero (fractional) ideal of $\mathcal{O}$ has a unique factorization as a product of prime ideals (with possibly negative multiplicities).
5. The nonzero fractional ideals of $\mathcal{O}$ form a group with respect to multiplication. Because of part (4), it is in fact the free Abelian group generated by the non-zero prime ideals of $\mathcal{O}$. It is called the *group of ideals of* $\mathcal{O}$ and is denoted by $\mathcal{I}(\mathcal{O})$.
6. Every nonzero prime ideal of $\mathcal{O}$ is a maximal ideal.

Proof. 1. This is theorem III.1.13 together with lemma III.1.12.

2. Use theorem III.1.13.

3. Clearly, we have that the integral domain $k[x]$ is a Dedekind domain: It is Noetherian since it is a PID, it has dimension 1 by theorem II.1.10 and it is integrally closed in its field of fractions $k(x)$, because if $z = f(x)/g(x) \in k(x)$ is integral over $k[x]$, there exists $a_{n-1}, \ldots, a_0 \in k[x]$ for $n \in \mathbb{N}$ such that

$$z^n + a_{n-1}z^{n-1} + \ldots + a_0 = 0,$$

i.e. $f(x)^n + g(x)a_{n-1}f(x)^{n-1} + \ldots + g(x)^n a_0 = 0$, which would imply that x is algebraic over k, a contradiction. Theorem II.7.5 now implies that $\mathcal{O}$ is a Dedekind domain.

4. See [AM69, Ch. 9, corollary 9.4, p. 95] for integral ideals of $\mathcal{O}$. Now, let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}$. By remark V.2.3, there exists an integral ideal I of $\mathcal{O}$ and a nonzero element $r \in \mathcal{O}$ such that $\mathfrak{a} = r^{-1}I$. Since I is integral, we can write down its unique factorization:

$$I = \prod_{\mathfrak{P} \in \mathrm{Spec}(\mathcal{O})} \mathfrak{P}^{m_{\mathfrak{P}}(I)},$$

where $m_{\mathfrak{P}}(I) \geq 0$ denotes the multiplicity of $\mathfrak{P}$ in the unique factorization of I. Furthermore, $(r) = \mathcal{O}r$ is an integral ideal and we also can write its factorization down:

$$(r) = \prod_{\mathfrak{P} \in \mathrm{Spec}(\mathcal{O})} \mathfrak{P}^{m_{\mathfrak{P}}((r))}.$$

Since $(r^{-1}) = (r)^{-1}$, this yields

$$\mathfrak{a} = \prod_{\mathfrak{P} \in \mathrm{Spec}(\mathcal{O})} \mathfrak{P}^{m_{\mathfrak{P}}(\mathfrak{a})}$$

where $m_{\mathfrak{P}}(\mathfrak{a}) := m_{\mathfrak{P}}(I) - m_{\mathfrak{P}}((r)) \in \mathbb{Z}$.

5. This is just theorem V.2.8.

6. This statement follows immediately from the trivial fact that an integral domain is of dimension 1 if and only if it contains a nonzero prime ideal and every nonzero prime ideal is maximal.

□

The last part of the lemma says that the set $\mathrm{Max}(\mathcal{O})$ of all maximal ideals of $\mathcal{O}$ is equal to $\mathrm{Spec}(\mathcal{O}) \setminus \{0\}$.

Proposition V.2.10. There is a one-to-one correspondence between the *finite* places of F/k (i.e. the places not extending the infinite place $\mathfrak{p}_\infty$ of $k(x)/k$) and the maximal

(resp. nonzero prime) ideals of $\mathcal{O}$ given by

$$\begin{aligned}\left\{P \in \mathbb{P}_{F/k} \mid P \nmid \mathfrak{p}_\infty\right\} &\xleftrightarrow{1:1} \operatorname{Max}(\mathcal{O}) \\ P &\longmapsto P \cap \mathcal{O},\end{aligned}$$

Moreover, we have an isomorphism for every $P \in \left\{P \in \mathbb{P}_{F/k} \mid P \nmid \mathfrak{p}_\infty\right\}$, namely

$$\mathcal{O}/(P \cap \mathcal{O}) \cong F_P \text{ defined by } x + (P \cap \mathcal{O}) \mapsto x + P.$$

Proof. See [Sti93, Ch. III, proposition 2.9, p. 70]. □

Because of this correspondence, $\mathcal{I}(\mathcal{O})$ is the (multiplicatively written) free Abelian group generated by the maximal ideals $P \cap \mathcal{O}$ and we can write down the unique factorization of $\mathfrak{a} \in \mathcal{I}(\mathcal{O})$ in the form

$$\mathfrak{a} = \prod_{P \nmid \mathfrak{p}_\infty} (P \cap \mathcal{O})^{m_P(\mathfrak{a})},$$

where $m_P(\mathfrak{a}) := m_{P \cap \mathcal{O}}(\mathfrak{a})$. This fact allows us to associate to every ideal $\mathfrak{a} \in \mathcal{I}(\mathcal{O})$ a divisor of F/k, namely

$$\operatorname{div}(\mathfrak{a}) := \sum_{P \nmid \mathfrak{p}_\infty} m_P(\mathfrak{a})(P) \in \operatorname{Div}(F).$$

It follows immediately from the definition that an ideal $\mathfrak{a} \in \mathcal{I}(\mathcal{O})$ is integral if and only if its divisor is effective. Also, it is clear that every divisor of F/k that does not contain an *infinite* place (i.e. a place of F/k that extends the infinite place $\mathfrak{p}_\infty$ of $k(x)/k$) is a divisor of some ideal $\mathfrak{a} \in \mathcal{I}(\mathcal{O})$. So an effective divisor $D \in \operatorname{Div}(F)$ does not contain an infinite place if and only if $D = \operatorname{div}(\mathfrak{a})$ for some integral ideal $\mathfrak{a} \in \mathcal{I}(\mathcal{O})$. We denote the subgroup of $\operatorname{Div}(F)$ consisting of those divisors that do not contain an infinite place by $\mathfrak{I}(\mathcal{O})$, i.e. divisors that correspond to ideals $\mathfrak{a} \in \mathcal{I}(\mathcal{O})$. Also, we can associate a divisor to a single element $z \in F$ by taking the divisor of its principal ideal, that is $\sum_{P \nmid \mathfrak{p}_\infty} m_P(z)(P)$. Then, we denote the subgroup of $\mathfrak{I}(\mathcal{O})$ consisting of all divisors of principal ideals by $\operatorname{Princ}(\mathcal{O})$. Finally, this allows us to define the ideal class group of $\mathcal{O}$:

Definition V.2.11. Let F/k be a function field extending the rational function field $k(x)$ with full constant field k and let $\mathcal{O}$ be the integral closure of $k[x]$ in F. We call the Abelian group

$$\operatorname{Cl}(\mathcal{O}) := \mathfrak{I}(\mathcal{O})/\operatorname{Princ}(\mathcal{O})$$

the *ideal class group of* $\mathcal{O}$. The number of elements in $\operatorname{Cl}(\mathcal{O})$ is called the *ideal class number*.

At the end of this section, we would like to make a note about the definition of a divisor of a principal ideal. For a nonzero element $z \in F$, one would naturally expect

that the divisor of the principal ideal (z) is equal to the principal divisor $\mathrm{div}(z)$ - infinite places. This is in fact true:

Remark V.2.12. The multiplicity of a maximal ideal $P \cap \mathcal{O}$ in the factorization of a principal ideal defines a discrete valuation of F/k, which is in fact equal to v_P, by putting $m_P(0) := \infty$. In particular, we have for $0 \neq z \in F$ that $\mathrm{div}(z) = \sum_{P \nmid \mathfrak{p}_\infty} m_P(z)(P) + \sum_{P|\mathfrak{p}_\infty} v_P(z)(P)$.

Proof. Let $P \cap \mathcal{O}$ be a maximal ideal of $\mathcal{O}$, given by some finite place P of F/k. Since the multiplicity of P in the factorization of some ideal can never be ∞, we have that $m_P(z) = \infty$ if and only if $z = 0$. If $z, w \in F$ are nonzero, then

$$\prod_{Q \nmid \mathfrak{p}_\infty} (Q \cap \mathcal{O})^{m_Q(zw)} = (zw) = (z)(w) = \prod_{Q \nmid \mathfrak{p}_\infty} (Q \cap \mathcal{O})^{m_Q(z)+m_Q(w)},$$

i.e. $m_P(zw) = m_P(z) + m_P(w)$. Furthermore, we have

$$\prod_{Q \nmid \mathfrak{p}_\infty} (Q \cap \mathcal{O})^{m_Q(z+w)} = (z+w) = (z,w) = \prod_{Q \nmid \mathfrak{p}_\infty} (Q \cap \mathcal{O})^{m_Q(z)} + \prod_{Q \nmid \mathfrak{p}_\infty} (Q \cap \mathcal{O})^{m_Q(w)}.$$

By putting $m_Q := \min\{m_Q(z), m_Q(w)\}$, it follows:

$$\prod_{Q \nmid \mathfrak{p}_\infty} (Q \cap \mathcal{O})^{m_Q(z+w)} \subseteq \prod_{Q \nmid \mathfrak{p}_\infty} (Q \cap \mathcal{O})^{m_Q},$$

i.e. $m_P(z+w) \geq m_P = \min\{m_P(z), m_P(w)\}$. Now, choose a uniformizer $t \in F$ for P. If $t \in \mathcal{O}$, then $P \cap \mathcal{O} = (t)$, i.e. $m_P(t) = 1$. If $t \notin \mathcal{O}$, then $t^{-1} \in \mathcal{O}$ as $\mathrm{Quot}(\mathcal{O}) = F$. On the other hand, we know that $\mathfrak{O}_P$ is a Dedekind domain and so we can form the inverse ideal $P^{-1} = t^{-1}\mathfrak{O}_P$ of P. This means that $t^{-1} \in P^{-1} \cap \mathcal{O}$ but $P^{-1} \cap \mathcal{O}$ certainly is a fractional ideal of $\mathcal{O}$ with $(P \cap \mathcal{O})(P^{-1} \cap \mathcal{O}) = \mathcal{O}$, i.e. $P^{-1} \cap \mathcal{O} = (P \cap \mathcal{O})^{-1}$. This in turn implies:

$$(t)^{-1} = (t^{-1}) = (P \cap \mathcal{O})^{-1},$$

i.e. $m_P(t) = 1$. Also, for $a \in k^* \subseteq \mathcal{O}$ we have $(a) = \mathcal{O}$, i.e. $m_P(a) = 0$. This shows that m_P defines a discrete valuation of F/k, and since $m_P(t) = 1 = v_P(t)$ it follows that $m_P(z) = v_P(z)$ for all $z \in F$. □

V.2.3 The Ideal Class Number and the Regulator

Let F/k be a function field extending the rational function field $k(x)$ with full constant field k and let $\mathcal{O}$ be the integral closure of $k[x]$ in F. One of our goals in this section is to show that the ideal class number is finite in the case where k is finite.

Let $P_{\infty_1}, \ldots, P_{\infty_r}$ be the distinct extensions of the infinite place $\mathfrak{p}_\infty$ of $k(x)/k$. By theorem III.1.10 we know that $\mathrm{div}_{k(x)}(x) = (\mathfrak{p}_x) - (\mathfrak{p}_\infty)$, so $\mathrm{div}_{k(x)}(x)_\infty = (\mathfrak{p}_\infty)$. By section III.3.1 this means

$$\mathrm{div}_F(x)_\infty = \mathrm{Con}_{F/k(x)}(\mathfrak{p}_\infty) = \sum_{i=1}^{r} e_i \cdot (P_{\infty_i}), \text{ where } e_i := e(P_{\infty_i}|\mathfrak{p}_\infty).$$

This shows that $\mathrm{div}_F(x)_\infty$ is an element of $\mathrm{Div}_\infty(\mathcal{O}) := \mathbb{Z}(P_{\infty_1}) + \ldots + \mathbb{Z}(P_{\infty_r})$. We denote the set of all degree zero divisors of $\mathrm{Div}_\infty(\mathcal{O})$ by $\mathrm{Div}^0_\infty(\mathcal{O})$.

Example V.2.13. Let $F = k(x, y)$ be a hyperelliptic function field over k. Recall that we can always assume that the infinite place $\mathfrak{p}_\infty$ of $k(x)$ is not inert, i.e. if P is a place of F lying over $\mathfrak{p}_\infty$, then $\deg(P) = \deg(\mathfrak{p}_\infty) = 1$ (cf. section V.1). So in this case, there is always a divisor of degree 1 in $\mathrm{Div}_\infty(\mathcal{O})$.

Since we are mostly interested in hyperelliptic curves, *we restrict the general case by requiring the existence of a divisor D_1 of degree 1 in $Div_\infty(\mathcal{O})$.*

Lemma V.2.14. Let F/k be a function field extending $k(x)$ and let $\mathcal{O}$ be the integral closure of $k[x]$ in F. Assume that it exists a divisor $D_1 \in \mathrm{Div}_\infty(\mathcal{O})$ of degree 1. Then the map

$$\pi_\mathcal{O} : \mathrm{Div}^0(F/k) \longrightarrow \mathfrak{I}(\mathcal{O}) \text{ defined by } \sum_{P \in \mathbb{P}_{F/k}} n_P(P) \longmapsto \sum_{P \nmid \mathfrak{p}_\infty} n_P(P)$$

is an epimorphism.

Proof. The fact that $\pi_\mathcal{O}$ is a homomorphism is trivial and so we only need to show that it is surjective. We already know that every element of $\mathfrak{I}(\mathcal{O})$ is of the form $\sum_{P \nmid \mathfrak{p}_\infty} n_P(P)$ (which does not necessarily have degree 0). Define the following divisor of F/k:

$$D_0 := \sum_{P \nmid \mathfrak{p}_\infty} n_P(P) - \left(\sum_{P \nmid \mathfrak{p}_\infty} n_P \deg(P) \right) D_1.$$

This divisor clearly has degree 0 and we have

$$\pi_\mathcal{O}(D_0) = \sum_{P \nmid \mathfrak{p}_\infty} n_P(P),$$

so $\pi_\mathcal{O}$ is surjective. □

Definition V.2.15. We define the *regulator* of $\mathcal{O}$ as

$$R(\mathcal{O}) := |\mathcal{R}(\mathcal{O})|$$

where $\mathcal{R}(\mathcal{O}) := \mathrm{Div}^0_\infty(\mathcal{O}) / \left(\mathrm{Div}^0_\infty(\mathcal{O}) \cap \mathrm{Princ}(F) \right)$.

As mentioned above, we want to show that the ideal class number is finite, if k is finite. We will see that the regulator of $\mathcal{O}$ is finite in this case, too.

Theorem V.2.16. Let F/k be a function field extending $k(x)$ and let $\mathcal{O}$ be the integral closure of $k[x]$ in F. Assume that it exists a divisor $D_1 \in \mathrm{Div}_\infty(\mathcal{O})$ of degree 1. Then:

$$\mathrm{Pic}^0(F) \cong \mathrm{Cl}(\mathcal{O}) \times \mathcal{R}(\mathcal{O}).$$

In particular, if k is finite then the ideal class number and the regulator of $\mathcal{O}$ are finite.

Proof. Let $\iota : \mathrm{Div}^0_\infty(\mathcal{O}) \hookrightarrow \mathrm{Div}^0(F)$ be the restriction of $\mathrm{id} : \mathrm{Div}^0(F) \to \mathrm{Div}^0(F)$ to $\mathrm{Div}^0_\infty(\mathcal{O})$. The map $\pi_\mathcal{O}$ in lemma V.2.14 is surjective and the kernel consists of precisely those divisors of degree 0 containing only infinite places, i.e. $\ker(\pi_\mathcal{O}) = \mathrm{Div}^0_\infty(\mathcal{O})$. Therefore we have the short exact sequence

$$0 \to \mathrm{Div}^0_\infty(\mathcal{O}) \xrightarrow{\iota} \mathrm{Div}^0(F) \xrightarrow{\pi_\mathcal{O}} \mathfrak{I}(\mathcal{O}) \to 0.$$

By remark V.2.12 we have $\pi_\mathcal{O}(\mathrm{Princ}(F)) = \mathrm{Princ}(\mathcal{O})$ and we can restrict the sequence to $\mathrm{Princ}(F)$ resp. $\mathrm{Princ}(\mathcal{O})$:

$$0 \to \mathrm{Div}^0_\infty(\mathcal{O}) \cap \mathrm{Princ}(F) \xrightarrow{\iota} \mathrm{Princ}(F) \xrightarrow{\pi_\mathcal{O}} \mathrm{Princ}(\mathcal{O}) \to 0.$$

So, we have the following commutative diagram of Abelian groups (i.e. $\mathbb{Z}$-modules):

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Div}^0_\infty(\mathcal{O}) \cap \mathrm{Princ}(F) & \longrightarrow & \mathrm{Princ}(F) & \xrightarrow{\pi_\mathcal{O}} & \mathrm{Princ}(\mathcal{O}) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Div}^0_\infty(\mathcal{O}) & \longrightarrow & \mathrm{Div}^0(F) & \xrightarrow{\pi_\mathcal{O}} & \mathfrak{I}(\mathcal{O}) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \mathcal{R}(\mathcal{O}) & & \mathrm{Pic}^0(F) & & \mathrm{Cl}(\mathcal{O}) & &
\end{array}$$

The snake lemma (cf. [AM69, Ch. 2, proposition 2.10, p. 23]) yields the short exact sequence

$$0 \to \mathcal{R}(\mathcal{O}) \to \mathrm{Pic}^0(F) \xrightarrow{\beta} \mathrm{Cl}(\mathcal{O}) \to 0, \tag{V.5}$$

where $\beta : \mathrm{Pic}^0(F) \to \mathrm{Cl}(\mathcal{O})$ is defined by $D + \mathrm{Princ}(F) \mapsto \pi_\mathcal{O}(D) + \mathrm{Princ}(\mathcal{O})$. Then, we define a homomorphism $\tau : \mathrm{Cl}(\mathcal{O}) \to \mathrm{Pic}^0(F)$ as follows:

1. Let $\mathrm{div}(\mathfrak{a}) + \mathrm{Princ}(\mathcal{O}) \in \mathrm{Cl}(\mathcal{O})$, i.e. $\mathrm{div}(\mathfrak{a}) \in \mathfrak{I}(\mathcal{O})$. This means that there exists a divisor $D \in \mathrm{Div}^0(F)$ such that $\pi_\mathcal{O}(D) = \mathrm{div}(\mathfrak{a})$.

2. The image of D in $\mathrm{Pic}^0(C)$ is the image of $\mathrm{div}(\mathfrak{a}) + \mathrm{Princ}(\mathcal{O})$ under τ, i.e.

$$\tau(\mathrm{div}(\mathfrak{a}) + \mathrm{Princ}(\mathcal{O})) := D + \mathrm{Princ}(F).$$

It is easily seen that τ is a well-defined homomorphism with the additional property that

$$\beta(\tau(\mathrm{div}(\mathfrak{a}) + \mathrm{Princ}(\mathcal{O}))) = \beta(D + \mathrm{Princ}(F)) = \mathrm{div}(\mathfrak{a}) + \mathrm{Princ}(\mathcal{O}).$$

This shows that the exact sequence (V.5) *splits* (cf. [Eis99, Ch. 0, p. 16]) and we have

$$\mathrm{Pic}^0(F) \cong \mathcal{R}(\mathcal{O}) \times \mathrm{Cl}(\mathcal{O}).$$

□

Corollary V.2.17. Let C/k be an imaginary quadratic hyperelliptic curve given by (V.4) and let $\mathcal{O}$ denote the integral closure of $k[x]$ in $k(C)$. Then,

$$\mathrm{Pic}^0(C) \cong \mathrm{Cl}(\mathcal{O}).$$

Proof. Since C/k is imaginary quadratic, the infinite place $\mathfrak{p}_\infty$ of $k(x)/k$ is ramified in $k(C)$ and if P_∞ denotes the unique place in $k(C)$ lying above $\mathfrak{p}_\infty$, we have $\mathrm{Div}_\infty(\mathcal{O}) = \mathbb{Z}(P_\infty)$. So the only divisor of degree 0 in $\mathrm{Div}_\infty(\mathcal{O})$ is the zero divisor, i.e. $\mathrm{Div}^0_\infty(\mathcal{O}) = \{0\}$. Hence, $\mathcal{R}(\mathcal{O}) = \{0\}$. By example V.2.13 we know that the assumptions of theorem V.2.16 are met. So we can apply the theorem to get $\mathrm{Pic}^0(C) \cong \mathrm{Cl}(\mathcal{O})$. □

The situation for real quadratic hyperelliptic curves is different, but if there exists a finite ramified place $\mathfrak{p}$ of $k(x)/k$ of degree 1 with uniformizer $p \in k[x]$, it is possible to convert the real into an imaginary quadratic representation.

Lemma V.2.18. Let C/k be a real quadratic hyperelliptic curve given by (V.4). Assume that there exists a finite ramified place $\mathfrak{p}$ of $k(x)/k$ of degree 1 with uniformizer $p \in k[x]$. Then $k(C)$ is an imaginary quadratic hyperelliptic function field over $k(\frac{1}{p})$.

Proof. By proposition III.1.4 we have

$$\mathrm{div}(\frac{1}{p})_\infty = \mathrm{div}(p)_0 = e(P|\mathfrak{p})v_\mathfrak{p}(p)(P) = 2(P),$$

i.e. $[k(C) : k(\frac{1}{p})] = \deg(\mathrm{div}(\frac{1}{p})_\infty) = 2$. In this representation, the infinite place of $k(\frac{1}{p})/k$ is ramified. □

V.2.4 Representatives of Ideal Classes

From now on, we specialize to the case of hyperelliptic curves C/k given by (V.4) and denote the integral closure of $k[x]$ in $k(C)$ by $\mathcal{O}$. We want to calculate in the ideal class group introduced in the previous section. For cryptographic purposes we need an explicit arithmetic that we can use in later algorithms. To this end, it is necessary to have concrete generators of the prime ideals of $\mathcal{O}$. Such generators can be provided, if certain integral bases are known.

Integral Bases and the Hyperelliptic Involution

Proposition V.2.19. Let $\mathfrak{p}$ be a finite place of $k(x)/k$, $\mathfrak{O}_\mathfrak{p}$ its valuation ring and $\overline{\mathfrak{O}_\mathfrak{p}}$ the integral closure of $\mathfrak{O}_\mathfrak{p}$ in $k(C)$. Then $\{1, y\}$ is a local integral basis *at* $\mathfrak{p}$, i.e.

$$\overline{\mathfrak{O}_\mathfrak{p}} = \mathfrak{O}_\mathfrak{p} + y\mathfrak{O}_\mathfrak{p}.$$

In particular, we have $\mathcal{O} = k[C]$.

Proof. This is [Eng00, Ch. 3, proposition 3.8, p. 47]. □

Knowing that $\{1, y\}$ is a local integral basis at the finite place $\mathfrak{p}$, we can apply Kummer's theorem (see theorem III.3.14) on $k(C)$, whereas the minimal polynomial of y is given by (V.4). Together with the fact that $k(x)_\mathfrak{p} \cong k[x]/(p)$ by theorem III.1.10 where $p \in k[x]$ is the uniformizer for $\mathfrak{p}$ we immediately deduce the following (cf. [Eng00, Ch. 3, proposition 3.10, p. 48]):

Proposition V.2.20. Let $\mathfrak{p}$ be a finite place of $k(x)/k$ with uniformizer $p \in k[x]$. Consider the roots of

$$Y^2 + h(x)Y - f(x) \pmod{(p)}$$

(by (V.4)), a polynomial in $k(x)_\mathfrak{p}[Y]$, in the residue class field $k(x)_\mathfrak{p} \cong k[x]/(p)$.

1. If there is no root, then $\mathfrak{p}$ is inert, and the only extension P of $\mathfrak{p}$ satisfies $p\mathcal{O} = P \cap \mathcal{O}$.
2. If there is a double root $b + (p)$, then $\mathfrak{p}$ is ramified, and the unique extension P of $\mathfrak{p}$ satisfies $p\mathcal{O} = (P \cap \mathcal{O})^2$ with $P \cap \mathcal{O} = (p, y - b) = p\mathcal{O} + (y - b)\mathcal{O}$.
3. If there are two distinct roots $b + (p)$ and $b' + (p) = -b - h(x) + (p)$, then $\mathfrak{p}$ is splitting, and the extensions P_1 and P_2 of $\mathfrak{p}$ satisfy $p\mathcal{O} = (P_1 \cap \mathcal{O})(P_2 \cap \mathcal{O})$ with $P_1 \cap \mathcal{O} = (p, y - b)$ and $P_2 \cap \mathcal{O} = (p, y - b')$.

In particular, any prime ideal of $\mathcal{O}$ is generated by at most two elements.

Remark V.2.21. In terms of the hyperelliptic involution, the theorem yields:

1. If $\mathfrak{p}$ is inert, then $P \cap \mathcal{O} = (p) = (\omega(p))$.
2. If $\mathfrak{p}$ is ramified, then $P \cap \mathcal{O} = (p, y - b) = (\omega(p), \omega(y - b))$.
3. If $\mathfrak{p}$ is splitting, then $P_2 \cap \mathcal{O} = (\omega(p), \omega(y - b))$.

Proof. 1. This follows as $p \in k[x]$.

2. Since $b + (p)$ is a double root in $k(x)_\mathfrak{p}$, we have

$$(Y - b)^2 \equiv Y^2 + h(x)Y - f(x) \pmod{(p)}.$$

Then, by Kummer's theorem, we know that $y - b \in P$. But by proposition V.1.9, this means that $\omega(y - b) = y - b$ since $\mathfrak{p}$ is ramified.

3. By the theorem, there exists $g \in k[x]$ such that $b' + b + h(x) = p \cdot g \in (p) \subseteq p\mathcal{O}$. Furthermore, we have $\omega(y - b) = -y - h(x) - b$ since $b \in k[x]$. Together, this means

$$(p, \omega(y - b)) = (p, -y - h(x) - b) = (p, -y + b') = (p, y - b') = P_2 \cap \mathcal{O}.$$

□

It is possible to extend the hyperelliptic involution to *finite* divisors (i.e. divisors not containing infinite places):

Definition V.2.22. Let $\mathfrak{p}$ be a finite place of $k(x)/k$ and let P_1, P_2 be the (not necessarily distinct) places of $k(C)/k$ extending it.

1. If $\mathfrak{p}$ is inert or ramified, then $P := P_1 = P_2$, and we define $\omega(P) := P$.

2. If $\mathfrak{p}$ is splitting, then $P_1 \neq P_2$, and we define $\omega(P_1) := P_2$ resp. $\omega(P_2) := P_1$.

It is trivial that, by this definition, ω is an involution on the set of finite places. This definition can be additively extended to $\mathfrak{I}(\mathcal{O})$.

Having defined it for finite divisors, we can also define it for fractional ideals:

Definition V.2.23. Let $P \cap \mathcal{O}$ be a prime ideal of $\mathcal{O}$ for some finite place P of $k(C)/k$. We define

$$\omega(P \cap \mathcal{O}) := \omega(P) \cap \mathcal{O}.$$

Since every fractional ideal is the product of prime ideals (with possibly negative multiplicities), we can extend this definition multiplicatively to $\mathcal{I}(\mathcal{O})$. It is clear that, in this way, ω is an involution on $\mathcal{I}(\mathcal{O})$.

As an immediate consequence of proposition V.2.20, we have the following result:

Corollary V.2.24. Let P be a place of $k(C)/k$ extending some finite place $\mathfrak{p}$ of $k(x)/k$. Then we have for every $z \in k(C)$:

$$v_{\omega(P)}(z) = v_P(\omega(z)).$$

Proof. Consider the prime ideal $P \cap \mathcal{O}$ of $\mathcal{O}$. By theorem V.2.20 we know that this ideal is generated by two elements, say $P \cap \mathcal{O} = (r, s)$. Consequently, we know that $\omega(P) \cap \mathcal{O} = (\omega(r), \omega(s))$ by remark V.2.21. Now, if $z \in \mathcal{O}$ then we have the relation

$$z \in \omega(P) \iff \omega(z) \in \omega(\omega(P)) = P.$$

By considering the generators of $P \cap \mathcal{O}$ and $\omega(P) \cap \mathcal{O}$ it follows immediately that $v_{\omega(P)}(z) = v_P(\omega(z))$. This in turn implies the result for $k(C)$ since it is the field of fraction of $\mathcal{O}$.

Another proof of this can be found in [Sti93, Ch. III, lemma 5.2, p. 89]. □

Principal Divisors

Recall from section V.2.3 that

$$\pi_{\mathcal{O}}(\mathrm{Princ}(C)) = \mathrm{Princ}(\mathcal{O}), \text{ i.e. } \mathrm{div}(z\mathcal{O}) = \pi_{\mathcal{O}}(\mathrm{div}(z))$$

for any $z \in k(C)$. Our first aim is to show that a similar result exists for finitely generated ideals, namely that it is possible to deduce the divisor of a finitely generated ideal from the divisors of its generators.

Definition V.2.25. We define the *greatest common divisor* of two divisors of $\mathrm{Div}(C)$ as

$$\gcd\left(\sum m_P(P), \sum n_P(P)\right) := \sum \min(m_P, n_P)(P).$$

Proposition V.2.26. For $r, s \in \mathcal{O}$, we have

$$\mathrm{div}(r\mathcal{O} + s\mathcal{O}) = \gcd(\pi_{\mathcal{O}}(\mathrm{div}(r)), \pi_{\mathcal{O}}(\mathrm{div}(s))) = \pi_{\mathcal{O}}(\gcd(\mathrm{div}(r), \mathrm{div}(s))).$$

So, the divisor of a finitely generated ideal is the image of the greatest common divisor of the divisors of its generators under $\pi_{\mathcal{O}}$.

Proof. See [Eng00, Ch. 3, proposition 3.12, p. 49]. □

This proposition actually concerns all ideals of $\mathcal{O}$ since $\mathcal{O}$ is Noetherian, which means that every integral ideal is finitely generated and so is every fractional ideal of $\mathcal{O}$ by remark V.2.3 (see also lemma V.2.2). We know that the divisor of an ideal of $\mathcal{O}$ determines its decomposition into prime ideals, so we have found an easy way to decompose an ideal of $\mathcal{O}$. In certain situations, we can write down the explicit form of a divisor of a principal ideal:

Proposition V.2.27. Let $a, b \in k[x]$ and let P denote the extention of a finite place $\mathfrak{p}$ of $k(x)/k$.

1. If $a = \prod_{\mathfrak{p}} p^{v_p(a)}$ with $p \in k[x]$ irreducible, $v_p := v_p(a) \geq 0$ and $\mathfrak{p}$ the place of $k(x)/k$ with uniformizer p, then

$$\mathrm{div}(a\mathcal{O}) = \sum_{\mathfrak{p} \text{ inert}} v_p(P) + \sum_{\mathfrak{p} \text{ ram.}} 2v_p(P) + \sum_{\mathfrak{p} \text{ spl.}} (v_p(P) + v_p(\omega(P))).$$

2. If $N_{k(C)/k(x)}(y - b) = \prod_{\mathfrak{p}} p^{v_p}$ with $p \in k[x]$ irreducible, $v_p \geq 0$ and $\mathfrak{p}$ the place of $k(x)/k$ with uniformizer p, then $v_p > 0$ implies that $\mathfrak{p}$ is not inert and that $b + (p)$ is a root of $Y^2 + hY - f \pmod p$. If $\mathfrak{p}$ is ramified, then $v_p \in \{0, 1\}$. Let P be such that $P \cap \mathcal{O} = (p, y - b)$. Then:

$$\mathrm{div}((y - b)\mathcal{O}) = \sum_{\mathfrak{p}} v_p(P).$$

3. If, in the situation of part 2, $a \mid N_{k(C)/k(x)}(y - b)$ with $a = \prod_{\mathfrak{p}} p^{v_p(a)}$ as in part 1, then

$$\mathrm{div}((a, y - b)\mathcal{O}) = \sum_{\mathfrak{p}} v_p(a)(P) \text{ with } \deg(\mathrm{div}((a, y - b)\mathcal{O})) = \deg(a).$$

Proof. Parts 1 and 2 are proved in [Eng00, Ch. 3, proposition 3.13, p. 49]. For the third part, we apply proposition V.2.26:

$$\mathrm{div}((a, y - b)\mathcal{O}) = \gcd(\mathrm{div}(a\mathcal{O}), \mathrm{div}((y - b)\mathcal{O})) = \sum_{\mathfrak{p}} v_p(a)(P).$$

Then, it is clear that

$$\deg(\mathrm{div}((a, y-b)\mathcal{O})) = \sum_{\mathfrak{p} \text{ inert}} 0 + \sum_{\mathfrak{p} \text{ ram.}} v_p(a)\deg(p) + \sum_{\mathfrak{p} \text{ spl.}} v_p(a)\deg(p) = \deg(a),$$

since $\deg(P) = f \cdot \deg(\mathfrak{p})$, where f denotes the inertia degree. □

The Unique Representation of Integral Ideals of $\mathcal{O}$

We state the main result of this section, which is a generalization of theorem V.2.20:

Theorem V.2.28. Let C/k be a hyperelliptic curve given by (V.4) and let $\mathfrak{a}$ be an integral ideal of $\mathcal{O}$. Then there exist unique elements $a, b, d \in k[x]$ with a, d monic, $\deg(b) < \deg(a)$ and $a \mid N_{k(C)/k(x)}(y-b) = b^2 + bh(x) - f(x)$ such that

$$\mathfrak{a} = (d)(a, y-b).$$

We will give a constructive proof based on [Eng00, Ch. 3, theorem 3.14, p. 50], which will be the starting point for later algorithms. Our proof will be much more detailed though. But before we are able to do so, we need to do some preliminary work, beginning with the *extended Euclidean algorithm* to find the greatest common divisor of two polynomials:

Algorithm 2 Extended Euclidean Algorithm

INPUT: Two polynomials $f, g \in k[x]$.
OUTPUT: Polynomials (u, v, d) such that $u \cdot f + v \cdot g = d$ with $d = \gcd(f, g)$.

1: $u \leftarrow 1, d \leftarrow f, v_1 \leftarrow 0$ and $v_3 \leftarrow g$
2: **repeat**
3: $\quad r \leftarrow (d \bmod v_3)$ and $q \leftarrow (d-r)/v_3$ {this is ED=Euclidean Division}
4: $\quad t \leftarrow u - v_1 \cdot q, u \leftarrow v_1, d \leftarrow v_3, v_1 \leftarrow t$ and $v_3 \leftarrow r$
5: **until** $v_3 = 0$
6: $v \leftarrow (d - f \cdot u)/g$
7: **return** (u, v, d)

Proof of algorithm 2. See [Coh96, Ch. 3, algorithm 3.2.2, p. 113]. □

Remark V.2.29. Clearly, by applying the extended Euclidean algorithm recursively, it is possible to compute the greatest common divisor of more than two polynomials $f_1, \ldots, f_n$ with corresponding representation. We calculate

$$f := \gcd(f_1, \ldots, f_{n-1}) = u_1 f_1 + \cdots + u_{n-1} f_{n-1}$$

and apply the algorithm to f and f_n:

$$\gcd(f, f_n) = uf + vf_n.$$

This in turn yields

$$\gcd(f_1, \ldots, f_n) = \gcd(f, f_n) = (uu_1)f_1 + \cdots + (uu_{n-1})f_{n-1} + vf_n.$$

Also, we will need the concept of the norm of an integral ideal which is defined with the help of the following lemma:

Lemma V.2.30. If $\mathfrak{a}$ is an integral ideal of $\mathcal{O}$, then $\mathfrak{a}\cdot\omega(\mathfrak{a})$ is a principal ideal, generated by an element of $k[x]$.

Proof. See [Eng00, Ch. 3, proposition 3.15, p. 51]. □

Definition V.2.31. Let $\mathfrak{a}$ be an integral ideal such that $\mathfrak{a}\cdot\omega(\mathfrak{a})$ is generated by $a \in k[x]$ (cf. lemma V.2.30). We define

$$N(\mathfrak{a}) := \mathfrak{a} \cdot \omega(\mathfrak{a}) \cap k[x] = ak[x]$$

and call it the *norm of* $\mathfrak{a}$.

If an integral ideal is of a special form, we can immediately write down its norm:

Lemma V.2.32. 1. If $\mathfrak{a} = (a, y - b)$ with $a, b \in k[x]$ and $a \mid b^2 + bh - f$, then $N(\mathfrak{a}) = ak[x]$.

2. If $\mathfrak{b} = (d)$ with $d \in k[x]$, then $N(\mathfrak{b}) = d^2k[x]$.

Proof. This is [Eng00, Ch. 3, lemma 3.16, p. 51]. □

We are finally able to prove the main result:

Proof of theorem V.2.28. **Existence.** Firstly, we prove the existence for prime ideals $P \cap \mathcal{O}$ of $\mathcal{O}$. We know that P lies above the unique finite place $\mathfrak{p} := P \cap k(x)$ of $k(x)$, which in turn has a monic irreducible polynomial $p \in k[x]$ as a uniformizer. It follows by theorem V.2.20 that

$$P \cap \mathcal{O} = (p, y - b)$$

with either $b = y$ or $b \in k[x]$ and $\deg(b) < \deg(a)$. If $b = y$, we are done. Otherwise, we know that $b + (p)$ is a root of $Y^2 + h(x)Y - f(x)$ modulo p, i.e. $p \mid b^2 + hb - f$, which proves the existence.

Now, since every integral ideal is the uniquely determined product of finitely many prime ideals, it suffices to show that the product of two ideals of the given form is in the same form again. So if $\mathfrak{a}_1 = (a_1, y - b_1)$ and $\mathfrak{a}_2 = (a_2, y - b_2)$ with $a_i, b_i \in k[x]$ and $a_i \mid b_i^2 + b_ih - f$ for $i = 1, 2$, we show that there exist $a, b, d \in k[x]$ with d, a monic, $\deg(b) < \deg(a)$ and $a \mid b^2 + hb - f$ such that $\mathfrak{a} := \mathfrak{a}_1\mathfrak{a}_2 = (d)(a, y - b)$. To find this representation, we simply calculate the product $\mathfrak{a}$:

$$\mathfrak{a} = (a_1a_2, a_1y - a_1b_2, a_2y - a_2b_1, y_2 - (b_1 + b_2)y + b_1b_2).$$

But $y^2 = f - hy$ by (V.4), i.e.

$$\mathfrak{a} = (a_1a_2, a_1y - a_1b_2, a_2y - a_2b_1, (b_1 + b_2 + h)y - (b_1b_2 + f)). \tag{V.6}$$

By algorithm 2, we can effectively compute elements $d, u_1, u_2, u_3 \in k[x]$ such that

$$d = \gcd(a_1, a_2, b_1 + b_2 + h) = u_1a_1 + u_2a_2 + u_3(b_1 + b_2 + h). \tag{V.7}$$

Furthermore, we can show that $b := \frac{u_1a_1b_2+u_2a_2b_1+u_3(b_1b_2+f)}{d}$ is an element of $k[x]$ as

$$b = \frac{u_1a_1b_2 + (d - u_1a_1 - u_3(b_1 + b_2 + h))b_1 + u_3(b_1b_2 + f)}{d}$$

by using (V.7), which in turn equals

$$b_1 + \frac{a_1}{d}(u_1(b_2 - b_1) - u_3c_1) = b_2 + \frac{a_2}{d}(u_2(b_1 - b_2) - u_3c_2) \in k[x] \tag{V.8}$$

by putting $c_i := \frac{b_i^2+b_ih-f}{a_i}$ for $i = 1, 2$. Now, the definition of b together with (V.7) yield

$$d(y - b) = dy - db = u_1a_1(y - b_2) + u_2a_2(y - b_1) + u_3((b_1 + b_2 + h)y - (b_1b_2 + f)),$$

i.e. $d(y - b) \in \mathfrak{a}$ by (V.6). An easy calculation reveals that $\mathfrak{a} = (a_1a_2, a_1(y - b_2) - \frac{a_1}{d}d(y-b), a_2(y-b_1) - \frac{a_2}{d}d(y-b), (b_1+b_2+h)y-(b_1b_2+f) - \frac{b_1+b_2+h}{d}d(y-b), d(y-b))$, i.e.

$$\mathfrak{a} = (a_1a_2, a_1(b - b_2), a_2(b - b_1), (b_1 + b_2 + h)b - (b_1b_2 + f), d(y - b)).$$

But, by (V.7), $(b_1 + b_2 + h)b$ is equal to

$$\frac{(u_1a_1b_1 + u_2a_2b_2)(b_1 + b_2 + h) + (d - u_1a_1 - u_2a_2)(b_1b_2 + u)}{d}$$

which, by definition of c_1 and c_2, equals

$$\frac{a_1a_2}{d}(u_1c_2 + u_2c_1) + (b_1b_2 + f).$$

We have shown:

$$\mathfrak{a} = \left(\frac{a_1a_2}{d}d, \frac{a_1a_2}{d}(u_2(b_1 - b_2) - u_3c_2), \frac{a_1a_2}{d}(u_1(b_2 - b_1) - u_3c_1), \frac{a_1a_2}{d}(u_1c_2 + u_2c_1), d(y - b)\right).$$

Since $\omega(y - b) = -y - h - b$, we can easily compute the norm of $y - b$ by remark V.1.8:

$$N_{k(C)/k(x)}(y - b) = (b - y)(y + h + b) = b^2 + hb - f.$$

One verifies that this is equal to

$$\frac{a_1a_2}{d}\big((u_1u_2(b_1+b_2)+u_3(u_1c_2+u_2c_1))h+u_3^2c_1c_2 \\ +(u_1a_1+2u_3b_1)u_1c_2+(u_2a_2+2u_3b_2)u_2c_1+2u_1u_2(b_1b_2-f)\big),$$

which is an element of $(d^{-1})\mathfrak{a}$ and is divisible by $a := \frac{a_1a_2}{d^2}$, i.e. $a \mid b^2+bh-f$. By computing

$$t = \gcd\left(d, u_2(b_1-b_2)-u_3c_2, u_1(b_2-b_1)-u_3c_1, u_1c_2+u_2c_1, \frac{(b^2+bh-f)d^2}{a_1a_2}\right)$$

with algorithm 2, we obtain

$$\mathfrak{a} = (d)\,(at, y-b)\,.$$

On the other hand, we know that the ideal norm is multiplicative and so we can apply lemma V.2.32, which yields:

$$N(\mathfrak{a}) = d^2at = a_1a_2tk[x],$$

since if $a\cdot\tilde{a} = b^2+bh-f$ for some $\tilde{a}\in k[x]$, then $t \mid \frac{(b^2+bh-f)d^2}{a_1a_2} = \tilde{a}$, i.e. $at \mid b^2+bh-f$. By the same argument, we obtain

$$N(\mathfrak{a}) = N(\mathfrak{a}_1)N(\mathfrak{a}_2) = a_1a_2k[x].$$

Together, this means that $t=1$, i.e. we have shown:

$$\mathfrak{a} = (d)(a, y-b).$$

By multiplying a and d by suitable constants in $k^*\subseteq\mathcal{O}^*$, we can achieve that they are both monic. Similarly, we can add a suitable multiple of a to b to achieve $\deg(b) < \deg(a)$. This shows the existence of the desired representation of $\mathfrak{a}$.

Uniqueness. By using the definition of ideal multiplication and the fact that (d) is a principal integral ideal, we obtain:

$$\mathfrak{a} = (d)(a, y-b) = da\mathcal{O} + d(y-b)\mathcal{O}.$$

But by proposition V.2.19, we have $\mathcal{O} = k[x]+yk[x]$, i.e.

$$\mathfrak{a} = d(ak[x]+k[x]-(b+h)k[x])y + d(ak[x]+fk[x]-bk[x]).$$

So elements of $\mathfrak{a}$ are of the form $ry+s$ for $r,s\in k[x]$ with $d\mid r$ and $d\mid s$. We have proven that $dy-db\in\mathfrak{a}$ and hence, $d = \gcd(r : ry+s\in\mathfrak{a})$. So d is uniquely defined by $\mathfrak{a}$. On the other hand, $N(\mathfrak{a}) = d^2ak[x]$ by lemma V.2.32, which yields the uniqueness of a. The uniqueness of b follows from proposition V.2.27(3), since a is unique. □

Semireduced Divisors

The unique representation of an integral ideal of $\mathcal{O}$ that we have met in the previous theorem can be used to find designated representatives of ideal classes.

Proposition V.2.33. Let $\mathfrak{a}$ be an integral ideal of $\mathcal{O}$ with corresponding divisor $D := \operatorname{div}(\mathfrak{a}) = \sum v_P(P)$. Then the following are equivalent:

1. $(p^{-1})\mathfrak{a}$ is not integral for any irreducible polynomial $p \in k[x]$.
2. $D - \pi_{\mathcal{O}}(\operatorname{div}(p)) = D - \operatorname{div}(p)_0 \not\geq 0$ for any irreducible polynomial $p \in k[x]$.
3. If P is inert, then $v_P = 0$; if P is ramified, then $v_P \in \{0, 1\}$; if P is splitting, then $v_P = 0$ or $v_{\omega(P)} = 0$.
4. $\mathfrak{a} = (a, y - b)$ for $a, b \in k[x]$, a monic, $\deg(b) < \deg(a)$ and $a \mid b^2 + bh - f$.

Proof. This is [Eng00, Ch. 3, proposition 3.18, p. 54]. □

This result leads to the following definition:

Definition V.2.34. If the assertions of the proposition are satisfied, we call the divisor $D = \operatorname{div}((a, y - b)\mathcal{O})$ *semireduced* and denote it by $\operatorname{div}(a, b)$.

Corollary V.2.35. If $D := \operatorname{div}(a, b)$ is a semireduced divisor, then $\omega(D) = \operatorname{div}(a, -b - h \bmod a)$ is semireduced and lies in the *opposite* ideal class, i.e. $D + \omega(D) = \operatorname{div}(d\mathcal{O})$ for some $d \in k[x]$ (here, "mod a" does not mean the residue class mod a but the actual residue from the Euclidean algorithm).

Proof. See [Eng00, Ch. 3, proposition 3.20, p. 55]. □

Now, the main result of this subsection is that every ideal class contains such a semireduced divisor. Unfortunately, this semireduced divisor need not be unique.

Theorem V.2.36. Any ideal class contains a (not necessarily unique) semireduced divisor.

Proof. Let $\operatorname{div}(\mathfrak{a}) \in \mathfrak{I}(\mathcal{O})$ be a representative of a given ideal class, where $\mathfrak{a}$ is an ideal of $\mathcal{O}$. Recall from section V.2.2 that $\mathfrak{a}$ is integral if and only if $\operatorname{div}(\mathfrak{a}) \geq 0$. Therefore, if $\mathfrak{a}$ is fractional, then it exists a place P of $k(C)/k$ extending some finite place $\mathfrak{p}$ of $k(x)/k$ with uniformizer $p \in k[x]$ such that $m_P(\mathfrak{a}) < 0$. If $\mathfrak{p}$ is splitting, we may assume that $m_{\omega(P)}(\mathfrak{a}) \geq m_P(\mathfrak{a})$ (otherwise we switch P and $\omega(P)$) and the ideal class of $\operatorname{div}(\mathfrak{a})$ is the same as of

$$\operatorname{div}((p\mathcal{O})^{-m_P(\mathfrak{a})}\mathfrak{a}) = \operatorname{div}((P \cap \mathcal{O})^{-m_P(\mathfrak{a})}(\omega(P) \cap \mathcal{O})^{-m_P(\mathfrak{a})}\mathfrak{a})$$

and if $\mathfrak{p}$ is ramified, it is the same as of

$$\operatorname{div}((p\mathcal{O})^{-m_P(\mathfrak{a})}\mathfrak{a}) = \operatorname{div}((P \cap \mathcal{O})^{-2m_P(\mathfrak{a})}\mathfrak{a}).$$

The multiplicity of P in this new representative is certainly non-negative and since $\operatorname{div}(\mathfrak{a})$ has only finitely many such places we may iterate this procedure to find a representative $\operatorname{div}(\mathfrak{b})$ of our given ideal class with $\mathfrak{b}$ an integral ideal.

Now, by theorem V.2.28 we have the representation

$$\mathfrak{b} = (d)(a, y - b).$$

In terms of divisors this means

$$\operatorname{div}(\mathfrak{b}) = \operatorname{div}(d\mathcal{O}) + \operatorname{div}(a, b)$$

which implies that $\operatorname{div}(\mathfrak{b})$ and $\operatorname{div}(a, b)$ represent the same ideal class. □

V.2.5 The Mumford Representation

As mentioned in the previous section, a semireduced divisor that represents an ideal class need not be unique. In this section, however, we introduce a special semireduced divisor among all the representatives of an ideal class, which is unique in the case of imaginary quadratic hyperelliptic curves.

Definition V.2.37. Let C/k be a hyperelliptic curve of genus g given by (V.4) and let D be a semireduced divisor of C. If $\deg(D) \leq g$, then D is called *reduced*.

Proposition V.2.38. Any ideal class contains a reduced representative.

Proof. Recall our convention for hyperelliptic curves that the transcendental element x is chosen such that the infinite place $\mathfrak{p}_\infty$ of $k(x)$ is not inert. Let P be an extension of $\mathfrak{p}_\infty$. Choose an arbitrary representative $\operatorname{div}(\mathfrak{a}) \in \mathfrak{I}(\mathcal{O})$ of a given ideal class and put $D := \operatorname{div}(\mathfrak{a}) - \deg(\operatorname{div}(\mathfrak{a}))(P) \in \operatorname{Div}^0(C)$, i.e. $\pi_{\mathcal{O}}(D) = \operatorname{div}(\mathfrak{a})$. Example V.2.13 showed that $\deg(P) = 1$, so $\ell(D + g(P)) \geq 1$ by theorem III.2.4(2) and we can pick a nonzero element $z \in L(D + g(P))$. This implies that $[D] = [D' - g(P)]$ for $D' := D + g(P) + \operatorname{div}(z)$ of degree g, which is effective since $\operatorname{div}(z) \geq -D - g(P)$ by definition of $L(D + g(P))$. From the definition of the map $\beta : \operatorname{Pic}^0(C) \to \operatorname{Cl}(\mathcal{O})$ in (V.5) it is clear that $\pi_{\mathcal{O}}(D' - g(P))$ and $\pi_{\mathcal{O}}(D)$ are in the same ideal class. Furthermore, we have $\deg(\pi_{\mathcal{O}}(D' - g(P))) \leq \deg(D') = g$. By removing the zero divisor of a polynomial in $k[x]$, it is possible to turn $\pi_{\mathcal{O}}(D' - g(P))$ into a semireduced divisor by theorem V.2.28, while further reducing its degree. □

Unfortunately, the given proof of the proposition is not constructive and so we need another way to find reduced representatives. This will be done in section V.3. As noted before, such a reduced representative is unique in the case of an imaginary quadratic hyperelliptic curve.

Theorem V.2.39. If C/k is imaginary quadratic, then any ideal class contains a unique reduced divisor.

Proof. This is [Eng00, Ch. 3, theorem 3.23, p. 56]. □

In proposition V.2.27(3) we have shown that the degree $\deg(\mathrm{div}(a,b))$ of a semireduced divisor is equal to $\deg(a)$, so the existence of unique reduced divisors as representatives for ideal classes in imaginary quadratic hyperelliptic curves yields, in terms of theorem V.2.28, the *Mumford representation* for ideal classes:

Corollary V.2.40. Let C/k be an imaginary quadratic hyperelliptic curve of genus g given by

$$y^2 + h(x)y = f(x), \text{ where } h, f \in k[x], \deg(f) = 2g+1, \deg(h) \leq g.$$

Then for each ideal class there exist unique polynomials $a, b \in k[x]$ with

1. a is monic,
2. $\deg(b) < \deg(a) \leq g$ and
3. $a \mid b^2 + bh - f$

such that it is represented by the divisor $\mathrm{div}(a,b)$.

The requirement of a being monic may be dropped to speed up the addition of two reduced divisors since the divisors $\mathrm{div}(a,b)$ and $\mathrm{div}(\lambda a, b)$ are the same for any $\lambda \in k^*$. In fact, this would save us an inversion and up to g multiplications in k as we have seen in the proof of theorem V.2.28. As a drawback, we would have to make a monic in order to check two reduced divisors for equality. In cryptographic applications, however, the comparison of reduced divisors occurs less frequently than the addition.

V.3 An Algorithm for the Group Law

As mentioned before, we want to restrict ourselves to the case of imaginary quadratic hyperelliptic curves C/k of genus g given by (V.4). In this section we want to give an algorithm that realises the group law in the Jacobian of C. From the previous sections, we already know that it is enough to do the arithmetic in the ideal class group $\mathrm{Cl}(\mathcal{O})$ with the usual notation. The idea of the algorithm we will describe is the same as Gauß used for number fields in [Gau01]. If D_1 and D_2 are two reduced divisors, we want to compute a reduced representative of the ideal class of $D_1 + D_2$. To this end, we *compose* D_1 and D_2, which yields a semireduced representative of the ideal class of $D_1 + D_2$ by theorem V.2.28. This semireduced divisor can be *reduced* to a reduced divisor lying in the same ideal class. This algorithm, consisting of the composition and a reduction step, was first described in [Can87] and is known as *Cantor's algorithm*.

Composition Step

Let $D_1 = \mathrm{div}(a_1, b_1)$ and $D_2 = \mathrm{div}(a_2, b_2)$ be two reduced divisors. We summarize the steps we have done in the proof of theorem V.2.28 that multiplied the two ideals corresponding to D_1 and D_2 and yielded the representation $(d)(a, y-b)$ of this ideal

Algorithm 3 Composition Step

INPUT: Two reduced divisors $D_1 = \mathrm{div}(a_1, b_1)$ and $D_2 = \mathrm{div}(a_2, b_2)$.
OUTPUT: A semireduced representative $\mathrm{div}(a, b)$ of the ideal class of $D_1 + D_2$.

1: $(\tilde{u}, \tilde{v}, \tilde{d}) \leftarrow \mathrm{EEA}(a_1, a_2)$ {EEA=Extended Euclidean Algorithm}
2: $(u, v, d) \leftarrow \mathrm{EEA}(\tilde{d}, b_1 + b_2 + h)$
3: $u_1 \leftarrow u\tilde{u}$ and $u_3 \leftarrow v$ {cf. remark V.2.29}
4: $a \leftarrow (a_1 a_2)/d^2$
5: $b \leftarrow b_1 + \frac{u_1 a_1 (b_2 - b_1) - u_3 (b_1^2 + b_1 h + f)}{d} \pmod{a}$
6: **return** $\mathrm{div}(a, b)$

multipliation. This newly found ideal obviously lies in the same ideal class as $D_1 + D_2$.

Proof of algorithm 3. See proof of theorem V.2.28, in particular the left side of equation (V.8). □

Reduction Step

Our next task is to reduce the semireduced divisor found in the previous algorithm. The reduction method we will provide has been suggested by Paulus and Stein in [PS98] and is based on an idea by Lagrange in [Lag73].

Algorithm 4 Lagrange Reduction

INPUT: A semireduced divisor $D = \mathrm{div}(a_0, b_0)$.
OUTPUT: A reduced representative $\mathrm{div}(a, b)$ of the ideal class of D.

1: $k \leftarrow 0$ {some index variable}
2: **if** $\deg(a_k) > g$ **then**
3: $k \leftarrow 1$
4: $a_1 \leftarrow (b_0^2 + b_0 h - f)/a_0$
5: $b_1 \leftarrow -b_0 - h \pmod{a_1}$ and $q_1 \leftarrow (-b_0 - h - b_1)/a_1$ {ED}
6: **while** $\deg(a_k) > g$ **do**
7: $a_k \leftarrow a_{k-2} + q_{k-1}(b_{k-2} - b_{k-1})$
8: $b_k \leftarrow -b_{k-1} - h \pmod{a_k}$ and $q_k \leftarrow (-b_{k-1} - h - b_k)/a_k$ {ED}
9: $k \leftarrow k + 1$
10: $a \leftarrow a_k$ and $b \leftarrow b_k$
11: **return** $\mathrm{div}(a, b)$

Proof of algorithm 4. Firstly, we prove by induction on k that

$$a_k = \frac{b_{k-1}^2 + b_{k-1} h - f}{a_{k-1}} \text{ for } k \geq 1. \tag{V.9}$$

This statement is clear by definition of a_k, if $k = 1$. Now, assume that the statement is true for $k - 1$ with $k \geq 2$. By inserting the definition of a_k, we have

$$a_k a_{k-1} = a_{k-2} a_{k-1} + q_{k-1} a_{k-1} (b_{k-2} - b_{k-1}),$$

which equals

$$b_{k-2}^2 + b_{k-2}h - f - (b_{k-2} + b_{k-1} + h)(b_{k-2} - b_{k-1}) = b_{k-1}^2 + b_{k-1}h - f$$

by using the induction hypothesis and the construction of q_{k-1}. This proves the statement.

For this form of a_k, it is easy to show that the while-loop terminates for some index k: We see that $\deg(a_k) \geq g+1$ in the while-loop of the algorithm which implies that

$$\begin{aligned}\deg(b_{k-1}^2 + b_{k-1}h - f) &\leq \max\{2\deg(b_{k-1}), \deg(b_{k-1}) + g, 2g+1\} \\ &\leq \max\{2\deg(a_{k-1}) - 2, 2g+1\} \\ &= 2\deg(a_{k-1}) - 2 \text{ by assumption.}\end{aligned}$$

By (V.9), this means that $\deg(a_k) \leq \deg(a_{k-1}) - 2 < \deg(a_{k-1})$. So if $\deg(a_{k-1}) = g+1$, we have $\deg(a_k) \leq g$ and the while-loop terminates.

Secondly, we show that $\operatorname{div}(a_k, b_k)$ is in the same ideal class as $\operatorname{div}(a_{k-1}, b_{k-1})$ for all $k \geq 1$. For simplicity, we let $a = a_{k-1}$ and $b = b_{k-1}$. By an easy induction on k, we immediately see that $\operatorname{div}(a_k, b_k)$ is a semireduced divisor for all k. This means in particular that $a \mid b^2 + bh - f$, i.e. it exists $c \in k[x]$ such that $ac = (y-b)(\omega(y) - b)$ and $\operatorname{div}(ac, b)$ and $\operatorname{div}(c, b)$ are obviously semireduced divisors. Now, by proposition V.2.27(3), we know that

$$\gcd\left(\operatorname{div}\left((b^2 + bh - f)\mathcal{O}\right), \operatorname{div}\left((y-b)\mathcal{O}\right)\right) = \sum_{\mathfrak{p}} v_p(P),$$

where $b^2 + bh - f = \prod_{\mathfrak{p}} p^{v_p}$ with $p \in k[x]$ irreducible, $v_p \geq 0$ and $\mathfrak{p}$ is the place of $k(x)/k$ with uniformizer p. On the other hand, proposition V.2.27(2) says that

$$\sum_{\mathfrak{p}} v_p(P) = \operatorname{div}\left((y-b)\mathcal{O}\right),$$

so we have

$$\operatorname{div}((y-b)\mathcal{O}) = \gcd\left(\operatorname{div}\left(ac\mathcal{O}\right), \operatorname{div}\left((y-b)\mathcal{O}\right)\right)$$

by inserting ac into the equation. This in turn is the same as $\operatorname{div}(ac, b)$ by proposition V.2.26. Using proposition V.2.27(3) twice, we also have

$$\operatorname{div}(ac, b) = \sum_{\mathfrak{p}} v_p(ac)(P) = \operatorname{div}(a, b) + \operatorname{div}(c, b)$$

with the usual notation. In total, we have shown

$$\operatorname{div}((y-b)\mathcal{O}) = \operatorname{div}(a, b) + \operatorname{div}(c, b).$$

By corollary V.2.35 and the definition of a_k and b_k, we know

$$\omega(\operatorname{div}(c, b)) = \operatorname{div}(c, -b - h \bmod c) = \operatorname{div}(a_k, b_k)$$

and that $\omega(\mathrm{div}(c,b))$ lies in the opposite ideal class of $\mathrm{div}(c,b)$, i.e.

$$\omega(\mathrm{div}(c,b)) = \mathrm{div}(a,b) + \mathrm{div}((d(y-b)^{-1})\mathcal{O}) \text{ for some } d \in k[x].$$

This shows that $\mathrm{div}(a_k, b_k)$ lies in the same ideal class as $\mathrm{div}(a,b)$. □

Chapter VI

Pairings

In the two previous chapters, we have met elliptic curves and their generalizations, called hyperelliptic curves. Starting with a point P on an elliptic curve E/k over some finite field k, we want construct a mapping

$$\pi : \langle P \rangle \times \langle P \rangle \to l^*,$$

where l is a certain finite field extension of k. By restricting the image of this mapping, we can prove that π is a non-degenerate *pairing*, i.e. a non-degenerate bilinear map. Such pairings can then be generalized to the case of hyperelliptic curves. Since we will consider cryptographic applications in chapter VII, we need an algorithm to compute these pairings efficiently.

We begin in section VI.1 with the basic notions of pairings on Abelian groups with given exponent. Very quickly, we come to the Weil pairing for elliptic curves, which we define in section VI.2.1 and prove its properties. For computational purposes, we give an alternative definition of this pairing in section VI.2.2. Since the existence of the Weil pairing has far-reaching consequences, we prove some of them in section VI.2.3. Interestingly, the Weil pairing can be described in terms of another pairing, called the Tate-Lichtenbaum pairing. As promised, we define this pairing and prove its properties in the more general case of arbitrary nonsingular curves in section VI.3. Certainly, the definition of the Tate-Lichtenbaum pairing for elliptic curves is just a special case of this, but we should state it and its consequences, that occur in this special situation, clearly in section VI.4. Then, we are finally in a position to explain an algorithm to compute these pairings, starting with the elliptic curve case in section VI.5.1, and generalize this to the hyperelliptic curve case in section VI.5.2. Section VI.6, the last section of this chapter, has mostly cryptographic purposes. We want to define so called distortion maps on supersingular elliptic curves, which can then be used to modify pairings, so that they are more useful in cryptographic applications.

There are many interesting and important ideas in this chapter, and we like the reader to take special notice of the following highlights/author's own contributions:

- New proofs of all properties of the ϕ-Weil pairing. In fact, the content of the whole section VI.2.1 is the author's own work. It is a generalization of the Weil pairing

as it is presented in [Sil86], and the enlightening paper [Gar04] by Theodoulos Garefalakis inspired the author with this idea.

- A proof of the equivalence of the two definitions of the Weil pairing in section VI.2.2, which is based on [Was03], but uses some more advanced methods.
- Complete proofs of the properties of the Tate-Lichtenbaum pairing in section VI.3, which are all the author's own work. Only the proof of the non-degeneracy is an elaboration of [Hes04], but uses a slightly different approach. Also, we fill all the gaps in [Hes04].
- Proofs of results on when the Tate pairing is non-trivial (see propositions VI.4.6 and VI.4.7).
- Elaboration of [Mil04], and generalization (based on [ACD$^+$06]) to hyperelliptic curves in section VI.5.
- Elaboration of [Ver04] concerning distortion maps in section VI.6.1. We also present ways to modify pairings by using distortion maps in section VI.6.2.

VI.1 Pairings on Abelian Groups

We want to give a short introduction to the notion of pairings on Abelian groups. To this end, let $m \in \mathbb{Z}_{>0}$ and let A and B be additively written Abelian groups with identity element 0 and both having exponent m. Suppose that C is a multiplicatively written cyclic group of order m with identity element 1.

Definition VI.1.1. Let $\pi : A \times B \longrightarrow C$ be a map.

1. π is called a *pairing* (or *bilinear*) if we have for all $P, P' \in A$ and all $Q, Q' \in B$:

$$\pi(P + P', Q) = \pi(P, Q)\pi(P', Q) \text{ and } \pi(P, Q + Q') = \pi(P, Q)\pi(P, Q').$$

2. π is called *non-degenerate* if the *associated homomorphisms*

$$A \to \mathrm{Hom}(B, C) \text{ defined by } P \mapsto [Q \mapsto \pi(P, Q)]$$

$$\text{and } B \to \mathrm{Hom}(A, C) \text{ defined by } Q \mapsto [P \mapsto \pi(P, Q)]$$

are both injective.

The following properties of a pairing can be easily verified by using the bilinearity:

Lemma VI.1.2. Let $\pi : A \times B \to C$ be a pairing. If $P \in A$ and $Q \in B$, then:

1. $\pi(P, 0) = \pi(0, Q) = 1$.
2. $\pi(-P, Q) = \pi(P, Q)^{-1} = \pi(P, -Q)$.
3. $\pi(nP, Q) = \pi(P, Q)^n = \pi(P, nQ)$ for all $n \in \mathbb{Z}$.

Proof. This is [BSS05, Ch. IX, lemma 1, p. 183]. □

If A and B are finite and of same order, we have a nice characterization of a pairing to be non-degenerate.

Lemma VI.1.3. Assume that A and B are finite and of the same order. A pairing $\pi : A \times B \to C$ is non-degenerate if and only if the associated homomorphism $A \to \mathrm{Hom}(B, C)$ is injective.

Proof. See [Hes04, lemma 4]. It is also an easy consequence of [Lan02, Ch. I, theorem 9.2, p. 49]. □

VI.2 The Weil Pairing

In this section, we would like to introduce a pairing (called the Weil pairing) on certain subgroups of elliptic curves. Later, we will also construct this pairing in terms of the so called Tate pairing (see section VI.4). We start with a very intuitive definition and also proof many properties of the Weil pairing.

VI.2.1 Definition and Properties

The general setting for the Weil pairing is as follows: Let E/k and E'/k be two elliptic curves, both defined over some perfect field k (k can be infinite) of characteristic p (p can be zero). Furthermore, let m be a positive integer, coprime to p if $p > 0$. It is sufficient to define the Weil pairing over a fixed algebraic closure K of k as we will see in section VI.2.3 (in short: $E[m]$ has order m^2), therefore we have all the results of chapter IV (where we mostly worked over K) at our disposal. Let $\phi : E \to E'$ be a separable isogeny and let $\hat{\phi}$ be its dual isogeny. We want to define a mapping

$$e_\phi : E[\phi] \times E'[\hat{\phi}] \to \mu_m.$$

If $T \in E'[\hat{\phi}]$, we know that $[m]T = \phi(\hat{\phi}T) = \hat{\phi}(\mathcal{O}_E) = \mathcal{O}_{E'}$ by using proposition IV.1.20, and therefore

$$\exists f \in K(E')^* : \mathrm{div}(f) = m(T) - m(\mathcal{O}_{E'}) \tag{VI.1}$$

by corollary IV.1.9. Applying ϕ^* to $(T) - (\mathcal{O}_{E'})$, yields

$$\phi^*((T)) - \phi^*((\mathcal{O}_{E'})) = \sum_{T' \in \phi^{-1}(T)} e_\phi(T')(T') - \sum_{S' \in E[\phi]} e_\phi(S')(S') =: D.$$

But ϕ is surjective (cf. section IV.1.3), i.e. it exists $T_0 \in E$ such that $\phi T_0 = T$. This gives us a bijection of sets:

$$\{T' \in E \mid \phi T' = T\} \overset{1:1}{\longleftrightarrow} E[\phi] \text{ given by } T' \mapsto T' - T_0,$$

whereas the inverse is given by $S' + T_0 \hookleftarrow S'$. Therefore, we have

$$D = \sum_{S' \in E[\phi]} (S' + T_0) - \sum_{S' \in E[\phi]} (S'). \tag{VI.2}$$

Clearly, $\deg(D) = 0$ and $\mathrm{sum}(D) = \sum_{S' \in E[\phi]} S' + T_0 - S' = mT_0 = \hat{\phi}(\phi T_0) = \hat{\phi}(T) = \mathcal{O}_E$ since $|E[\phi]| = m$ by theorem IV.1.18(3) and proposition IV.1.20(3). Again by corollary IV.1.9, this means

$$\exists g \in K(E)^* : \mathrm{div}(g) = \phi^*((T)) - \phi^*((\mathcal{O}_{E'})) = D.$$

Now, with lemma IV.1.16(2) we get a relation between g and f:

$$\mathrm{div}(\phi^* f) = \phi^*(\mathrm{div}(f)) = m(\phi^*((T)) - \phi^*((\mathcal{O}_{E'}))) = m \cdot \mathrm{div}(g) = \mathrm{div}(g^m).$$

By corollary III.1.5, there exists a constant $c \in K^*$ such that $\phi^* f = c g^m$. By switching f to $c^{-1} f$ (again by corollary III.1.5, we have $\mathrm{div}(f) = \mathrm{div}(c^{-1} f)$ and so equation (VI.1) remains true), we may assume that

$$\phi^* f = g^m.$$

For $S \in E[\phi]$ we have that $\phi \circ \tau_S = \phi$, yielding

$$\mathrm{div}(g) = (\phi \circ \tau_S)^*((T)) - (\phi \circ \tau_S)^*((\mathcal{O}_{E'})) = \tau_S^*(\mathrm{div}(g)) = \mathrm{div}(\tau_S^* g)$$

by using parts (2) and (3) of lemma IV.1.16. Again, by corollary III.1.5, we know that there exists a constant $\zeta \in K^*$ such that $\tau_S^* g = \zeta g$. This in turn means that

$$\zeta = \frac{g(X+S)}{g(X)} \text{ for all } X \in E \setminus \{\text{zeros and poles of } g\} \neq \emptyset,$$

whereas the set on the right is nonempty as g has only finitely many zeros and poles. We want to stress that the constant ζ is independent of the choice of X. Since $\mathrm{div}(g \circ \tau_S) = \mathrm{div}(g)$, it is clear that

$$X + S \in E \setminus \{\text{zeros and poles of } g\} \tag{$*$}$$

for any $X \in E \setminus \{\text{zeros and poles of } g\}$, making sure that ζ indeed can be written in the above form. Furthermore, we see that ζ is an m-th root of unity:

$$\zeta^m = \frac{g(X+S)^m}{g(X)^m} = \frac{f(\phi(X+S))}{f(\phi(X))} = 1,$$

since $S \in E[\phi]$.

We summarize the above in the following definition and are finally able to define the Weil pairing.

Definition VI.2.1. If $(S, T) \in E[\phi] \times E'[\hat{\phi}]$, then there exist functions $f_T \in K(E')^*$

and $g_T \in K(E)^*$ such that

$$\operatorname{div}(f_T) = m(T) - m(\mathcal{O}_{E'}) \text{ and } g_T^m = \phi^* f_T, \tag{WP}$$

making

$$e_\phi : E[\phi] \times E'[\hat{\phi}] \to \mu_m, (S,T) \mapsto \frac{g_T(X+S)}{g_T(X)}$$

a well-defined mapping for all $X \in E \setminus \{\text{zeros and poles of } g\}$. This mapping is called the *ϕ-Weil pairing*.

Our next aim is to prove several properties of this pairing, starting with the justification of its name. But first, we want to summarize, for the convenience of the reader, two well-known results from Galois theory, that we will need to prove the non-degeneracy of this pairing.

Lemma VI.2.2. Let k be a field and let G be a finite group of order r of automorphisms of k. Let $k^G = \{a \in k \mid \sigma(a) = a \text{ for all } \sigma \in G\}$ be the *fixed field*. Then:

1. (Artin's Theorem) k^G/k is a finite Galois extension of order r with Galois group G.

2. (Fundamental theorem of Galois theory) If l/k is a finite Galois extension with Galois group G, then there is a bijection between the set of subfields E of l containing k and the set of subgroups H of G, given by $E = l^H$.

Proof. Part (1) is [Lan02, Ch. VI, theorem 1.8, p. 264], whereas part (2) is [Lan02, Ch. VI, theorem 1.1, p. 262]. □

Now, here comes the main result of this section.

Theorem VI.2.3. Let e_ϕ be the ϕ-Weil pairing for an isogeny $\phi : E \to E'$ of two elliptic curves.

1. e_ϕ is bilinear.

2. e_ϕ is non-degenerate.

3. e_ϕ is *Galois invariant*, i.e.

$$e_\phi(\sigma(S), \sigma(T)) = \sigma(e_\phi(S,T)) \text{ for all } \sigma \in G_{K/k}.$$

Proof. 1. (a) We prove the linearity in the first argument: Let $S_1, S_2 \in E[\phi]$ and $T \in E'[\hat{\phi}]$. Then:

$$\begin{aligned} e_\phi(S_1+S_2,T) = \frac{g_T(X+S_1+S_2)}{g_T(X)} &\overset{(*)}{=} \frac{g_T(X+S_1+S_2)}{g_T(X+S_2)} \frac{g_T(X+S_2)}{g_T(X)} \\ &\overset{(*)}{=} \frac{g_T((X+S_2)+S_1)}{g_T(X+S_2)} e_\phi(S_2,T) = e_\phi(S_1,T) e_\phi(S_2,T). \end{aligned}$$

(b) We prove the linearity in the second argument: Let $T_1, T_2 \in E'[\hat{\phi}]$ and $S \in E[\phi]$. For convenience, we give the functions in the definition that satisfy (WP) shorter names:

$$f_i := f_{T_i} \text{ and } g_i := g_{T_i} \text{ for } i = 1, 2.$$

Put $\Delta := (T_1)+(T_2)-(T_1+T_2)-(\mathcal{O}_{E'}) \in \mathrm{Div}^0(E')$. Clearly, $\mathrm{sum}(\Delta) = \mathcal{O}_{E'}$, i.e.

$$\exists h \in K(E')^* : \mathrm{div}(h) = \Delta$$

by corollary III.1.5. Let $f := \frac{f_1 f_2}{h^m}, g := \frac{g_1 g_2}{\phi^* h} \in K(E')^*$. Then:

$$\begin{aligned}\mathrm{div}(f) &= \mathrm{div}(f_1) + \mathrm{div}(f_2) - m\mathrm{div}(h) \\ &= m(T_1) - m(\mathcal{O}_{E'}) + m(T_2) - m(\mathcal{O}_{E'}) - m(T_1) \\ &- m(T_2) + m(T_1 + T_2) + m(\mathcal{O}_{E'}) \\ &= m(T_1 + T_2) - m(\mathcal{O}_{E'})\end{aligned}$$

and

$$\phi^* f = \frac{(\phi^* f_1)(\phi^* f_2)}{(\phi^* h)^m} = \frac{g_1^m g_2^m}{(\phi^* h)^m} = g^m$$

by (WP) in the definition of the Weil pairing. Therefore, we have

$$e_\phi(S, T_1 + T_2) = \frac{g(X+S)}{g(X)} = \frac{g_1(X+S)}{g_1(X)} \frac{g_2(X+S)}{g_2(X)} \frac{h(\phi(X))}{h(\phi(X+S))}.$$

But $\frac{h(\phi(X))}{h(\phi(X+S))} = 1$ as $S \in E[\phi]$, i.e.

$$e_\phi(S, T_1 + T_2) = e_\phi(S, T_1) e_\phi(S, T_2).$$

2. By proposition IV.1.20 we know that

$$|E[\phi]| = |E'[\hat{\phi}]| = m$$

and so it is enough to prove that the associated homomorphism

$$E'[\hat{\phi}] \to \mathrm{Hom}(E[\phi], \mu_m)$$

is injective by lemma VI.1.3. So let $T \in E'[\hat{\phi}]$ and suppose that $e_\phi(S, T) = 1$ for all $S \in E[\phi]$, i.e.

$$\tau_S^* g_T = g_T \text{ for all } S \in E[\phi]. \tag{VI.3}$$

Recall that τ_S is birational by example IV.1.13 and that therefore, τ_S^* is an automorphism of the field $K(E)$ as we have proven in theorem II.3.10. We want to show that $K(E)/\phi^* K(E')$ is a Galois extension of order $m = \deg(\phi) = [K(E) : \phi^* K(E')]$. To this end, we firstly show that $\tau_S^* \in \mathrm{Aut}_{\phi^* K(E')}(K(E)) =: G$, the

group of all automorphisms of $K(E)$ fixing $\phi^*K(E')$. Now, if $h \in K(E')$, then

$$\tau_S^*(\phi^*(h(P))) = h(\phi(\tau_S(P))) = h(\phi(P+S)) = \phi^*(h(P))$$

for all $P \in E'$ since $S \in E[\phi]$, i.e. $\tau_S^*(\phi^*h) = \phi^*h$ which proves the claim. So $|G| \geq m$ as it contains $m = |E[\phi]|$ distinct elements τ_S^*. On the other hand, $|G|$ can have at most m elements since $[K(E) : \phi^*K(E')] = m$ (cf. [Bos04, Ch. 4, Bemerkung 1.3, p. 140]), so $|G| = m$. By lemma VI.2.2(1) this means that $K(E)/\phi^*K(E')$ is a Galois extension with Galois group G. Now (VI.3) together with lemma VI.2.2(2) yield that $g_T \in \phi^*K(E')$, i.e. $\exists h \in K(E') : g_T = \phi^*h$ and we have

$$\phi^* f_T = g_T^m = \phi^*(h^m) \text{ by (WP).}$$

But ϕ^* is injective as a homomorphism of fields and so: $f_T = h^m$. On the other hand, we have

$$\operatorname{div}(f_T) = m(T) - m(\mathcal{O}_{E'}), \text{ i.e. } \operatorname{div}(h) = (T) - (\mathcal{O}_{E'}).$$

By corollary III.1.5 this implies that $\operatorname{sum}((T) - (\mathcal{O}_{E'})) = \mathcal{O}_{E'}$, so $T = \mathcal{O}_{E'}$.

3. We apply an arbitrary element $\sigma \in G_{K/k}$ to $\operatorname{div}(f_T) = m(T) - m(\mathcal{O}_{E'})$ and to $\phi^* f_T = g_T^m$:

$$\operatorname{div}(\sigma(f_T)) = \sigma(\operatorname{div}(f_T)) = m(\sigma(T)) - m(\mathcal{O}_{E'})$$

since $\mathcal{O}_{E'}$ is a k-rational point, and

$$\phi^*(\sigma(f_T)) = \sigma(\phi^* f_T) = \sigma(g_T^m) = \sigma(g_T)^m.$$

So, $e_\phi(\sigma(S), \sigma(T)) = \frac{\sigma(g_T)(\sigma(S)+X)}{\sigma(g_T)(X)}$ for all $X \in E \setminus \{\text{zeros and poles of } \sigma(g_T)\}$, but this set also contains $\sigma(X)$ and so, this equals

$$\frac{\sigma(g_T)(\sigma(S)+\sigma(X))}{\sigma(g_T)(\sigma(X))} = \sigma\left(\frac{g_T(S+X)}{g_T(X)}\right) = \sigma(e_\phi(S,T)).$$

□

From this point on, we want to discuss a special case of this pairing. Recall by example IV.1.11 that the multiplication-by-m map $\phi := [m]$ is an isogeny from E to $E' := E$. By proposition IV.1.20 we know that $\widehat{[m]} = [m]$. In this case, the ϕ-Weil pairing becomes

$$e_m : E[m] \times E[m] \to \mu_m$$

and is simply called the *Weil pairing*, denoted by e_m.

In addition to the properties we have shown in the previous theorem, the Weil pairing e_m fulfills the following.

Proposition VI.2.4. Let e_m be the Weil pairing on an elliptic curve E.

1. e_m is *alternating*, i.e. $e_m(T,T) = 1$ for all $T \in E[m]$.

In particular, $e_m(S,T) = e_m(T,S)^{-1}$.

2. e_m is *compatible*, i.e. if $S \in E[mr]$ and $T \in E[m]$, then

$$e_{mr}(S,T) = e_m(rS,T).$$

3. e_m *preserves duality*, i.e. if $\phi : E \to E$ is an isogeny with dual isogeny $\hat{\phi}$, then

$$e_m(S,\hat{\phi}(T)) = e_m(\phi(S),T) \text{ for all } S,T \in E[m].$$

In particular: $e_m(\phi(S),\phi(T)) = e_m(S,T)^{\deg(\phi)}$.

Proof. 1. Let $T \in E[m]$. For convenience, we write $f := f_T$ and $g := g_T$. Then:

$$\begin{aligned}
\operatorname{div}\left(\prod_{i=0}^{m-1} \tau_{iT}^* f\right) &= \sum_{i=0}^{m-1} \operatorname{div}(\tau_{iT}^* f) = \sum_{i=0}^{m-1} \tau_{iT}^*(\operatorname{div}(f)) \text{ (lemma IV.1.16(2))} \\
&= \sum_{i=0}^{m-1} \tau_{iT}^*(m(T) - m(\mathcal{O}_E)) \\
&= \sum_{i=0}^{m-1} m(T - iT) - m(\mathcal{O}_E - iT) \\
&= m \sum_{i=0}^{m-1} ((1-i)T) - (-iT) \\
&= m\left((T) - ((1-m)T)\right) \qquad \text{(telescoping series)} \\
&= m\left((T) - (T - mT)\right) = m((T) - (T)) = 0.
\end{aligned}$$

So $\prod_{i=0}^{m-1} \tau_{iT}^* f \in K^*$ by proposition III.1.4. Since $[m]$ is surjective, we can choose a point $T' \in E$ with $mT' = T$. But for this T' we have

$$\left(\prod_{i=0}^{m-1} \tau_{iT'}^*(g)\right)^m = \prod_{i=0}^{m-1} (g \circ \tau_{iT'})^m = \prod_{i=0}^{m-1} (f \circ [m] \circ \tau_{iT'}) \qquad (*)$$

On the other hand, we know that

$$[m](\tau_{iT'}(P)) = [m](P + iT') = mP + iT = \tau_{iT}([m]P) \text{ for all } P \in E.$$

Together with lemma IV.1.16(3), this means

$$(*) = \prod_{i=0}^{m-1} [m]^*(\tau_{iT}^*(f)) = [m]^*\left(\prod_{i=0}^{m-1} \tau_{iT}^*(f)\right),$$

implying

$$m \cdot \operatorname{div}\left(\prod_{i=0}^{m-1} \tau_{iT'}^*(g)\right) = \operatorname{div}\left([m]^*\left(\prod_{i=0}^{m-1} \tau_{iT}^*(f)\right)\right)$$
$$= [m]^*\left(\operatorname{div}\left(\prod_{i=0}^{m-1} \tau_{iT}^*(f)\right)\right) = [m]^*(0) = 0,$$

i.e. $\prod_{i=0}^{m-1} \tau_{iT'}^*(g) \in K^*$. So for the points $X, X+T' \in E \setminus \{\text{zeros and poles of } g\}$, we have

$$\prod_{i=0}^{m-1} g(X+iT') = \prod_{i=0}^{m-1} g(X+(i+1)T')$$

and so, by reducing:

$$g(X) = g(X+mT') = g(X+T).$$

In other words: $e_m(T,T) = \frac{g(X+T)}{g(X)} = 1$.

The second statement follows easily by using the bilinearity of e_m:

$$1 = e_m(S+T, S+T) = e_m(S,S)e_m(S,T)e_m(T,S)e_m(T,T)$$

for all $S, T \in E[m]$. Now, e_m is alternating and therefore, we have

$$e_m(S,T)e_m(T,S) = 1.$$

2. With the same notation as in part (1), we have

$$\operatorname{div}(f^r) = r \cdot \operatorname{div}(f) = mr(T) - mr(\mathcal{O}_E)$$

and

$$(g \circ [r])^{mr} = (g^m \circ [r])^r = (f \circ [mr])^r = f^r \circ [mr].$$

Together, this yields

$$e_{mr}(S,T) = \frac{(g \circ [r])(X+S)}{(g \circ [r])(X)} = \frac{g(rX+rS)}{g(rX)} = e_m(rS,T)$$

for all $S \in E[mr]$ and $T \in E[m]$.

3. Again, we are using the notation from above and let $S, T \in E[m]$. By proposition IV.1.20(3), we have

$$\hat{\phi}(T) = \operatorname{sum}(\phi^*((T) - (\mathcal{O}_E))) = \operatorname{sum}(\phi^*((T)) - \phi^*((\mathcal{O}_E))),$$

so it exists $h \in K(E)$ such that $\operatorname{div}(h) = \phi^*((T)) - \phi^*((\mathcal{O}_E)) - (\hat{\phi}(T)) + (\mathcal{O}_E)$ by

corollary IV.1.9. On the other hand, we have

$$\begin{aligned}\operatorname{div}\left(\frac{\phi^* f}{h^m}\right) &= \operatorname{div}(\phi^* f) - \operatorname{div}(h^m) = \phi^* \operatorname{div}(f) - m\operatorname{div}(h) \\ &= m\phi^*((T)) - m\phi^*((\mathcal{O}_E)) - m\phi^*((T)) \\ &+ m\phi^*((\mathcal{O}_E)) + m(\hat{\phi}(T)) - m(\mathcal{O}_E) = m(\hat{\phi}(T)) - m(\mathcal{O}_E)\end{aligned}$$

and

$$\left(\frac{g \circ \phi}{h \circ [m]}\right)^m = \frac{g^m \circ \phi}{h^m \circ [m]} = \frac{f \circ [m] \circ \phi}{h^m \circ [m]} = \left(\frac{f \circ \phi}{h^m}\right) \circ [m]$$

as ϕ is a group homomorphism by theorem IV.1.18. In terms of the definition of e_m, this means

$$\begin{aligned}e_m(S, \hat{\phi}(T)) &= \frac{\left(\frac{g\circ\phi}{h\circ[m]}\right)(X+S)}{\left(\frac{g\circ\phi}{h\circ[m]}\right)(X)} = \frac{(g\circ\phi)(X+S)}{(h\circ[m])(X+S)} \cdot \frac{(h\circ[m])(X)}{(g\circ\phi)(X)} \\ &= \frac{g(\phi(X)+\phi(S))}{g(\phi(X))} \cdot \frac{h(mX)}{h(mX+mS)} = e_m(\phi(S), T),\end{aligned}$$

as $\frac{h(mX)}{h(mX+mS)} = 1$ (since $S \in E[m]$).

The second statement follows by applying the above to S and $\phi(T)$, and by using the bilinearity of e_m.

□

VI.2.2 Alternative Definition

The computation of the Weil pairing, in the definition we gave in the previous section, turns out to be inefficient, so it seems to be a good idea to find an alternative, but equivalent, definition of e_m. We do this by defining an efficiently computable (this part will be dealt with in section VI.5) map

$$\tilde{e}_m : E[m] \times E[m] \to \mu_m$$

and then showing that it actually is the Weil pairing. Although the following alternative approach will seem much easier than the definition we gave in the previous section, it has the drawback that proving the properties of the Weil pairing is much harder and more explicit. We are in the fortunate situation that we have already proven all the properties in the previous section. An advantage of the new definition will be the relation to the Tate-Lichtenbaum pairing, we will define in section VI.3. From this relation it will become clear that to compute the Weil pairing, we only have to compute the Tate-Lichtenbaum pairing twice together with a division step.

Definition VI.2.5. Let E be an elliptic curve. For $S, T \in E[m]$, we choose coprime divisors $D_S, D_T \in \operatorname{Div}^0(E)$ such that

$$\operatorname{sum}(D_S) = S \text{ and } \operatorname{sum}(D_T) = T.$$

(For instance, we could take $D_S := (S) - (\mathcal{O}_E)$ and $D_T := (R) - (R - T)$, where $R \in E$ with $\mathcal{O}_E \neq R \neq S$). By corollary IV.1.9 there exist $\mathfrak{f}_S, \mathfrak{f}_T \in K(E)$ such that

$$\operatorname{div}(\mathfrak{f}_S) = m \cdot D_S \text{ and } \operatorname{div}(\mathfrak{f}_T) = m \cdot D_T.$$

We define the map

$$\tilde{e}_m : E[m] \times E[m] \to \mu_m \text{ by } (S, T) \mapsto \frac{\mathfrak{f}_T(D_S)}{\mathfrak{f}_S(D_T)}.$$

(Recall by section III.5 that $f_T(D_S)$ and $f_S(D_T)$ are defined as D_S and D_T are coprime)

It is not a priori clear why $\tilde{e}_m$ is defined, i.e. why $\tilde{e}_m(S, T) \in \mu_m$. But in what follows, we will show that $\tilde{e}_m(S, T) = e_m(S, T)$ which automatically lets the definition of $\tilde{e}_m$ make sense. The idea of our proof is based on [Was03, Ch. 11, p. 370], whereas we will use some of the machinery that we have introduced in previous chapters, making our approach a bit more involved. Also, we need two more definitions, before we are able to understand it.

Definition VI.2.6. For $V, W \in E[m^2]$, we define

$$c(mV, mW) := \frac{f_{mV+mW}(X)}{f_{mV}(X) f_{mW}(X - mV)} \text{ and } d(V, W) := \frac{g_{mV+mW}(X)}{g_{mV}(X) g_{mW}(X - V)},$$

where $X \in E$ is chosen such that the expression of $c(mV, mW)$ respectively $d(V, W)$ is defined. Note that f_T and g_T denote the functions corresponding to $T \in E[m]$ in the *original* definition of the Weil pairing e_m in the previous section. In particular, this means

$$\operatorname{div}(f_T) = m(T) - m(\mathcal{O}_E).$$

We would like to stress that it is not without reason that the variable point X does not occur as an argument of neither $c(mV, mW)$ nor $d(V, W)$, which is explained in the next result.

Lemma VI.2.7. For $V, W \in E[m^2]$, $c(mV, mW)$ and $d(V, W)$ are independent of X.

In fact: $d(V, W)^m = c(mV, mW)$ and $c(mV, mW), d(V, W)$ are constants.

Proof. Recall that the translation-by-S map τ_S is unramified for all $S \in E$ (cf. example IV.1.17). Together with lemma IV.1.16, this means

$$\begin{aligned} \operatorname{div}(\tau_{-mV}^* f_{mW}) &= \tau_{-mV}^*(\operatorname{div}(f_{mW})) = m\tau_{-mV}^*((mW)) - m\tau_{-mV}^*((\mathcal{O}_E)) \\ &= m(mV + mW) - m(mV). \end{aligned}$$

and

$$\operatorname{div}(\tau_{-V}^*(g_{mW})) = \sum_{S' \in E[m]} \big((S' + W + V) - (S' + V)\big).$$

Therefore, we have

$$\begin{aligned}\operatorname{div}(c(mV,mW)) &= \operatorname{div}(f_{mV+mW}) - \operatorname{div}(f_{mW}) - \operatorname{div}(\tau_{-mW}^*(f_{mW}))\\ &= m(mV+mW) - m(\mathcal{O}_E) - m(mV) + m(\mathcal{O}_E)\\ &\quad - m(mV+mW) + m(mV) = 0,\end{aligned}$$

i.e. $c(mV,mW) \in K^*$. Also, we get the following, by using (VI.2):

$$\begin{aligned}\operatorname{div}(d(V,W)) &= \operatorname{div}(g_{mV+mW}) - \operatorname{div}(g_{mV}) - \operatorname{div}(\tau_{-V}^* g_{mW})\\ &= \sum_{S'\in E[m]} ((S'+W+V) - (S') - (S'+V)\\ &\quad + (S') - (S'+W+V) + (S'+V)) = 0,\end{aligned}$$

i.e. $d(V,W) \in K^*$. So we have shown that $c(mV,mW)$ and $d(V,W)$ are independent of X.

Furthermore, we have:

$$\begin{aligned}d(V,W)^m &= \frac{g_{mV+mW}^m(X)}{g_{mV}^m(X)g_{mW}^m(X-V)}\\ &= \frac{f_{mV+mW}(mX)}{f_{mV}(mX)f_{mW}(mX-mV)} = c(mV,mW)\end{aligned}$$

by what we have shown above. □

For the proof of the main result we need one further lemma.

Lemma VI.2.8. Let $U,V,W \in E[m^2]$.

1. $d(V,W) = d(V,W+mU)$.
2. $e_m(mU,mW) = \frac{d(V+mU,W)}{d(V,W)}$.
3. $\frac{d(U,V)}{d(V,U)} = \frac{d(V,W)d(U+W,V)}{d(V,U+W)d(W,V)}$.
4. $e_m(S,T) = \frac{c(S,T)}{c(T,S)}$ for all $S,T \in E[m]$.

Proof. 1. From $m(W+mU) = mW + \mathcal{O}_E = mW$, it follows:

$$d(V,W+mU) = \frac{g_{mV+m(W+mU)}(X)}{g_{mV}(X)g_{m(W+mU)}(X-V)} = d(V,W).$$

2. From $m(V+mU) = mV + \mathcal{O}_E = mV$, it follows:

$$\begin{aligned}d(V+mU,W) &= \frac{g_{m(V+mU)+mW}(X)}{g_{m(V+mU)}(X)g_{mW}(X-V-mU)}\\ &= \frac{g_{mV+mW}(X)}{g_{mV}(X)g_{mW}(X-V)} \cdot \frac{g_{mW}(X-V)}{g_{mW}(X-V-mU)}\\ &= d(V,W)e_m(mU,mW).\end{aligned}$$

3. From
$$d(U, V+W) = \frac{g_{mU+m(V+W)}(X)}{g_{mU}(X)g_{m(V+W)}(X-U)}$$
together with
$$d(V, W) = \frac{g_{mV+mW}(X)}{g_{mV}(X)g_{mW}(X-V)},$$
it follows that
$$g_{mU+m(V+W)}(X) = d(U, V+W)d(V, W)g_{mU}(X)g_{mV}(X-U)g_{mW}(X-U-V),$$
and similarly, that
$$g_{m(U+V)+mW}(X) = d(U+V, W)d(U, V)g_{mU}(X)g_{mV}(X-U)g_{mW}(X-U-V).$$
On the other hand, we know that $m(U+V)+mW = mU+m(V+W)$, so the above yields
$$d(U, V+W)d(V, W) = d(U+V, W)d(U, V).$$
Since this equality holds for all $U, V, W \in E[m^2]$, we also have
$$d(V, U+W)d(U, W) = d(V+U, W)d(V, U).$$
Putting these two equations together, we obtain
$$\frac{d(U, V)}{d(V, U)} = \frac{d(U, V+W)d(V, W)d(U+V, W)}{d(V, U+W)d(U, W)d(U+V, W)}.$$
But we also know that
$$d(U, V+W)d(W, V) = d(U+W, V)d(U, W),$$
which yields
$$\frac{d(U, V)}{d(V, U)} = \frac{d(U, V+W)d(V, W)d(U+W, V)}{d(V, U+W)d(U, V+W)d(W, V)}.$$

4. Recall that $[m]$ is an isogeny, so surjective, i.e. there exist $U, V \in E[m^2]$ such that $mU = S$ and $mV = T$. By lemma VI.2.7, this means
$$\frac{c(S, T)}{c(T, S)} = \frac{c(mU, mV)}{c(mV, mU)} = \left(\frac{d(U, V)}{d(V, U)}\right)^m. \qquad (*)$$
Using part (3) with $W = jU$ for $0 \leq j < m$, we get
$$\begin{aligned}(*) &= \prod_{j=0}^{m-1} \frac{d(V, jU)d(U+jU, V)}{d(V, U+jU)d(jU, V)} = \frac{d(V, \mathcal{O}_E)d(mU, V)}{d(V, mU)d(\mathcal{O}_E, V)} \\ &= \frac{d(V, \mathcal{O}_E)d(S, V)}{d(V, S)d(\mathcal{O}_E, V)} \\ &= \frac{d(V, \mathcal{O}_E)d(\mathcal{O}_E, V)e_m(S, T)}{d(V, \mathcal{O}_E)d(\mathcal{O}_E, V)} = e_m(S, T),\end{aligned}$$

by using part (1) twice, yielding

$$d(V,S) = d(V, \mathcal{O}_E + mU) = d(V, \mathcal{O}_E)$$

and together with part (2):

$$d(S,V) = d(\mathcal{O}_E + mU, V) = d(\mathcal{O}_E, V) e_m(mU, mV).$$

□

The next step to the main result is the answer to the question whether $\tilde{e}$ is well-defined. This will turn out to be the most important ingredient in the proof of the equality of the two definitions.

Proposition VI.2.9. $\tilde{e}_m$ is well-defined.

Proof. Let $S, T \in E[m]$ and let D_S, D_T be arbitrarily chosen as in the definition of $\tilde{e}_m$, and let $D'_S := (S) - (\mathcal{O}_E)$ and $D'_T := (R) - (R - T)$ for $R \in E \setminus \{\mathcal{O}_E, S\}$, be the "standard" or "natural" choices for divisors that satisfy the definition of $\tilde{e}_m$. Furthermore, let f_S and f_T be the functions from definition VI.2.1 corresponding to the points S and T, respectively. Then, there exist functions $\mathfrak{f}_S, \mathfrak{f}_T \in K(E)^*$ such that $\mathrm{div}(\mathfrak{f}_S) = mD_S$ and $\mathrm{div}(\mathfrak{f}_T) = mD_T$. We define

$$\mathfrak{f}'_S := f_S \text{ and } \mathfrak{f}'_T := ((\tau_R \circ [-1])^* f_T)^{-1}.$$

We show that

$$(\tilde{e}(S,T) =) \quad \frac{\mathfrak{f}_T(D_S)}{\mathfrak{f}_S(D_T)} = \frac{\mathfrak{f}'_T(D'_S)}{\mathfrak{f}'_S(D'_T)}.$$

By using the properties of lemmas IV.1.16 and IV.1.22, and the fact that both $[-1]$ and τ_R are ramified, we obtain:

$$\begin{aligned}\mathrm{div}(\mathfrak{f}'_T) &= -\mathrm{div}((\tau_R \circ [-1])^* f_T) = -[-1]^*(\tau_R^*(\mathrm{div}(f_T))) \\ &= -m[-1]^*((T-R)) + m[-1]^*((-R)) = m(R) - m(R-T) = mD'_T.\end{aligned}$$

Trivially, we also have

$$\mathrm{div}(\mathfrak{f}'_S) = \mathrm{div}(f_S) = m(S) - m(\mathcal{O}_E) = mD'_S.$$

This shows that

$$\mathrm{div}(\mathfrak{f}_S) - \mathrm{div}(\mathfrak{f}'_S) = mD_S - mD'_S = m(D_S - D'_S).$$

But $\mathrm{sum}(D_S - D'_S) = S - S = \mathcal{O}_E$ and $\deg(D_S - D'_S) = 0$, i.e.

$$\exists h_S \in K(E) : \mathrm{div}(h_S) = D_S - D'_S, \tag{VI.4}$$

by corollary IV.1.9. So $\mathrm{div}(\mathfrak{f}_s) = \mathrm{div}(\mathfrak{f}'_S) + m \cdot \mathrm{div}(h_S) = \mathrm{div}(h_S^m \cdot \mathfrak{f}'_S)$, i.e.

$$\exists c_S \in K^* : \mathfrak{f}_S = c_S \cdot h_S^m \cdot \mathfrak{f}'_S,$$

by corollary III.1.5. Similarly, we have:

$$\exists c_T \in K^*, h_T \in K(E) : \mathfrak{f}_T = c_T \cdot h_T^m \cdot \mathfrak{f}'_T.$$

Now, there are two cases that may occur concerning the intersections of the supports of the divisors D'_S, D'_T, D_S and D_T (recall that D_S and D_T, as well as, D'_S and D'_T have disjoint supports by definition).

Case 1 ($\mathbf{supp}(D'_S) \cap \mathbf{supp}(D_T) = \emptyset$ and $\mathbf{supp}(D'_T) \cap \mathbf{supp}(D_S) = \emptyset$): By the above and the fact that for $c \in K^*$ and $D = \sum n_P(P) \in \mathrm{Div}^0(E)$, we have

$$c(D) = \prod_{P \in E} c(P)^{n_P} = c^{\sum n_P} = c^{\deg(D)} = c^0 = 1,$$

we get

$$\frac{\mathfrak{f}_T(D_S)}{\mathfrak{f}_S(D_T)} = \frac{h_T(D_S)^m \mathfrak{f}'_T(D_S)}{h_S(D_T)^m \mathfrak{f}'_S(D_T)} = \frac{h_T(\mathrm{div}(h_S))^m h_T(D'_S)^m \mathfrak{f}'_T(\mathrm{div}(h_S)) \mathfrak{f}'_T(D'_S)}{h_S(\mathrm{div}(h_T))^m h_S(D'_T)^m \mathfrak{f}'_S(\mathrm{div}(h_T)) \mathfrak{f}'_S(D'_T)} \qquad (*)$$

whereas the second equality is obtained by using (VI.4). Now, we prove three properties of h_S resp. h_T, which will yield the result we are looking for.

1. Using theorem III.5.4 (Weil's reciprocity law), we have

   $$h_T(\mathrm{div}(h_S)) = h_S(\mathrm{div}(h_T)),$$

   by our assumption on the supports.

2. By the same reasoning, we obtain

   $$h_T(D'_S)^m = h_T(mD'_S) = h_T(\mathrm{div}(\mathfrak{f}'_S)) = \mathfrak{f}'_S(\mathrm{div}(h_T)).$$

3. Again, the above argument yields

   $$h_S(D'_T)^m = \mathfrak{f}'_T(\mathrm{div}(h_S)).$$

Applying these properties to $(*)$, we obtain

$$\frac{\mathfrak{f}_T(D_S)}{\mathfrak{f}_S(D_T)} = \frac{\mathfrak{f}'_T(D'_S)}{\mathfrak{f}'_S(D'_T)}.$$

Case 2 (the supports in case 1 are not disjoint): We want to reduce this case to the previous one. To this end, let $D''_S := (X_1 + S) - (X_1)$ and $D''_T := (Y_1 + T) - (Y_1)$ where $X_1 \neq Y_1$ are chosen such that the following two conditions are satisfied

1. $\operatorname{supp}(D'_S) \cap \operatorname{supp}(D''_S) = \emptyset$ and $\operatorname{supp}(D'_T) \cap \operatorname{supp}(D''_T) = \emptyset$

2. $\operatorname{supp}(D_S) \cap \operatorname{supp}(D''_S) = \emptyset$ and $\operatorname{supp}(D_T) \cap \operatorname{supp}(D''_T) = \emptyset$.

With these two divisors D''_S and D''_T, we can apply case 1 twice to obtain

$$\frac{\mathfrak{f}_T(D_S)}{\mathfrak{f}_S(D_T)} = \frac{\mathfrak{f}'_T(D'_S)}{\mathfrak{f}'_S(D'_T)} = \frac{\mathfrak{f}''_T(D''_S)}{\mathfrak{f}''_S(D''_T)},$$

where $\mathfrak{f}''_S$ and $\mathfrak{f}''_T$ are, as usual, chosen such that

$$\operatorname{div}(\mathfrak{f}''_S) = mD''_S \text{ and } \operatorname{div}(\mathfrak{f}''_T) = mD''_T.$$

□

Finally, we are able to prove the main result of this section, namely that $\tilde{e}_m$ and e_m are actually the same.

Theorem VI.2.10. For all $S, T \in E[m]$, we have

$$e_m(S,T) = \tilde{e}_m(S,T).$$

Proof. Since $[m]$ is surjective, we may choose points $U, V \in E$ with $mU = S$ and $mV = T$, yielding

$$c(S,T) = \frac{f_{S+T}(X)}{f_S(X) f_T(X-S)}$$

by definition of c. Together with lemma VI.2.8(4), this means

$$e_m(S,T) = \frac{c(S,T)}{c(T,S)} = \frac{f_T(X) f_S(X-T)}{f_S(X) f_T(X-S)}.$$

This expression is independent of X by lemma VI.2.7. Now, let $R \in E$ with $\mathcal{O}_E \neq R \neq S$ and put $D'_S := (S) - (\mathcal{O}_E)$ and $D'_T := (R) - (R-T)$ as in proposition VI.2.9. Furthermore, define

$$\mathfrak{f}'_S := f_S \text{ and } \mathfrak{f}'_T := ((\tau_R \circ [-1])^* f_T)^{-1}.$$

Proposition VI.2.9 says that

$$\tilde{e}_m(S,T) = \frac{\mathfrak{f}'_T(D'_S)}{\mathfrak{f}'_S(D'_T)}.$$

On the other hand, we have

$$\frac{\mathfrak{f}'_T(D'_S)}{\mathfrak{f}'_S(D'_T)} = \frac{f_T(R) f_S(R-T)}{f_T(R-S) f_S(R)} = e_m(S,T)$$

which proves the theorem. □

VI.2.3 Consequences

In this section, we want to explain why it was sufficient to define the Weil pairing over an algebraic closure K of k. Also, we want to give some consequences of the existence of the Weil pairing, while examining the structure of $E[m]$.

Recall that, by proposition IV.2.3, we have

$$E[m] \cong \mathbb{Z}_m \oplus \mathbb{Z}_m \text{ as groups with } \mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}.$$

On the other hand, we know that $m\mathbb{Z} \subseteq \mathrm{Ann}_{\mathbb{Z}}(E[m])$, and so we can consider $E[m]$ as a $\mathbb{Z}_m$-module as described in remark II.5.7. It is easy to see that the above $\mathbb{Z}$-module homomorphism (resp. group homomorphism) turns into a $\mathbb{Z}_m$-module homomorphism and $E[m]$ is therefore a free $\mathbb{Z}_m$-module.

Definition VI.2.11. We say that two points T_1 and T_2 form a *basis of* $E[m]$, if they form a $\mathbb{Z}_m$-module basis of $E[m]$.

Remark VI.2.12. By this definition, it is clear that if $\{T_1, T_2\}$ is a basis of $E[m]$, then every point S of $E[m]$ has a representation $S = aT_1 + bT_2$ with $a, b \in \mathbb{Z}$ where a and b are uniquely determined *modulo* m.

Corollary VI.2.13. Let $\{T_1, T_2\}$ be a basis of $E[m]$. Then, $e_m(T_1, T_2)$ is a primitive m-th root of unity.

In particular, if $E[m] \subseteq E(k)$, then $\mu_m \subseteq k^*$.

Proof. This is [Was03, Ch. 3, corollary 3.10 + 3.11, p. 87]. □

The corollary gives a necessary condition for two points being ($\mathbb{Z}_m$-linearly) independent in $E[m]$, which will become quite useful for the cryptographic applications in chapter VII. In addition, it also yields a nice characterization for $e_m(P, Q) = 1$ for two points $P, Q \in E[m]$.

Proposition VI.2.14. Let $\{T_1, T_2\}$ be a basis of $E[m]$ and let $a_P, b_P, a_Q, b_Q \in \mathbb{Z}$ (uniquely determined modulo m) and $P, Q \in E[m]$ such that

$$P = a_P T_1 + b_P T_2 \text{ and } Q = a_Q T_1 + b_Q T_2.$$

Then, we have the following equivalence:

$$e_m(P, Q) = 1 \iff a_P b_Q \equiv a_Q b_P \pmod{m}.$$

Proof. Using the bilinearity of the Weil pairing, we see that

$$e_m(P, Q) = e(T_1, T_1)^{a_P a_Q} e_m(T_1, T_2)^{a_P a_Q} e_m(T_2, T_1)^{a_Q b_P} e_m(T_2, T_2)^{b_P b_Q}.$$

Since e_m is alternating, this means that

$$e_m(P, Q) = e_m(T_1, T_2)^{a_P b_Q - a_Q b_P}.$$

Now, by corollary VI.2.13, we have

$$e_m(P,Q) = 1 \iff m \mid a_P b_Q - a_Q b_P.$$

□

Corollary VI.2.15. If $P, Q \in E[m]$ are independent, then $e_m(P,Q) \neq 1$.

Proof. Assume that $e_m(P,Q) = 1$, i.e. $a_P b_Q \equiv a_Q b_P \pmod{m}$ in the notation of the previous proposition. But this means that

$$b_Q P = a_P b_Q T_1 + b_P b_Q T_2 = b_P(a_Q T_1 + b_Q T_2) = b_P Q,$$

so P and Q are dependent. □

VI.3 The Tate-Lichtenbaum Pairing

We want to introduce a second pairing, called the Tate-Lichtenbaum pairing. Unlike the Weil pairing, we want to define this pairing in a more general setting by considering arbitrary curves. In addition, we let $k = \mathbb{F}_q$ be a finite field with q elements, since this is the situation we need in chapter VII for cryptographic applications.

Let C/k be an absolutely irreducible nonsingular projective curve over k. In order to define the Tate-Lichtenbaum pairing, we need some more information about the Jacobian of C.

Definition VI.3.1. Let $m \in \mathbb{Z}_{\geq 1}$. We denote the group of divisor classes of C with order dividing m by $\mathrm{Pic}^0(k(C))[m]$, i.e.

$$\mathrm{Pic}^0(k(C))[m] = \{[D] \in \mathrm{Pic}^0(k(C)) \mid m[D] = [0], \text{ i.e. } mD \in \mathrm{Princ}(k(C))\}.$$

It is a subgroup of $\mathrm{Pic}^0(k(C))$. Define $\mathrm{Pic}^0(k(C))[0] := \mathrm{Pic}^0(k(C))$.

Recall that $\mathrm{Pic}^0(k(C))$ is a finite group by corollary III.2.6, so we can choose an integer $m \in \mathbb{Z}_{\geq 1}$, coprime to q, with $m \mid |\mathrm{Pic}^0(k(C))|$. Let $l = k(\mu_m)$ be the smallest field with $\mu_m \subseteq l$, where μ_m denotes the set of all m-th roots of unity in K. Note that by example III.3.8, we also have that $m \mid |\mathrm{Pic}^0(l(C))|$. We want to define a map

$$t_m : \mathrm{Pic}^0(l(C))[m] \times \mathrm{Pic}^0(l(C))/m\mathrm{Pic}^0(l(C)) \longrightarrow l^*/(l^*)^m.$$

Let $x \in \mathrm{Pic}^0(l(C))[m]$ and $y \in \mathrm{Pic}^0(l(C))/m\mathrm{Pic}^0(l(C))$. This means that it exists a divisor $D_x \in \mathrm{Div}^0(l(C))$ with $mD_x \in \mathrm{Princ}(l(C))$ s.t. $[D_x] = x$ and a divisor $\tilde{E} \in \mathrm{Div}^0(l(C))$ s.t. $y = [\tilde{E}] + m\mathrm{Pic}^0(l(C))$. Now, put $S := \mathrm{supp}(D_x) \cup \mathrm{supp}(\tilde{E}) \subseteq \mathbb{P}_{l(C)/l}$. By proposition III.1.2, $\mathbb{P}_{l(C)/l}$ is an infinite set and so S is a proper subset, since the support of a divisor is always finite. Let $P_1, \ldots, P_r$ be all the places that are shared by D_x and $\tilde{E}$, i.e.

$$\{P_1, \ldots, P_r\} = \mathrm{supp}(D_x) \cap \mathrm{supp}(\tilde{E}).$$

Furthermore, we denote the size of $\mathrm{supp}(D_x) \setminus \{P_1, \ldots, P_r\}$ by s, so we can write

$$\mathrm{supp}(D_x) = \{P_1, \ldots, P_r, Q_1, \ldots, Q_s\}.$$

Now, $\tilde{E}$ has the form $\tilde{E} = \sum n_P(P)$ and by corollary III.2.7 there exists an element $g \in l(C)$ such that

$$\begin{aligned} v_{P_i}(g) &= n_{P_i} && \text{for all } i = 1, \ldots, r \\ v_{Q_j}(g) &= 0 && \text{for all } j = 1, \ldots, s \\ v_P(g) &\geq 0 && \text{for all } Q \in S \setminus \mathrm{supp}(D_x). \end{aligned}$$

So the supports of the divisors $E_y := \tilde{E} - \mathrm{div}(g)$ and D_x are disjoint (E_y and D_x are called *coprime* in this case). But E_y and $\tilde{E}$ are linearly equivalent by definition (clearly, $\deg E_y = \deg \tilde{E} - \deg \mathrm{div}(g) = 0 - 0 = 0$), so

$$y = [\tilde{E}] + m\mathrm{Pic}^0(l(C)) = [E_y] + m\mathrm{Pic}^0(l(C)).$$

We sum up the above: For $x \in \mathrm{Pic}^0(l(C))[m]$ and $y \in \mathrm{Pic}^0(l(C))/m\mathrm{Pic}^0(l(C))$ there exist coprime divisors $D_x, E_y \in \mathrm{Div}^0(l(C))$ such that

$$x = [D_x] \text{ with } mD_x = \mathrm{div}(f_x) \text{ for some } f_x \in l(C)^* \tag{TLP-1}$$

$$\text{and } y = [E_y] + m\mathrm{Pic}^0(l(C)). \tag{TLP-2}$$

This allows us to define the desired map from above

Definition VI.3.2. The map

$$t_m : \mathrm{Pic}^0(l(C))[m] \times \mathrm{Pic}^0(l(C))/m\mathrm{Pic}^0(l(C)) \longrightarrow l^*/(l^*)^m$$

defined by $(x, y) \mapsto f_x(E_y) \pmod{(l^*)^m}$ is called the *Tate-Lichtenbaum pairing*. By abuse of notation, we sometimes simply write $f_x(E_y)$ when we actually mean its residue in $l^*/(l^*)^m$. Similarly, we sometimes write $t_m(x, z)$ for $x, z \in \mathrm{Pic}^0(l(C))$, where x has order dividing m and z is a representative of $y \in \mathrm{Pic}^0(l(C))/m\mathrm{Pic}^0(l(C))$, when we actually mean $t_m(x, y)$ (this is possible since t_m is well-defined, see next lemma).

Remark VI.3.3. It is trivial to see that if x and y can be represented by divisors that are defined over a proper subfield ℓ of l that contains k, we can choose f_x to be defined over that same field. Then, $t_m(x, y)$ can be represented by an element of ℓ^*.

Firstly, we check that this map is well-defined and bilinear which justifies its name. Then, we want to show another important property of this map, namely that it commutes with the action of Galois.

Lemma VI.3.4. Let t_m be the Tate-Lichtenbaum pairing. Then:

1. t_m is well-defined.

2. t_m is bilinear.

3. t_m is Galois invariant, i.e.

$$t_m(\sigma(x), \sigma(y)) = \sigma(t_m(x, y))$$

for $\sigma \in G_{K/k}$ and $x \in \mathrm{Pic}^0(l(C))[m], y \in \mathrm{Pic}^0(l(C))/m\mathrm{Pic}^0(l(C))$.

Proof. 1. To show that t_m is well-defined we need to consider coprime divisors D'_x, E'_y and a function f'_x as in (TLP-1) and (TLP-2), and show that

$$\frac{f'_x(E'_y)}{f_x(E_y)} \in (l^*)^m.$$

By (TLP-1) we can write $D'_x = D_x + \mathrm{div}(g)$ for some $g \in l(C)^*$, which implies

$$\mathrm{div}(f'_x) = mD'_x = mD_x + m\mathrm{div}(g) = \mathrm{div}(f_x) + \mathrm{div}(g^m) = \mathrm{div}(f_x g^m),$$

i.e. $f'_x = cf_x g^m$ for some constant $c \in l^*$ by corollary III.1.5. On the other hand, we have

$$[E'_y] = [E_y] + m[E] = [E_y + mE] \text{ for some } E \in \mathrm{Div}^0(l(C))$$

by (TLP-2) which implies that

$$E'_y = E_y + mE + \mathrm{div}(h) \text{ for some } h \in l(C)^*.$$

Now, let us see how t_m behaves on our new ingredients:

$$f'_x(E'_y) = cf_x g^m(E'_y) = 1 \cdot f_x(E'_y) \cdot g(E'_y)^m$$

by remark III.5.2 (recall that the evaluation of a rational function f at a divisor D is homomorphic both in f and in D). But, $f_x(E'_y) = f_x(E_y) f_x(E)^m f_x(\mathrm{div}(h))$ and we can use Weil reciprocity on that last part, since $\mathrm{div}(h)$ and $\mathrm{div}(f_x)$ have disjoint supports ($\mathrm{div}(h)$ and $\mathrm{div}(f'_x)$ have disjoint support by our assumption on D'_x and E'_y, so $\mathrm{div}(h)$ and $\mathrm{div}(f_x)$ have disjoint support as $f'_x = cf_x g^m$):

$$f_x(\mathrm{div}(h)) = h(\mathrm{div}(f_x)) = h(mD_x) = h(D_x)^m.$$

We have seen:

$$\frac{f'_x(E'_y)}{f_x(E_y)} = (f_x(E)h(D_x)g(E'_y))^m \in (l^*)^m.$$

2. We treat the linearity in each argument separately.

   (a) Let $x, u \in \mathrm{Pic}^0(l(C))[m]$ and $y \in \mathrm{Pic}^0(l(C))/m\mathrm{Pic}^0(l(C))$ then, by (TLP-1), we have

$$D_{x+u} = D_x + D_u + \mathrm{div}(g) \text{ for some } g \in l(C)^*$$

and, therefore, it exists a nonzero constant $c \in l^*$ such that

$$f_{x+u}(E_y) = cf_x f_u g^m(E_y) = f_x(E_y) f_u(E_y) g(E_y)^m$$

as before. Modulo $(l^*)^m$ this yields

$$t_m(x+u, y) = t_m(x, y) t_m(u, y).$$

(b) Let $x \in \mathrm{Pic}^0(l(C))[m]$ and $y, z \in \mathrm{Pic}^0(l(C))/m\mathrm{Pic}^0(l(C))$ then, by (TLP-2), we have

$$E_{y+z} = E_y + E_z + mE + \mathrm{div}(h) \text{ for some } E \in \mathrm{Div}^0(l(C)), h \in l(C)^*.$$

This implies

$$f_x(E_{y+z}) = f_x(E_y) f_x(E_z) f_x(E)^m f_x(\mathrm{div}(h))$$

which yields modulo $(l^*)^m$ (by using Weil reciprocity)

$$t_m(x, y+z) = t_m(x, y) t_m(x, z).$$

3. Recalling the action of Galois in section II.8, we see that it exist a divisor $E \in \mathrm{Div}^0(l(C))$ and functions $g, h \in l(C)^*$ such that

$$D_{\sigma(x)} = \sigma(D_x) + \mathrm{div}_{l(C)}(g) \text{ and } E_{\sigma(y)} = \sigma(E_y) + mE + \mathrm{div}_{l(C)}(h).$$

Furthermore, we already know by proposition III.3.9 that

$$\sigma(\mathrm{div}_{l(C)}(f_x)) = \mathrm{div}_{l(C)}(\sigma(f_x)),$$

which immediately gives us

$$mD_{\sigma(x)} = \sigma(mD_x) + \mathrm{div}_{l(C)}(g^m) = \mathrm{div}_{l(C)}(\sigma(f_x) g^m),$$

i.e.

$$f_{\sigma(x)}(E_{\sigma(y)}) = \sigma(f_x)(\sigma(E_y)) \sigma(f_x)(E)^m \sigma(f_x)(\mathrm{div}_{l(C)}(h)) g(E_{\sigma(y)})^m.$$

This, in turn, implies modulo $(l^*)^m$ together with the trivial fact that $\sigma(f_x(P)) = \sigma(f_x)(\sigma(P))$:

$$t_m(\sigma(x), \sigma(y)) = \sigma(f_x)(\sigma(E_y)) \pmod{(l^*)^m} = \sigma(t_m(x, y)).$$

□

The main result of this section shows that t_m is non-degenerate. But before we are able to prove it, we need some preliminaries. Firstly, it should be noted that since $l(C)$

contains all m-th roots of unity, it also contains all r-th roots of unity, if r divides m. Let us recall a result on *cyclic field extensions*, i.e. finite Galois extensions with cyclic Galois group.

Theorem VI.3.5. Let $r \in \mathbb{Z}_{>0}$ with $r \mid m$ (so it is coprime to $\mathrm{char}(l(C))$) and let $M/l(C)$ be a finite extension of fields. Then:

1. If $M/l(C)$ is a cyclic extension of degree r, then $M = l(C)(\alpha)$ for some $\alpha \in M$ with minimal polynomial $X^r - f \in l(C)[X]$, where $f \in l(C)$.

2. Conversely, if $M = l(C)(\alpha)$ where $\alpha \in M$ is a root of a polynomial of the form $X^r - f \in l(C)[X]$ (in some splitting field) then $M/l(C)$ is a cyclic extension. Furthermore, $d = [M : l(C)]$ divides r, $\alpha^d \in l(C)$ and $X^d - \alpha^d \in l(C)[X]$ is the minimal polynomial of α over $l(C)$.

Proof. See [Bos04, Ch. 4, Satz 8.3, p. 201]. □

Now, let $x = [D] \in \mathrm{Pic}^0(l(C))[m]$ be of precise order r (so r divides m) with $rD = \mathrm{div}(f)$ for some $f \in l(C)^*$. Put $M := l(C)(\alpha)$ where α is a root of the polynomial $X^r - f \in l(C)[X]$. By the theorem, this means that $M/l(C)$ is cyclic of degree $d := [M : l(C)]$ and that $X^d - \alpha^d \in l(C)[X]$ is the minimal polynomial of α. We want to show that $X^r - f$ is irreducible over $l(C)$, i.e. that $d = r$.

We assume that $d < r$ and show that $d \cdot D \in \mathrm{Princ}(l(C))$ which is a contradiction to the minimality of r. Recall that the conorm map is a homomorphism on $\mathrm{Div}(l(C))$ and that it maps principal divisors of $l(C)$ to principal divisors of M (cf. proposition III.3.6). Therefore, we have

$$r \cdot \mathrm{Con}_{M/l(C)}(D) = \mathrm{div}_M(f) = r \cdot \mathrm{div}_M(\alpha),$$

which implies that $\mathrm{Con}_{M/l(C)}(D) = \mathrm{div}_M(\alpha)$. So,

$$\mathrm{Con}_{M/l(C)}(d \cdot D) = \mathrm{div}_M(\alpha^d) = \mathrm{Con}_{M/l(C)}(\mathrm{div}_{l(C)}(\alpha^d)).$$

But the conorm map is injective on $\mathrm{Div}(l(C))$ and so we have

$$d \cdot D = \mathrm{div}_{l(C)}(\alpha^d) \in \mathrm{Princ}(l(C)).$$

It will turn out that $M/l(C)$ is a *Kummer extension*, so we should recall what that actually means.

Definition VI.3.6. Let L'/L be a cyclic field extension of degree n, where n is coprime to the characteristic of L, and L contains all n-th roots of unity. Suppose that there exists an element $\alpha \in L'$ such that $L' = L(\alpha)$ with

$$\alpha^n = c \in L \text{ and } c \neq \gamma^d \text{ for all } \gamma \in L \text{ with } d \mid n, d > 1. \tag{VI.5}$$

Such a field extension is called a *Kummer extension.*

To see that $M/l(C)$ is such an extension, it remains to show condition (VI.5) for the element α with $\alpha^r = f$. Assume that it exists an element $\gamma \in l(C)$ with $\gamma^d = f$ for some $d > 1, d \mid r$, say $r = d \cdot e$ with $e \in \mathbb{N}$. Clearly, $l(C)$ contains all d-th roots of unity since d divides r. Choose a primitive d-th root of unity ζ_d. Since γ is an element of $l(C)$ this means that $X^d - f$ splits in $l(C)$ into pairwise distinct linear factors:

$$X^d - f = (X - \zeta_d^0\gamma) \cdots (X - \zeta_d^{d-1}\gamma).$$

But α^e is a root of $X^d - f$ by definition of M, so $\alpha^e = \zeta_d^i\gamma \in l(C)$ for some $i \in \{0, \ldots, d-1\}$. Exactly as we have shown above, this yields that $e \cdot D \in \mathrm{Princ}(l(C))$, which is a contradiction to the minimality of r.

We have seen:

Lemma VI.3.7. For $x = [D] \in \mathrm{Pic}^0(l(C))[m]$ of precise order r with $rD = \mathrm{div}(f)$ for some $f \in l(C)$, the polynomial $X^r - f \in l(C)[X]$ is irreducible over $l(C)$ and defines a Kummer extension of $l(C)$.

There are a lot of other results about Kummer extensions and there is another one in which we have particular interest:

Theorem VI.3.8. Let F'/k' be a Kummer extension of a function field F/k over a perfect field k and let P be a place of F/k. Suppose that it exists an element $y \in F'$ that is integral over $\mathfrak{O}_P$ such that $F' = F(y)$. Let $\varphi(X) \in \mathfrak{O}_P[X]$ denote the minimal polynomial of y over F. We have the decomposition of

$$\overline{\varphi}(X) = \prod_{i=1}^{r} \gamma_i(X)^{\epsilon_i}$$

into irreducible factors over F_P, where $\overline{\varphi}$ is the polynomial in $F_P[X]$ that emerges by taking the coefficients of φ modulo P.

Then, $\epsilon_i = 1$ for all $i = 1, \ldots, r$ (so $[F' : F] = r \cdot s$ for some $s \in \mathbb{N}$) and there exist exactly r places $P_1, \ldots, P_r$ of F' lying over P.

Furthermore, P is unramified in F' and

$$\deg \gamma_i(X) = f(P_i|P) = s \text{ for all } i = 1, \ldots, r.$$

Proof. Since k is assumed to be perfect, it follows that $\overline{\varphi}$ is separable, i.e. $\epsilon_i = 1$ for all $i = 1, \ldots, r$. Then, the result follows immediately by applying theorem III.3.14 together with corollary III.3.11. □

Also, we will need the following two group-theoretic results:

Theorem VI.3.9. Let G be a finite Abelian group of order r. If $n \in \mathbb{N}$ is a divisor of r, then it exists a subgroup H of G of order n.

Proof. See [KS04, Ch. 2, theorem 1.4, p. 45]. □

Theorem VI.3.10. Let G be a cyclic group of order n and let $r \in \mathbb{N}$ be a divisor of n. Define G^r as the image of the group homomorphism $G \ni g \mapsto g^r$. Then:

$$|G^r| = \frac{n}{r}.$$

Proof. This follows immediately from [KS04, Ch. 1, theorem 4.3, p. 22]. □

The next theorem is the long-awaited result, showing that t_m is non-degenerate. Its proof is based on a paper by Hess [Hes04], where the *van der Waerden criterion* (see [vdW71, Ch. 8, section 10, p. 198]) is needed. We take a slightly different approach by using theorem VI.3.9 instead. It should be noted that this result was first proved in [FR94] with cohomological methods, though we choose to forgo this technique.

Theorem VI.3.11. The Tate-Lichtenbaum pairing t_m is non-degenerate.

Proof. We prove the theorem in several steps to make it more comprehensible.

Let $0 \neq x = [D_x] \in \mathrm{Pic}^0(l(C))[m]$ (define $D := D_x$) be of precise order r with $rD = \mathrm{div}(f)$ for some $f \in l(C)$. By lemma VI.3.7, the polynomial $X^r - f \in l(C)[X]$ is irreducible over $l(C)$ and defines a Kummer extension $M = l(C)(\alpha)$ of $l(C)$ for some root α of $X^r - f$. We denote the full constant field of M by l'.

Step 1. For any $d \in \mathbb{N}$ with $r = d \cdot n$, for some $n \in \mathbb{N}$, there exists a constant $\nu(n)$ such that for every $a \geq \nu(n)$ there exists a place $P \in \mathbb{P}_{l(C)/l}$ of degree a such that $X^r - f(P)$ splits into irreducible factors of degree $\frac{r}{d}$ in $l(C)_P[X]$.

We know that $G := G_{M/l(C)}$ is cyclic of degree r (hence Abelian) and every conjugacy class of G has therefore exactly one element. Let $d \in \mathbb{N}$ be a divisor of r, i.e. $r = d \cdot n$ for some $n \in \mathbb{N}$. By theorem VI.3.9, there exists a cyclic subgroup of G of order n. We denote its generator by τ_n and consider its conjugacy class $\tau_n^G = \{\tau_n\}$ in G. By Chebotarev's density theorem III.6.5 we know that

$$\delta\left(\left\{P \in \mathbb{P}_{l(C)/l} \mid \left(\frac{M/l(C)}{P}\right) = \tau_n^G\right\}\right) = \frac{1}{r} \neq 0$$

and so, by proposition III.6.6, there are infinitely many places $P \in \mathbb{P}_{l(C)/l}$ that are unramified in M such that the decomposition group D of P' over P is generated by τ_n for all places P' of M/l' lying over P. Now, (III.4) implies

$$f(P'|P) = [M_{P'} : l(C)_P] = |\mathrm{Gal}(M_{P'}/l(C)_P)| = n \text{ for all } P' \in \mathbb{P}_{M/l'},\ P'|P.$$

As noted in section III.6, lemma III.6.7 says that it exists a constant $\nu(n)$ such that for every $a \geq \nu(n)$ there exists at least one place $P \in \left\{P \in \mathbb{P}_{l(C)/l} \mid \left(\frac{M/l(C)}{P}\right) = \tau_n^G\right\}$ with $\deg(P) = a$. Since f has only finitely many zeros and poles, there exists a place $P \in \left\{P \in \mathbb{P}_{l(C)/l} \mid \left(\frac{M/l(C)}{P}\right) = \tau_n^G\right\}$ of degree a for some $a \geq \nu(n)$ such that $X^r - f \in \mathfrak{O}_P^*[X]$. So α is integral over $\mathfrak{O}_P$ and there are exactly d irreducible factors of $X^r - f(P)$ in $l(C)_P[X]$, all having precise degree $n = \frac{r}{d}$ by theorem VI.3.8. *q.e.d.*

Step 2. Choose $d \in \mathbb{N}$ with $d \mid r$ and a place $P \in \mathbb{P}_{l(C)/l}$ of degree $a \geq \nu(r/d)$ as in step 1. Then: $f(P) \cdot (l(C)_P^*)^r$ is a generator of the cyclic group $(l(C)_P^*)^d/(l(C)_P^*)^r$.

Since l contains all r-th roots of unity, it is clear that μ_r is a subgroup of $l(C)_P^*$, so $r \mid |l(C)_P^*|$. By theorem VI.3.10 this means that

$$v\left((l(C)_P^*)^d/(l(C)_P^*)^r\right) = \frac{r}{d}.$$

Now, the first thing we need to prove is that $f(P)$ is an element of $(l(C)_P^*)^d$. To this end, we pick a root β of $X^r - f(P)$ in some field extension of $l(C)_P$. This field extension must have degree $\frac{r}{d}$ since all the irreducible factors of $X^r - f(P)$ have degree $\frac{r}{d}$ by step 1 and β is a root of one of those. This in turn means that $\gamma := \beta^{\frac{r}{d}}$ lies in $l(C)_P$ with minimal polynomial $X^{\frac{r}{d}} - \gamma$ over $l(C)_P$ by theorem VI.3.5, so

$$f(P) = \beta^r = \gamma^d \in (l(C)_P^*)^d.$$

It remains to show that $\overline{f(P)} := f(P) \cdot (l(C)_P^*)^r$ is of order $\frac{r}{d}$. We clearly have

$$f(P)^{\frac{r}{d}} = \gamma^{d \cdot \frac{r}{d}} = \gamma^r \in (l(C)_P^*)^r.$$

So, $\mathrm{ord}(\overline{f(P)})$ divides $\frac{r}{n}$. Assume it exists $\xi \in \mathbb{N}$ with $\xi \mid \frac{r}{d}, \xi < \frac{r}{d}$ such that $f(P)^\xi = c^r$ for some $c \in l(C)_P^*$. This means:

$$c^r = f(P)^\xi = \gamma^{d\xi} = (\beta^\xi)^r, \text{ i.e. } \frac{\beta^\xi}{c} \in \mu_r \subseteq l(C)_P^*.$$

But $c \in l(C)_P^*$ and so $\beta^\xi \in l(C)_P^*$ which is a contradiction to the fact that $X^{\frac{r}{d}} - \gamma$ is the minimal polynomial of β over $l(C)_P$. *q.e.d.*

Step 3. Let d, P, a be as in step 2. Then: $N_{l(C)_P/l}(f(P))$ is a generator of the cyclic group $(l^*)^d/(l^*)^r$.

First of all, we know that the restriction of the norm map $N := N_{l(C)_P/l} : l(C)_P \to l$ to $l(C)_P^*$ gives us a group homomorphism $N : l(C)_P^* \to l^*$ which is surjective and has the group $\{\mathfrak{g} \in l(C)_P^* \mid g^{|l^*|} = \mathfrak{g} \text{ for some } g \in l(C)_P^*\}$ as its kernel (cf. solution of exercise 4.8.2 in the appendix of [Bos04, p. 351]). We want to show that

$$N^{-1}((l^*)^r) = (l(C)_P^*)^r. \tag{VI.6}$$

Obviously, we have $N((l(C)_P^*)^r) \subseteq (l^*)^r$ since N is a group homomorphism. Now, let $b \in (l^*)^r$, i.e. $b = c^r$ for some $c \in l^*$ and let $\beta \in N^{-1}(b)$ (possible since N is surjective). We have to show that $\beta \in (l(C)_P^*)^r$. Because of the surjectivity of N we can choose an element $\gamma \in l(C)_P^*$ with $N(\gamma) = c$, so $N(\gamma^r) = c^r = b$. Furthermore, we have that

$$N(\beta\gamma^{-r}) = \frac{N(\beta)}{N(\gamma^r)} = \frac{b}{b} = 1, \text{ i.e. } \beta\gamma^{-1} \in \ker(N).$$

This means that it exists $g \in l(C)_P^*$ such that $g^{|l^*|} = \beta\gamma^{-1}$. But $\mu_r \subseteq l^*$ and so r divides

$|l^*|$ which ensures the existence of an element $t \in \mathbb{N}$ such that $|l^*| = t \cdot r$. Therefore, we have

$$\beta = \gamma^r \cdot g^{|l^*|} = (\gamma \cdot g^t)^r \in (l(C)_P^*)^r.$$

Having shown equation (VI.6), it is obvious that N induces an isomorphism

$$l(C)_P^*/(l(C)_P^*)^r \cong l^*/(l^*)^r.$$

It follows that $N(f(P))$ is a generator of $(l^*)^d/(l^*)^r$ by step 2. *q.e.d.*

Step 4. t_m is non-degenerate.

Applying step 1 with $d = 1$ and $d = r$ we see that there exist places P and Q of the same degree and both not in the support of D (recall that $\operatorname{div}(f) = rD$ and that in step 1, we chose the places P such that $v_P(f) = 0$). The divisors $E := P - Q$ and D are therefore coprime. Then, we know by step 3 that $N_{l(C)_P/l}(f(P)) \notin (l^*)^r$ and that $N_{l(C)_Q/l}(f(Q)) \in (l^*)^r$. Also, we have that

$$\operatorname{div}(f_x) = mD = \frac{m}{r}\operatorname{div}(f) = \operatorname{div}(f^{\frac{m}{r}}),$$

so it exists a nonzero constant $c \in l^*$ such that $f_x = c \cdot f^{\frac{m}{r}}$. By putting $y := [E] + m\mathrm{Pic}^0(l(C))$ we see that

$$f_x(E) = f(E)^{\frac{m}{r}} = N_{l(C)_P/l}(f(P))^{\frac{m}{r}} \cdot N_{l(C)_Q/l}(f(Q))^{\frac{m}{r}} \notin (l^*)^m,$$

i.e. $t_m(x, y) \neq 1$. The kernel of the associated homomorphism

$$\mathrm{Pic}^0(l(C))[m] \to \mathrm{Hom}(\mathrm{Pic}^0(l(C))/m\mathrm{Pic}^0(l(C)), l^*/(l^*)^m)$$

defined by $x \mapsto [y \mapsto t_m(x, y)]$ is equal to the set

$$\left\{x \in \mathrm{Pic}^0(l(C))[m] \mid \forall y \in \mathrm{Pic}^0(l(C))/m\mathrm{Pic}^0(l(C)) : t_m(x, y) = 1\right\},$$

and is therefore trivial, which means that the associated homomorphism is injective. Since l^* is cyclic, we know by theorem VI.3.10 that $l^*/(l^*)^m$ is a cyclic group of order m, which is therefore isomorphic to $\mathbb{Z}/m\mathbb{Z}$ (e.g. [KS04, Ch. 1, 1.4.2, p. 22]). Furthermore, we see by considering the mapping

$$\mathrm{Pic}^0(l(C)) \to \mathrm{Pic}^0(l(C)), z \mapsto m \cdot z$$

that $\mathrm{Pic}^0(l(C))/\left(\mathrm{Pic}^0(l(C))[m]\right)$ is isomorphic to $m\mathrm{Pic}^0(l(C))$, which implies that

$$\left|\mathrm{Pic}^0(l(C))[m]\right| = \frac{\left|\mathrm{Pic}^0(l(C))\right|}{\left|m\mathrm{Pic}^0(l(C))\right|} = \left|\mathrm{Pic}^0(l(C))/m\mathrm{Pic}^0(l(C))\right|.$$

So t_m is non-degenerate by lemma VI.1.3. □

In later sections we are mainly interested in the special case, where m is a divisor

of $|\mathrm{Pic}^0(k(C))|$ and $l = \mathbb{F}_{q^s} = k(\mu_m)$ (recall that this is indeed a special case by section II.8). μ_m is a subgroup of l^* and we therefore have

$$m = \mathrm{ord}(\mu_m) \mid \mathrm{ord}(l^*) = q^s - 1.$$

Assume that it exists an integer $r \in \mathbb{N}$ with $r \leq s$ such that m divides $q^r - 1$. Then, a primitive m-th root of unity $\zeta_m \in \mu_m$ is a root of the polynomial $f := X^{q^r} - X \in k[X]$. But the splitting field of f is precisely the field $\mathbb{F}_{q^r}$ (e.g. by [Bos04, Ch. 3, Theorem 8.2, p. 127]), so $\zeta_m \in \mathbb{F}_{q^r}$ which implies that $k(\zeta_m) \subseteq \mathbb{F}_{q^r} \subseteq \mathbb{F}_{q^s} \subseteq k(\zeta_m)$, i.e. $r = s$.

Definition VI.3.12. The number

$$s = [k(\mu_m) : k]$$

is called the *embedding degree* or *security multiplier*. It is the smallest positive integer such that m divides $(q^s - 1)$. Strictly speaking, s is a function $s(q, m)$ of q and m but if the context is clear, we simply write s.

VI.4 The Tate Pairing for Elliptic Curves

In this section, we want to explain how the Tate-Lichtenbaum pairing looks like, in the special case where C is an elliptic curve. To this end, let $k = \mathbb{F}_q$ be a finite field with q elements and let E/k be an elliptic curve defined over k. Recall by proposition IV.1.4 that $E(k) \cong \mathrm{Pic}^0(k(E))$. Now, for an integer m that is coprime to q with $m \mid |E(k)|$, we consider the field extension $l := k(\mu_m) = \mathbb{F}_{q^s}$ of k, where s is the embedding degree. In this situation, the Tate-Lichtenbaum pairing becomes

$$t_m : E(l)[m] \times E(l)/mE(l) \to l^*/(l^*)^m$$

(recall that $l^*/(l^*)^m \cong \mu_m$ as groups via $x \cdot (l^*)^m \mapsto x^{\mathrm{ord}(l^*)/m}$) while we need to be careful with its precise definition: Let $P \in E(l)[m]$ and $Q \in E(l)$, by our definition (cf. (TLP-1)) there exists a function $f_P \in l(E)^*$ such that (cf. proposition IV.1.4)

$$\mathrm{div}(f_P) = m(P) - m(\mathcal{O}_E).$$

For (TLP-2) to work, we need a degree zero divisor D_Q that lies in the divisor class of $(Q) - (\mathcal{O}_E)$ but is coprime to $(P) - (\mathcal{O}_E)$. This can be easily achieved by taking an arbitrary point $S \in E(l) \setminus \{\mathcal{O}_E, P, -Q, P - Q\}$ and defining $D_Q = (Q + S) - (S)$. It is obvious that D_Q and $\mathrm{div}(f_P)$ have disjoint supports and that $[D_Q] = [(Q) - (\mathcal{O}_E)]$ since $\deg(D_Q - (Q) + (\mathcal{O}_E)) = 0$ and $\mathrm{sum}(D_Q - (Q) + (\mathcal{O}_E)) = \mathcal{O}_E$. Now, the definition of the Tate-Lichtenbaum pairing says:

$$t_m(P, Q) := t_m(P, Q + mE(l)) = f_P(D_Q) \pmod{(l^*)^m}.$$

We denote the representative $f_P(D_Q)$ of $t_m(P,Q)$ by $\langle P,Q\rangle_m$, i.e.

$$\langle P,Q\rangle_m = f_P(D_Q) \in l^*.$$

Remark VI.4.1. If the order of Q divides m (i.e. $Q \in E(l)[m]$), f_P and D_Q fulfill the assumptions in the definition of the Weil pairing (cf. definition VI.2.5). Therefore, we have

$$e_m(P,Q) = \frac{\langle P,Q\rangle_m}{\langle Q,P\rangle_m}.$$

Recall that the fact that l contains μ_m is only needed in order to prove the non-degeneracy of the Tate-Lichtenbaum pairing (and of course, so that it is defined over l). This allows us to do the defining steps from above also for an intermediate field $k \subseteq k_1 \subsetneq l$ (here we are assuming that the embedding degree $s > 1$) in the case where $P \in E(k_1)[m]$ and $Q \in E(k_1)$ are defined over k_1, yielding an m-th root of unity $t_m(P,Q) \in k_1$ (w.r.t. $l^*/(l^*)^m \cong \mu_m$) that is contained in k_1. Now, if we assume that m is prime, there are exactly $(m-1)$ primitive m-th roots of unity. But l is already chosen as the smallest field that contains both μ_m and k, and so $t_m(P,Q)$ can not be a primitive m-th root of unity, i.e. it has to be trivial. This means that $k_1^* \subseteq (l^*)^m$. We have shown:

Lemma VI.4.2. Let k, l, q, E, m be as above with m being a prime, and let $k \subseteq k_1 \subsetneq l$ be an intermediate field. Then:

$$\text{If } P \in E(k_1)[m] \text{ and } Q \in E(k_1) \implies t_m(P,Q) \in (l^*)^m.$$

By writing out the above isomorphism $l^*/(l^*)^m \cong \mu_m$ explicitly, we see that we can modify the Tate-Lichtenbaum pairing to obtain the pairing

$$e : E(l)[m] \times E(l)/mE(l) \to \mu_m, (P,Q) \mapsto \langle P,Q\rangle_m^{(q^s-1)/m}$$

(we will refer to this pairing simply as the *(reduced) Tate pairing*). Now, each value $t_m(P,Q)$ of t_m has the unique representative $e(P,Q)$ in μ_m and so, all the properties of t_m transfer to e. Similarly to the Weil pairing, we prove some compatibility results.

Theorem VI.4.3. Let E/k be an elliptic curve defined over $k = \mathbb{F}_q$ and let $m \in \mathbb{Z}_{>0}$ be coprime to q with $m \mid |E(k)|$. Suppose that $s = [l : k]$ is the embedding degree where $l := k(\mu_m)$. Furthermore, let M be a multiple of m with $M \mid (q^s - 1)$. Then:

1. If $P \in E(l)[m]$ and $Q \in E(l)$, then

$$\langle P,Q\rangle_M^{(q^s-1)/M} = \langle P,Q\rangle_m^{(q^s-1)/m}.$$

2. If $P \in E(l)[M]$ and $Q \in E(l)$, then

$$\langle P,Q\rangle_M^{(q^s-1)/M} = \langle (M/m)P,Q\rangle_m^{(q^s-1)/m}.$$

Proof. 1. By the assumption, it exists an integer h with $M = hm$, then we have

$$\operatorname{div}(f_P^h) = h \cdot \operatorname{div}(f_P) = M(P) - M(\mathcal{O}_E)$$

which is coprime to $D_Q = D_M$. This yields

$$\langle P, Q\rangle_M^{(q^s-1)/M} = f_P^h(D_M)^{(q^s-1)/M} = f_P(D_Q)^{(q^s-1)/m} = \langle P, Q\rangle_m^{(q^s-1)/m}.$$

2. Again, write $M = hm$. Then we have by part 1 together with bilinearity

$$\langle hP, Q\rangle_m^{(q^s-1)/m} = \langle hP, Q\rangle_M^{(q^s-1)/M} = \langle P, Q\rangle_m^{(q^s-1)/m}.$$

□

Remark VI.4.4. Obviously, we can compose the same isomorphism $l^*/(l^*)^m \cong \mu_m$ with the Tate-Lichtenbaum pairing in the general case of an absolutely irreducible nonsingular curve C/k. We then obtain the *(reduced) Tate pairing*

$$e : \operatorname{Pic}^0(l(C)) \times \operatorname{Pic}^0(l(C))/m\operatorname{Pic}^0(l(C)) \to \mu_m, (x, y) \mapsto f_x(E_y)^{\frac{q^s-1}{m}}.$$

The rest of this section deals with some cryptographic concerns. By corollary IV.3.3, we know that if $m > 4\sqrt{q}$ is a prime number and E is supersingular, then $E(l)[m]$ is a system of representatives for $E(l)/mE(l)$. This allows us to regard the Tate pairing as a mapping on $E(l)[m] \times E(l)[m]$. So, we have shown:

Remark VI.4.5. Let E/k be a supersingular elliptic curve over $k = \mathbb{F}_q$ with a prime number $m \mid |E(k)|$, coprime to q and $m > 4\sqrt{q}$. Then, the Tate pairing is the non-degenerate pairing

$$e : E(l)[m] \times E(l)[m] \to \mu_m, (P, Q) \mapsto \langle P, Q\rangle_m^{(q^s-1)/m},$$

and we have: $m^2 \mid |E(l)|$, but $m^3 \nmid |E(l)|$.

We can prove a similar result in a different setting. Recall that in the more general situation, where E/k is an elliptic curve over k with some $m \mid |E(k)|$, coprime to q, we have

$$|E(l)[m]| = |E(l)/mE(l)|, \tag{VI.7}$$

from the proof of theorem VI.3.11, where $l = k(\mu_m)$. Now if m is prime with $m^2 \nmid |E(l)|$, then $E(l)$ contains no subgroup of order m^2, i.e.

$$E(l)[m] \cong (\mathbb{Z}/m\mathbb{Z}).$$

$E(l)[m]$ cannot be trivial, as $E(l)$ contains at least one point of order m (cf. theorem VI.3.9). Also, we have the homomorphism

$$E(l)[m] \subseteq E(l) \to E(l)/mE(l). \tag{VI.8}$$

We can prove that this is an isomorphism:

Proposition VI.4.6. Let E/k be an elliptic curve over k with a prime number $m \mid |E(k)|$, coprime to q. If $m^2 \nmid |E(l)|$ (i.e. there are no l-rational points of order m^2), then

$$E(l)[m] \cong E(l)/mE(l).$$

Proof. Because of (VI.7), we only have to show that (VI.8) is injective. So let $P \in E(l)$ be a generator of $E(l)[m]$ and let $Q = rP, R = tP \in E(l)[m]$ with $0 \leq t \leq r \leq m-1$. Assume that Q and R lie in the same residue class under (VI.8), i.e. it exists $S \in E(l)$ with $Q - R = mS$. But this means that $mS = (r-t)P \in E(l)[m]$, which is either $\mathcal{O}_E$ or a point of order m, implying that either $S = \mathcal{O}_E$ or S has order m^2. Since the latter case would yield a contradiction, we see that $r = t$, i.e. $Q = R$. □

As for the Weil pairing, we can prove in certain situations that the Tate pairing is non-trivial on independent points.

Proposition VI.4.7. Let E/k be an elliptic curve defined over k with a prime number $m \mid |E(k)|$. Assume that the embedding degree of E and m is $s > 1$, and that $m^2 \nmid |E(l)|$ (i.e. E has no l-rational points of order m^2). If $\mathcal{O}_E \neq P \in E(k)[m]$ and $R \in E(l)[m] \setminus E(k)$, then $e(P, R) \neq 1$.

Proof. Recall from proposition VI.4.6 that

$$E(l)[m] \cong E(l)/mE(l).$$

Now, since e is non-degenerate, there exists a point $Q \in E(l)[m]$ of precise order m (as m is prime) such that $e(P, Q) \neq 1$, and so $Q \notin E(k)$ by lemma VI.4.2. The latter fact means that P and Q are independent, i.e. $\{P, Q\}$ is a ($\mathbb{Z}_m$-vector space) basis of $E[m]$ (over the algebraic closure K of k). So every $R \in E(l)[m]$ is of the form $R = aP + bQ$ for some $a, b \in \mathbb{Z}$ that are uniquely determined modulo m. On the other hand, P generates $E(k)[m]$, so if $R \notin E(k)[m]$, then $b \not\equiv 0 \pmod{m}$. In total, we have shown that for every point $R \in E(l)[m] \setminus E(k)$, we have

$$e(P, R) = e(P, Q)^b \neq 1.$$

□

VI.5 Implementation of Pairings

As noted in the previous section, we only have to compute the (reduced) Tate pairing in order to compute the Tate-Lichtenbaum pairing. The reason for this was, that it is enough to find one representative in $l^*/(l^*)^m$. So in what follows, we will only give algorithms that compute the reduced Tate pairing.

We start with the case of elliptic curves and then explain how the ideas used there can be generalized to the case of imaginary quadratic hyperelliptic curves.

VI.5.1 Elliptic Curve Case

The recent algorithms to compute the Weil and the Tate-Lichtenbaum pairing reduce the problem to finding a function $f \in K(E)$ such that $\mathrm{div}(f) = m(P) - m(\mathcal{O}_E)$ for a point $P \in E[m]$ and evaluating $f(D_Q)$ for the divisor $D_Q = (Q+S)-(S)$ where $Q \in E$ and $S \in E \setminus \{\mathcal{O}_E, P, -Q, P-Q\}$. Because of the relation between the Weil and the Tate-Lichtenbaum pairing (cf. remark VI.4.1), it is obvious that, in the general case, the calculation of the Tate-Lichtenbaum pairing is much faster than the calculation of the Weil pairing. With this in mind, we will only explain how to compute the Tate-Lichtenbaum pairing. The Weil pairing can then be computed by a double computation of the Tate-Lichtenbaum pairing with a final division.

The idea to compute the above function f efficiently is due to Victor Miller's paper [Mil04] that has been published in 2004. First of all, let $l = k(\mu_m)$ denote the smallest field that contains both k and all the m-th roots of unity. We want to construct f from the function $1 \in l(E)$ where E/k is the elliptic curve in question. For this, we pick points $P, Q \in E(l)$ with P having order dividing m, together with a random point $S \in E \setminus \{\mathcal{O}_E, P, -Q, P-Q\}$. Now for $i = 1, \ldots, m$, we will construct functions $f_i \in l(E)^*$ with

$$\mathrm{div}(f_i) = i(P) - ([i]P) - (i-1)(\mathcal{O}_E)$$

(this is possible by corollary IV.1.9). Recall that by corollary III.1.5, the functions f_i are unique up to multiplication with constants, but since we are only interested in the evaluation of those f_i's at D_Q, this is of no interest by remark III.5.2. It is immediately clear that f_m is the function we are looking for, as

$$\mathrm{div}(f_m) = m(P) - m(\mathcal{O}_E) = \mathrm{div}(f).$$

Lemma VI.5.1. 1. We can choose $f_1 = 1$.

2. If $[i]P = (x_i, y_i)$ for $i < m$, then algorithm 1 efficiently computes the point $[i+j]P = (x_{i+j}, y_{i+j})$ and the lines $L = y - \lambda_{i,j}x - \nu_{i,j}$, through $[i]P$ and $[j]P$, and $V = x - x_{i+j}$ through $[i+j]P$ and $\mathcal{O}_E$. With this notation, we can choose

$$f_{i+j} = f_i \cdot f_j \cdot \frac{L}{V}.$$

Proof. 1. This is trivial by the paragraph above the lemma.

2. By definition of the group law on E, we have

$$\mathrm{div}(L) = ([i]P) + ([j]P) + (-[i+j]P) - 3(\mathcal{O}_E)$$

and

$$\mathrm{div}(V) = (-[i+j]P) + ([i+j]P) - 2(\mathcal{O}_E)$$

(see also [Was03, Ch. 11, proposition 1, p. 342]), i.e.

$$\operatorname{div}\left(\frac{L}{V}\right) = ([i]P) + ([j]P) - ([i+j]P) - (\mathcal{O}_E).$$

From this, we obtain

$$\begin{aligned}\operatorname{div}\left(f_i f_j \frac{L}{V}\right) &= i(P) - ([i]P) - (i-1)(\mathcal{O}_E) \\ &\quad + j(P) - ([j]P) - (j-1)(\mathcal{O}_E) + \operatorname{div}\left(\frac{L}{V}\right) \\ &= (i+j)(P) - ([i+j]P) - ((i+j)-1)(\mathcal{O}_E) \\ &= \operatorname{div}(f_{i+j}).\end{aligned}$$

We are done by the paragraph above the lemma.

□

Before we give the actual algorithm that computes the Tate pairing, we come back to the homomorphic property of evaluating functions at divisors. This simply tells us in our case that

$$f_{i+j}(D_Q) = f_i(D_Q) f_j(D_Q) \frac{L(D_Q)}{V(D_Q)} = \frac{f_{i+j}(Q+S)}{f_{i+j}(S)}.$$

Now, the idea of the following algorithm (algorithm 5) is as follows. Firstly, we represent m to the base 2, i.e.

$$m = m_{n-1}2^{n-1} + \cdots + m_1 2 + m_0,$$

where $m_i \in \{0,1\}$ for $i = 0, \ldots, n-1$ and $m_{n-1} = 1$. Obviously, we have $n = \lfloor \log_2(m) \rfloor$. By using the above formula with $j = i$, we can compute f_{2^r} for all $r = 1, \ldots, n-1$. Having those values, we can easily compute f_m by using the formula again.

All of the above is summarized in the following algorithm, and by using the homomorphic property of evaluating functions at divisors, we will evaluate the intermediate results at D_Q in each step. We do a small runtime analysis of this algorithm. The "for"-loop is executed $\log_2(m)$ times, i.e. we are doubling T that many times. The addition step of T and P is executed $H(m)-1$ times, where $H(m)$ is the *Hamming weight* of m, i.e. the number of nonzero coefficients in $m = m_{n-1}2^{n-1} + \cdots + m_1 2 + m_0$. Since the computation of the lines L and V in each step of the algorithm takes polynomial time, it is clear that Miller's algorithm runs in polynomial time.

VI.5.2 Hyperelliptic Curve Case

In this section, we want to generalize the idea of Miller's algorithm of the previous section to the case of imaginary quadratic hyperelliptic curves. So, let C/k be an imaginary quadratic hyperelliptic curve defined over k of genus g with our usual conventions (cf. chapter V). Furthermore, we pick $x = [D] \in \mathrm{Pic}^0(l(C))[m]$ with $\operatorname{div}(f) = mD$ for $f \in l(C)^*$ (choosen as in (TLP-1)) and $y = [E] + m\mathrm{Pic}^0(l(C)) \in \mathrm{Pic}^0(l(C))/m\mathrm{Pic}^0(l(C))$

Algorithm 5 Miller's Algorithm

INPUT: Points $P, Q \in E(l)$ where P has order dividing m.
OUTPUT: The (reduced) Tate pairing $e(P, Q)$.

1: $S \in_R E(l) \setminus \{\mathcal{O}_E, P, -Q, P - Q\}$
2: $Q' \leftarrow Q + S$, $T \leftarrow P$ and $f \leftarrow 1$
3: **for** $n = \lfloor \log_2(m) \rfloor - 1$ **down to** 0 **do**
4: Compute lines L and V for doubling T
5: $T \leftarrow [2]T$
6: $f \leftarrow f^2 \frac{L(Q')V(S)}{V(Q')L(S)}$
7: **if** $m_n = 1$ **then**
8: Compute lines L and V for adding T and P
9: $T \leftarrow T + P$
10: $f \leftarrow f \frac{L(Q')V(S)}{V(Q')L(S)}$
11: $n \leftarrow n - 1$
12: **return** $f^{\frac{q^8-1}{m}}$

(cf. (TLP-2)), which we want to pair with the reduced Tate pairing (cf. remark VI.4.4), i.e. we want to compute a function $f \in l(C)^*$ with $\mathrm{div}(f) = mD$ for some representative D of x (recall that the Tate pairing was independent of the choices of f, D and E). In order to compute the pairing in the same manner as in the elliptic case, we need to choose special representatives of x and y. Recall that Cantor's algorithm can compute positive reduced divisors D_x and E_y of degree g such that

$$x = [D_x - g(P_\infty)] \text{ and } y = [E_y - g(P_\infty)] + m\mathrm{Pic}^0(l(C)),$$

where P_∞ is the unique extension to $l(C)$ of the infinite place $\mathfrak{p}_\infty$ of $l(x)$ (see also proof of proposition V.2.38). By the construction in Cantor's algorithm, we know that E_y and D_x are coprime since E and D are coprime by definition of the Tate pairing. We also need the same type of representation for $[i]x$ for all $i = 1, \ldots, m$, and Cantor's algorithm gives us positive reduced divisors D_i of degree g such that

$$[i]x = [D_i - g(P_\infty)].$$

Now since $[i]x + [j]x = [i + j]x$ for $i + j \leq m$, we have

$$D_i - g(P_\infty) + D_j - g(P_\infty) - (D_{i+j} - g(P_\infty)) \in \mathrm{Princ}(l(C)) \text{ for } i + j \leq m,$$

i.e. there exist functions $h_{i,j} \in l(C)^*$ such that

$$\mathrm{div}(h_{i,j}) = D_i + D_j - D_{i+j} - g(P_\infty) \text{ for } i + j \leq m.$$

Furthermore, we use the convention $D_0 := g(P_\infty)$. We are almost done finding suitable representatives, we only need a different representative for y. To find it, we introduce algorithm 6:

Proof of algorithm 6. In lines 4 and 5, we use Cantor's algorithm to compute B_2 and

Algorithm 6 Relative Prime Representation (RPR)

INPUT: Positive divisors A, B of degree g.
OUTPUT: Divisors B_1, B_2 with $[B_1 - B_2] = [B - g(P_\infty)]$ and $B_1 + B_2$ coprime to $A + (P_\infty)$.

1: **repeat**
2: Choose $P \in_R \mathbb{P}_{l(C)/l}$ of degree 1
3: Choose $n \in_R \mathbb{N}$ such that $n \leq |\mathrm{Pic}^0(l(C))|$
4: Compute $B_2 \geq 0$ of degree g with $[B_2 - g(P_\infty)] = [n(P) - n(P_\infty)]$
5: Compute $C \geq 0$ of degree g with $[C - g(P_\infty)] = [0]$
6: $B_1 \leftarrow B - C + B_2$
7: **until** $B_1 + B_2$ coprime to $A + (P_\infty)$
8: **return** (B_1, B_2)

C. Because of line 6, we have $[B_1 - B_2] = [B - C] = [B - g(P_\infty)]$. Since we choose our ground field l big enough, it is clear that there always exists a place P with integer n such that $B_1 + B_2$ is coprime to $A + (P_\infty)$. In fact, this condition will only fail in very rare cases as it is shown in [ACD$^+$06, Ch. 16, lemma 16.3, p. 391]. □

Remark VI.5.2. By corollary V.1.11, it is certainly easier to find such a representative of y if the genus of C is even. Since we only want to deal with the most general case, we leave the proof to the reader. For genus 2, it is proved in [ACD$^+$06, Ch. 16.3, p. 398].

Now, we can apply this algorithm to $A = D_x$ and $B = E_y$, yielding divisors B_1 and $B_2 \geq 0$ with $y = [B_1 - B_2] + m\mathrm{Pic}^0(l(C))$ and such that $B_1 + B_2$ is coprime to $D_x + (P_\infty)$. The functions f_i we used in Miller's algorithm look very similar in the hyperelliptic case. For $1 \leq i \leq m$, we choose $f_i \in l(C)^*$ such that

$$\mathrm{div}(f_i) = iD_x - D_i - (i-1)g(P_\infty),$$

where the right side is clearly a principal divisor as

$$[i(D_x - g(P_\infty))] = [D_i - g(P_\infty)].$$

With this definition and the independence of the Tate pairing of the choices of f, D and E, we are now looking for f_m, since

$$\begin{aligned}\mathrm{div}(f_m) &= mD_x - D_m - (m-1)g(P_\infty) \\ &= m(D_x - g(P_\infty)) - g(P_\infty) + g(P_\infty).\end{aligned}$$

Following the idea of the previous section, we write m to the base 2, i.e.

$$m = m_{n-1}2^{n-1} + \cdots + m_1 2 + m_0,$$

where $m_i \in \{0, 1\}$ for $i = 0, \ldots, n-1$, $m_{n-1} = 1$ and $n = \lfloor \log_2(m) \rfloor$. Also, we need to prove a similar version of lemma VI.5.1, namely:

Lemma VI.5.3. 1. We can choose $f_1 = 1$.

2. We can choose
$$f_{i+j} = f_i \cdot f_j \cdot h_{i,j} \text{ for } i + j \leq m.$$
Recall that Cantor's algorithm efficiently computes the functions $h_{i,j}$.

Proof. 1. We have
$$\operatorname{div}(f_1) = D_x - D_1 - (1-1)g(P_\infty) = 0,$$
i.e. we can choose $f_1 = 1$.

2. By definition, we have
$$\begin{aligned}\operatorname{div}(f_i f_j h_{i,j}) &= iD_x - D_i - (i-1)g(P_\infty) + jD_x - D_j - (j-1)g(P_\infty) \\ &\quad + D_i + D_j - D_{i+j} - g(P_\infty) \\ &= (i+j)D_x - D_{i+j} - (i+j-1)g(P_\infty) = \operatorname{div}(f_{i+j}).\end{aligned}$$

□

Similarly to the previous section, we summarize the above in algorithm 7.

Algorithm 7 Hyperelliptic Miller Algorithm

INPUT: Elements $x = [D_x - g(P_\infty)] \in \mathrm{Pic}^0(l(C))[m]$ and $y = [E_y - g(P_\infty)] + m\mathrm{Pic}^0(l(C)) \in \mathrm{Pic}^0(l(C))/m\mathrm{Pic}^0(l(C))$.
OUTPUT: The (reduced) Tate pairing $e(x, y)$.

1: $(B_1, B_2) \leftarrow RPR(D_x, E_y)$ and $E \leftarrow B_1 - B_2$
2: $f \leftarrow 1$
3: **for** $i = \lfloor \log_2(m) \rfloor - 1$ **down to** 0 **do**
4: $\quad j \leftarrow \lfloor \log_2(m) \rfloor - i$
5: $\quad$ Compute $h_{j,j}$ using Cantor's algorithm
6: $\quad f \leftarrow f^2 h_{j,j}(E)$
7: $\quad$ **if** $m_i = 1$ **then**
8: $\quad\quad$ Compute $h_{j,1}$ using Cantor's algorithm
9: $\quad\quad f \leftarrow f h_{j,1}(E)$
10: $\quad i \leftarrow i - 1$
11: **return** $f^{\frac{q^s-1}{m}}$

Remark VI.5.4. Since we are evaluating functions at the divisor E in each step of the loop, we might encounter the problem that E is not coprime to the divisors of those functions. If that happens, we would have to use algorithm 6 again with other random values. On the other hand, we know by [ACD+06, Ch. 16, lemma 16.3, p. 391] that it is highly unlikely that this happens.

VI.6 Distortion Maps and Modified Pairings

In this section, we want to modify the Tate pairing on elliptic curves in a special way. This modification is very important in cryptographic applications as we will see in later

sections. Most of the ideas presented here are based on Eric Verheul's paper [Ver04]. The general setting is as follows:

Let E/k be an elliptic curve defined over a finite field $k = \mathbb{F}_q$ with q elements and let m be a prime number coprime to q with $m \mid |E(k)|$. Assume that the embedding degree in this situation is $s > 1$ and let $l := \mathbb{F}_{q^s}$ be the minimal field extension of k for the Tate pairing to be non-degenerate.

VI.6.1 Distortion Maps

Definition VI.6.1. A *distortion map* (defined over l) with respect to a k-rational point $P \in E(k)$ of prime order m is an endomorphism $\delta \in \mathrm{End}_l(E)$ (defined over l) such that

$$\delta(Q) \text{ is independent from } Q,$$

for all $\mathcal{O}_E \neq Q \in \langle P \rangle$, the cyclic group generated by P in $E(k)$.

Remark VI.6.2. Let $\delta \in \mathrm{End}_l(E)$ be a distortion map w.r.t. $P \in E(k)$ of order m, and let $Q = [n]P \in \langle P \rangle$ with $1 \leq n \leq m-1$. Then

$$\mathcal{O}_E \neq \delta(Q) \in E[m].$$

Proof. By theorem IV.1.18(1), we know that δ is a group homomorphism, so

$$[m]\delta(Q) = \delta([mn]P) = \delta([n]\mathcal{O}_E) = \delta(\mathcal{O}_E) = \mathcal{O}_E.$$

Furthermore, we have that $\delta(Q)$ is non-trivial by the definition of δ ($\mathcal{O}_E$ and Q are always dependent). □

Remark VI.6.3. By proposition IV.2.3(2), we know that

$$E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \oplus (\mathbb{Z}/m\mathbb{Z}).$$

Also, we know that $E(k)[m] \subsetneq E[m]$ is a proper subset, since the embedding degree s is assumed to be larger than 1 (cf. corollary VI.2.13). But m is a prime number, and so we see that

$$\text{either } E(k)[m] \cong \{\mathcal{O}_E\} \text{ or } E(k)[m] \cong (\mathbb{Z}/m\mathbb{Z}).$$

Now, since the point $P \in E(k)$ in the definition of a distortion map has order m, it must be the generator of $E(k)[m]$, i.e.

$$E(k)[m] = \langle P \rangle \cong (\mathbb{Z}/m\mathbb{Z}).$$

In particular, such a k-rational point P does always exist. Indeed, by theorem VI.3.9 it exists a subgroup of order m of $E(k)$ since m divides $|E(k)|$. Any non-trivial point in that subgroup has an order dividing m, i.e. it lies in $E(k)[m]$. This means that $E(k)[m]$ is non-trivial, i.e. isomorphic to $(\mathbb{Z}/m\mathbb{Z})$, which is a cyclic group.

Remark VI.6.4. By the previous remark, we know that P generates $E(k)[m]$. Now, if δ is a distortion map w.r.t. P and $\mathcal{O}_E \neq Q \in \langle P \rangle$ is arbitrarily chosen then, by the definition of δ, we know that $\delta(Q)$ is independent from Q, in particular, this means by remark VI.6.2:

$$\delta(Q) \notin E(k).$$

The next theorem is the main result of this section. It tells us that there always exist such distortion maps in the case, where E is supersingular.

Theorem VI.6.5. If E/k is a supersingular elliptic curve defined over k with a point $P \in E(k)$ of order m, then there exist distortion maps (defined over l) with respect to P.

Proof. This is [Ver04, Theorem 5]. □

Let E/k be an elliptic curve in Weierstraß form. Recall the Frobenius morphism of example II.2.7:

$$\phi_q : E \to E^{(q)}, (x, y) \mapsto (x^q, y^q),$$

where $E^{(q)}/k$ is the elliptic curve given by the same Weierstraß equation in which the coefficients are raised to the q-th power (cf. [Sil86, Ch. III, example 4.6, p. 74]). In our case (k finite with q elements), the q-th power map on k is the identity, i.e. the Weierstraß equations are the same. This means that $E^{(q)} = E$ and $\phi_q \in \mathrm{End}(E)$. We call it the *Frobenius endomorphism.*

Remark VI.6.6. Let E/k be an elliptic curve over k in Weierstraß form, and let $\mathcal{O}_E \neq P = (x, y) \in E(K)$ where K denotes an algebraic closure of k. Then:

$$P \in E(k) \iff \phi_q(P) = P.$$

(The statement is trivial, if $P = \mathcal{O}_E$)

Proof. Clearly, we have

$$\begin{aligned} P \in E(k) &\iff x, y \in k \\ &\iff \phi_q(x) = x \text{ and } \phi_q(y) = y \\ &\iff \phi_q(x, y) = (x, y). \end{aligned}$$

□

Now, this endomorphism allows us to prove the next result, which says that the converse of above's theorem also holds.

Theorem VI.6.7. If E/k is an elliptic curve over k, which has a distortion map δ (defined over l) w.r.t. some point $P \in E(k)$ of order m, then E is supersingular.

Proof. If ϕ_q is the q-th power Frobenius endomorphism, we have $\phi_q(P) = P$ since P is k-rational. Now, by remark VI.6.4, we know that $\delta(P) \notin E(k)$, which means

$\phi_q(\delta(P)) \neq \delta(P)$ $(= \delta(\phi_q(P)))$ by remark VI.6.6. So, we have shown

$$\delta \circ \phi_q \neq \phi_q \circ \delta \text{ in } \mathrm{End}(E).$$

Therefore, $\mathrm{End}(E)$ is non-commutative, and so E is supersingular by theorem IV.2.5. □

Although we know by theorem VI.6.5 that distortion maps always exist for supersingular elliptic curves, there is yet no way known on how to construct them. Fortunately, there are certain supersingular elliptic curves for which distortion maps have been successfully found. Comprehensive tables, containing distortion maps for the most popular supersingular elliptic curves over certain fields, can be found in [BSS05, Ch. IX, table IX.1, p. 204] and in [Jou02, Figure 1, p. 22]. Here, we only want to discuss one particular example.

Example VI.6.8. Consider the supersingular elliptic curve

$$E : y^2 = x^3 + 3x \text{ over } k = \mathbb{F}_{11}$$

from example IV.2.7. Let $m := 3$, then $m \mid |E(k)| = 12$ and m is coprime to $q = 11$. We showed in example IV.3.4 that the embedding degree of E and 3 is $s = 2$. Let $P \in E(k)$ be of prime order 3 (i.e. $P = (3, 5)$ or $P = (3, 6)$). We want to find a distortion map (defined over $l := \mathbb{F}_{11^2}$) with respect to P. First of all, we observe for a given non-trivial l-rational point $(x, y) \in E(l)$ that $(-x, \zeta_4 y) \in E(l)$ is also an l-rational point on E, since

$$(-x)^3 - 3x = -(x^3 + 3x) = -y^2 = (\zeta_4 y)^2,$$

where $\zeta_4 \in l$ is a 4-th root of unity (i.e. $\zeta_4^2 = -1$). This defines an endomorphism

$$\delta : E(l) \to E(l) \text{ given by } S \mapsto \begin{cases} (-x, \zeta_4 y), \text{ if } S = (x, y) \\ \mathcal{O}_E, \text{ if } S = \mathcal{O}_E \end{cases}.$$

Obviously, the image of a non-trivial k-rational point $(a, b) \in E(k)$ (with $b \neq 0$) under δ is $(-a, \zeta_4 b)$, but $\zeta_4 \notin k$ since $s > 1$, i.e. $\delta(a, b) \in E(l) \setminus E(k)$. This, in turn, means that $\delta(Q)$ is independent from Q for all points $\mathcal{O}_E \neq Q \in \langle P \rangle$, since $s > 1$ (otherwise $E(k)[3] = E(l)[3]$, which is a contradiction). Therefore, δ is a distortion map (defined over l) with respect to P.

VI.6.2 Modified Pairings

For the concept of modified pairings we want to present, a distortion map with respect to some point P on an elliptic curve E/k is needed. As we have seen in the previous section, those maps do only exist for supersingular curves (cf. theorem VI.6.7), and in this case, there always exist distortion maps with respect to any given non-trivial point P on E (cf. theorem VI.6.5).

In this section, we describe the modified Weil and Tate pairing, starting with the former.

The Modified Weil Pairing

Let E/k be a supersingular elliptic curve over k with $m \mid |E(k)|$ for some prime number $m \in \mathbb{N}$, coprime to q. This ensures that $E(k)[m] \cong (\mathbb{Z}/m\mathbb{Z})$ (cf. remark VI.6.3), i.e. a cyclic group of order m. So we can choose a k-rational point $P \in E(k)$ of precise order m, i.e. a generator of $E(k)[m]$. Furthermore, let δ be a distortion map (defined over $l = k(E[m])$) with respect to P. We want to define a mapping $\langle P \rangle \times \langle P \rangle \to \mu_m$.

Definition VI.6.9. For points $Q, R \in \langle P \rangle$, we define

$$\hat{e}_m(Q, R) := e_m(Q, \delta(R)),$$

which yields the *modified* Weil pairing

$$\hat{e}_m : \langle P \rangle \times \langle P \rangle \to \mu_m \text{ by } (Q, R) \mapsto e_m(Q, \delta(R)).$$

The next proposition summarizes some properties of this new pairing, while justifying its name.

Proposition VI.6.10. The modified Weil pairing $\hat{e}_m$ is

1. bilinear.
2. *symmetric*, i.e. for all $Q, R \in \langle P \rangle$, we have
$$\hat{e}_m(Q, R) = \hat{e}_m(R, Q).$$
3. *strongly* non-degenerate, i.e. $\hat{e}_m(P, P) \neq 1$.

   In other words, we have $\hat{e}_m(Q, P) \neq 1$ and $\hat{e}_m(P, R) \neq 1$ for all $\mathcal{O}_E \neq Q, R \in \langle P \rangle$.

Proof. 1. The linearity in the first argument is simply inherited from the bilinearity of e_m.

   The linearity in the second argument is also inherited from e_m by using the fact that δ, as an endomorphism, is a homomorphism.

2. This follows immediately from the fact that $\hat{e}_m$ is bilinear and that $Q, R \in \langle P \rangle$.

3. By corollary VI.2.15, we have:
$$\hat{e}_m(P, P) = e_m(P, \delta(P)) \neq 1,$$
   since $\delta(P)$ is independent from P by definition.

□

The Modified Tate Pairing

Let E/k be a supersingular elliptic curve defined over k with $m \mid |E(k)|$ for some prime number $m \in \mathbb{N}$ such that the embedding degree of E and m is $s > 1$. As we have seen before, $s > 1$ ensures that $E(k)[m] \cong (\mathbb{Z}/m\mathbb{Z})$ (cf. remark VI.6.3), i.e. a cyclic group of order m. So we can choose a k-rational point $P \in E(k)$ of precise order m, i.e. a generator of $E(k)[m]$. Furthermore, let δ be a distortion map (defined over $l = k(\mu_m)$) with respect to P. As for the Weil pairing, we want to define a mapping $\langle P \rangle \times \langle P \rangle \to \mu_m$.

Definition VI.6.11. For points $Q, R \in \langle P \rangle$, we define

$$\hat{e}(Q, R) := e(Q, \delta(R)),$$

which yields the *modified* Tate pairing

$$\hat{e} : \langle P \rangle \times \langle P \rangle \to \mu_m \text{ by } (Q, R) \mapsto e(Q, \delta(R)).$$

For the modified Tate pairing to be strongly non-degenerate, we need to have that m^2 does not divide $E(l)$. The reason for this is the following result, which is based on Steven Galbraith's paper [Gal01].

Proposition VI.6.12. Let E/k be a supersingular elliptic curve over k with a prime number $m \mid |E(k)|$, coprime to q. Assume that the embedding degree of E and m is $s > 1$, and that $m^2 \nmid |E(l)|$ (i.e. E has no l-rational points of order m^2). Let $\mathcal{O}_E \neq P \in E(k)[m]$ and let δ be a distortion map (defined over l) with respect to P. Then $e(P, \delta(P)) \neq 1$.

Proof. Recall by proposition VI.4.7 that for every point $R \in E(l)[m] \setminus E(k)$, we have

$$e(P, R) \neq 1.$$

But, by definition, $\delta(P)$ is such a point in $E(l)[m] \setminus E(k)$, i.e.

$$e(P, \delta(P)) \neq 1.$$

□

The next proposition summarizes some properties of this new pairing, while justifying its name.

Proposition VI.6.13. The modified Tate pairing $\hat{e}$ is bilinear, symmetric and strongly non-degenerate.

Proof. The proof for the bilinearity and the symmetry works exactly as for the modified Weil pairing. For the non-degeneracy, we use the previous proposition to obtain $\hat{e}(P, P) = e(P, \delta(P)) \neq 1$. □

Chapter VII

Applications in Cryptography

In this chapter, we want to give some applications of pairings for elliptic curves in cryptography. Although most of the results we will present can be easily modified to work with hyperelliptic curves as well, we will focus on the elliptic case. The reason for this is an analysis by Galbraith, Hess and Vercauteren in [GHV07], which indicates that hyperelliptic curves are not more efficient than elliptic curves for general pairing applications. They certainly have their advantages in non-pairing-based cryptosystems, and we refer the interested reader to [ACD$^+$06] and [Eng00] for information on that topic.

There are a lot of ways to use pairings in cryptography, and it would go beyond the scope of this thesis, if we would discuss them all. Therefore, we concentrate on three applications: In section VII.1, we explain a key exchange protocol for 3 participants that uses only one round of communication. The section is an elaboration of [Jou04], whereas we give all the details that are missing in that reference. The second application is the so called identity-based encryption that we discuss in section VII.2. Essentially, we quickly explain the basic scheme of [BF01]. Besides these two constructive applications, we also demonstrate destructive applications, like the MOV and the Frey-Rück attack, in section VII.3. Those attacks present ways to break the DLP of certain elliptic curves in adequate time. Last but not least, we give some examples of elliptic curve that are more suitable for pairing-based applications than others in section VII.4.

Throughout this chapter, we let E/k denote an elliptic curve defined over a finite field $k = \mathbb{F}_q$, where q is some power of a prime $p = \mathrm{char}(k)$.

VII.1 Tripartite Diffie-Hellman Protocol

Assume that Alice (A), Bob (B) and Chris (C) want to share a common secret $K_{A,B,C}$ by using only a *single round of communication*, i.e. each participant is allowed to broadcast data to the others precisely one time. In what follows, we describe a realization of this as it has been suggested by Joux in [Jou04].

The general setting is as follows: Starting from the elliptic curve E/k, an integer m coprime to p and a point $P \in E[m]$, A, B and C choose random numbers a, b and c, respectively. Then, they respectively compute $P_A = [a]P$, $P_B = [b]P$ and $P_C = [c]P$

and communicate those points to the others.

For the moment, we consider the Weil pairing e_m on $E[m]\times E[m]$. Now, every participant can, by section VI.5, easily calculate $e_m(P_B, P_C)^a$, $e_m(P_A, P_C)^b$ and $e_m(P_A, P_B)^c$, respectively which all yield the same value $e_m(P, P)^{abc}$. This value is then taken as the common secret $K_{A,B,C}$. Unfortunately, e_m is alternating and so $K_{A,B,C}$ is in fact the constant 1, which would make this exchange highly insecure. Joux presents two approaches to resolve this problem, which we will explain in the next two subsections.

VII.1.1 Two Points Approach

In chapter VI, we introduced two pairings for elliptic curves, namely the Weil and the Tate-Lichtenbaum pairing. Both of them can be used for the following tripartite Diffie-Hellman Protocol. We will start with the Weil pairing.

Using the Weil Pairing

Let m be an integer coprime to the characteristic p of k and let $l = k(E[m])$ be the field extension of k generated by the coordinates of all the points in $E[m]$. Recall that this extension is needed for the Weil pairing to be defined on the points of $E(l)[m]$, which is a finite group since l is finite. The algebraic closure of k, on the other hand, is an infinite field. So, we consider E as an elliptic curve over the bigger field l (cf. section II.8).

First of all, A, B and C publicly agree on two randomly chosen ($\mathbb{Z}_m$-linearly) independent points $P, Q \in E[m]$. This is always possible by proposition IV.2.3 (see also section VI.2), for instance, we could choose P, Q as the $\mathbb{Z}_m$-basis elements of $E[m]$. According to corollary VI.2.15 this ensures the non-degeneracy of e_m at (P, Q), i.e. $e_m(P, Q) \neq 1$. Now, the three participants respectively choose secret random numbers a, b and c and compute and distribute the tuples (P_A, Q_A), (P_B, Q_B) and (P_C, Q_C) where $P_A = [a]P, Q_A = [a]Q, P_B = [b]P, Q_B = [b]Q, P_C = [c]P, Q_C = [c]Q$. Each of them is now able to compute the common secret $K_{A,B,C}$, which is to be taken as $e_m(P, Q)^{abc}$ since

$$e_m(P_B, Q_C)^a = e_m(P_A, Q_C)^b = e_m(P_A, Q_B)^c = e_m(P, Q)^{abc}.$$

Concerning the security, we should note that an attacker could either solve the usual DHP by finding one of the secret numbers a, b or c, or he could solve the CBDHP, i.e. computing $e_m(P, Q)^{abc}$ without knowing a, b or c, respectively the DBDHP, i.e. checking whether $e_m(P, Q)^{abc} = e_m(P, Q)^r$ for some number r.

We want to summarize the steps the participant A has to perform in this protocol:

Using the Tate Pairing

The setting for the Tate Pairing is slightly different from that for the Weil pairing. We choose an elliptic curve E/k defined over k, together with a prime number $m \mid |E(k)|$,

Algorithm 8 Tripartite Diffie-Hellman using the Weil Pairing

INPUT: E/k with $\mathrm{char}(k) = p > 0$, $m \in \mathbb{Z}_{>0}$ coprime to p and independent points $P, Q \in E[m]$.

OUTPUT: The common secret $K_{A,B,C} \in \mu_m$.

1: choose $a \in_R \mathbb{N}$ $\{a \in_R \mathbb{N}$ means: a is a random element of $\mathbb{N}\}$
2: $(P_A, Q_A) \leftarrow ([a]P, [a]Q)$
3: broadcast (P_A, Q_A)
4: receive (P_B, Q_B) from B $\{P_B = [b]P$ and $Q_B = [b]Q\}$
5: receive (P_C, Q_C) from C $\{P_C = [c]P$ and $Q_C = [c]Q\}$
6: **return** $e_m(P_B, P_C)^a$

coprime to p. Assume that the embedding degree of E and m is $s > 1$, and that $m^2 \nmid |E(l)|$, where $l = k(\mu_m)$. This condition ensures, by proposition VI.4.7, that $e(P, Q) \neq 1$ for all $\mathcal{O}_E \neq P \in E(k)[m]$ and $Q \in E(l)[m] \setminus E(k)$.

Similarly to the Weil pairing, A, B and C publicly agree on a randomly chosen point $\mathcal{O}_E \neq P \in E(k)[m]$ and a randomly chosen point $Q \in E(l)[m] \setminus E(k)$, i.e. $e(P, Q) \neq 1$ as we have seen above. Now, the three participants respectively choose secret random numbers a, b and c and compute and distribute the tuples (P_A, Q_A), (P_B, Q_B) and (P_C, Q_C), where $P_A = [a]P, Q_A = [a]Q, P_B = [b]P, Q_B = [b]Q, P_C = [c]P, Q_C = [c]Q$. Each of them is now able to compute the common secret $K_{A,B,C}$, which is to be taken as $e(P, Q)^{abc}$ since

$$e(P_B, Q_C)^a = e(P_A, Q_C)^b = e(P_A, Q_B)^c = e(P, Q)^{abc}.$$

Concerning the security, we should note that an attacker could either solve the usual DHP by finding one of the secret numbers a, b or c, or he could solve the CBDHP, i.e. computing $e(P, Q)^{abc}$ without knowing a, b or c, respectively the DBDHP, i.e. checking whether $e(P, Q)^{abc} = e(P, Q)^r$ for some number r.

We want to summarize the steps the participant A has to perform in this protocol:

Algorithm 9 Tripartite Diffie-Hellman using the Tate Pairing

INPUT: E/k, prime $m \mid |E(k)|$ coprime to q with $s > 1$ and $m^2 \nmid |E(l)|$. The points $\mathcal{O}_E \neq P \in E(k)[m]$ and $Q \in E(l)[m] \setminus E(k)$.

OUTPUT: The common secret $K_{A,B,C} \in \mu_m$.

1: choose $a \in_R \mathbb{N}$
2: $(P_A, Q_A) \leftarrow ([a]P, [a]Q)$
3: broadcast (P_A, Q_A)
4: receive (P_B, Q_B) from B $\{P_B = [b]P$ and $Q_B = [b]Q\}$
5: receive (P_C, Q_C) from C $\{P_C = [c]P$ and $Q_C = [c]Q\}$
6: **return** $e(P_B, P_C)^a$

VII.1.2 Single Point Approach

As we have seen in the introduction of this section, the Weil pairing is alternating, i.e. $e_m(P,P) = 1$ for all points $P \in E[m]$. A similar thing can happen for the Tate pairing. Now, in section VI.6, we introduced the notion of modified pairings, which present a way out of this dilemma. Again, we start with the Weil pairing.

Using the Weil Pairing

The setting is the same as before, except that the elliptic curve E/k is assumed to be supersingular: Let m be a prime number coprime to the characteristic p of k and let $l = k(E[m])$ be the field extension of k generated by the coordinates of all the points in $E[m]$. Since E is supersingular, we can use the modified Weil pairing $\hat{e}_m$ instead of e_m. Recall that $\hat{e}_m$ is strongly non-degenerate.

The protocol looks as follows: A, B and C publicly agree on a randomly chosen k-rational point $\mathcal{O}_E \neq P \in E(k)$ of precise order m (such points do always exist since m is prime). Then, the three participants respectively choose secret random numbers a, b and c, and compute and distribute P_A, P_B and P_C, where $P_A = [a]P, P_B = [b]P$ and $P_C = [c]P$. Each of them is now able to compute the common secret $K_{A,B,C}$, which is to be taken as $\hat{e}_m(P,P)^{abc}$ since

$$\hat{e}_m(P_B, P_C)^a = \hat{e}_m(P_A, P_C)^b = \hat{e}_m(P_A, P_B)^c = \hat{e}_m(P,P)^{abc}.$$

By the strongly non-degenerate property of $\hat{e}_m$, $\hat{e}_m(P,P)$ is not trivial. Again, an attacker would be left with an instance of the CBDHP.

Using the Tate Pairing

Let E/k be a supersingular elliptic curve defined over k, together with a prime number $m \mid |E(k)|$, coprime to p. Assume that the embedding degree of E and m is $s > 1$, and that $m^2 \nmid |E(l)|$, where $l = k(\mu_m)$. As for the Weil pairing, we can now use the modified Tate pairing $\hat{e}$ instead of e.

The protocol looks similar to the one with the modified Weil pairing: A, B and C publicly agree on a randomly chosen k-rational point $\mathcal{O}_E \neq P \in E(k)$ of precise order m (such points do always exist since m is prime). Then, the three participants respectively choose secret random numbers a, b and c, and compute and distribute P_A, P_B and P_C, where $P_A = [a]P, P_B = [b]P$ and $P_C = [c]P$. Each of them is now able to compute the common secret $K_{A,B,C}$, which is to be taken as $\hat{e}(P,P)^{abc}$ since

$$\hat{e}(P_B, P_C)^a = \hat{e}(P_A, P_C)^b = \hat{e}(P_A, P_B)^c = \hat{e}(P,P)^{abc}.$$

By the strongly non-degenrate property of $\hat{e}$, $\hat{e}(P,P)$ is not trivial, and an attacker would be left with an instance of the CBDHP.

VII.2 Identity-Based Encryption

We will present the basic ideas of an identity-based encryption scheme that relies on the Tate pairing on elliptic curves. The scheme is due to Dan Boneh and Matthew Franklin who first proposed this idea in [BF01]. We take a slightly different approach by using the Tate pairing instead of the Weil pairing on elliptic curves. It should be noted that we only want to explain the mathematics behind the scheme and refer to [BF01] for a more complete description and security discussions.

VII.2.1 Introduction

In chapter I, we introduced the basic notions of public-key cryptography, of which we make use now. Assume that Alice (A) wants to send Bob (B) an encrypted message by using Bob's public key. As it turned out (see man-in-the-middle attack), B needs to give A some kind of proof of his identity. To avoid this problem, we give B a certain public key that is uniquely identifiable with his identity (e.g. his social security number or his email address). This is the main idea of *identity-based cryptography*.

Recall from chapter I that we firstly generated a private key and then associated a public key. In identity-based cryptography, we do this the other way around, i.e. we firstly take a public key, which is uniquely identifiable with the user's identity, and then somehow derive the private key from it. Obviously, this cannot be done by the user him/herself, but has to be done by some *trusted authority (TA)*. The TA has some additional secret information about the user, the so called *master key*. The user's private key is then computed by some one-way function of the public and master key.

Before we are able to describe the scheme, we need the following definition.

Definition VII.2.1. Let $H : S \to T$ be a map between two sets S and T. We call H a *(cryptographic) hash function*, if the following conditions are satisfied.

1. For an element $s \in S$, we can compute $H(s)$ in polynomial time.

2. (*preimage resistant*) For an element $t \in T$, it is computationally infeasible to find $s \in S$ with $H(s) = t$.

3. (*strongly collision-free*) It is computationally infeasible to find distinct elements $s_1, s_2 \in S$ with $H(s_1) = H(s_2)$.

Usually, one takes $S = \{0,1\}^*$, the set of all finite sequences consisting of 0's and 1's (= set of all words over the alphabet $\{0,1\}$), and $T = \{0,1\}^n$, the set of all words of length n. This construction allows us to efficiently reduce a word of arbitrary length to a word of the fixed length n (e.g. $n = 160$, so it is a 160-bit word). In this context, we will always assume that points on a curve and elements of finite fields are given in binary form, i.e. as elements of $\{0,1\}^*$. There are several prominent examples of such functions, like MD5 and the secure hash algorithm (see [MvOV96]). Since we do not want to discuss more details, we refer to chapter 4 in [Sti95], which gives a very nice introduction on the topic.

VII.2.2 The Scheme

As we have explained before, the participants do not possess private keys until the TA sets the system up and distributes the private keys to their owners on demand. So this is the first step, we want to describe.

Setup: The TA chooses

- a supersingular elliptic curve E/k defined over a finite field $k = \mathbb{F}_q$ with q elements, together with a prime number $m \mid |E(k)|$ (coprime to q), but $m^2 \nmid |E(k)|$, such that the embedding degree of E and m is $s > 1$.
- a k-rational point $\mathcal{O}_E \neq P \in E(k)$ of order m (this is possible since $m \mid |E(k)|$ is prime).
- two hash functions $H_1 : \{0,1\}^* \to E(k)[m] \setminus \{\mathcal{O}_E\}$ and $H_2 : \mu_m \to \{0,1\}^n$, where n is the fixed length of the messages that can be sent.
- the master-key $r \in \mathbb{Z}$ with $1 \leq r < m$.

Then, the TA computes $P_{\text{pub}} = [r]P$ and makes the chosen system parameters

$$q, E, m, P, H_1, H_2, n, P_{\text{pub}}$$

publicly available.

The next step would be for a user (with identity $\mathcal{ID} \in \{0,1\}^*$) to extract his/her private key from the TA.

Extract: The TA

- computes $\mathcal{O}_E \neq Q_{\mathcal{ID}} = H_1(\mathcal{ID}) \in E(k)[m]$.
- computes $d_{\mathcal{ID}} = [r]Q_{\mathcal{ID}}$ (the user's private key).
- verifies that $\mathcal{ID}$ is the identification for the user, and sends $d_{\mathcal{ID}}$ to him/her.

Finally, we can encrypt messages $M \in \{0,1\}^*$ under the public key $\mathcal{ID}$ by doing the following.

Encrypt: The user

- computes $Q_{\mathcal{ID}} = H_1(\mathcal{ID})$.
- chooses a random integer $1 \leq t < m$.
- computes $1 \neq g_{\mathcal{ID}} = \hat{e}(Q_{\mathcal{ID}}, P_{\text{pub}}) \in \mu_m$, where $\hat{e} : \langle P \rangle \times \langle P \rangle \to \mu_m$ is the modified Tate pairing.
- sets the ciphertext to be the pair

$$C = ([t]P, M \oplus H_2(g_{\mathcal{ID}}^t)),$$

where $\oplus$ denotes XOR, i.e. the bitwise addition modulo 2.

Now, to decrypt a ciphertext $C = (U, V)$ that was encrypted by the above method using the public key $\mathcal{ID}$ works as follows.

Decrypt: The user (with identification $\mathcal{ID}$)

- uses his/her private key $d_{\mathcal{ID}}$ to compute the message

$$m = V \oplus H_2(\hat{e}(d_{\mathcal{ID}}, U)).$$

We want to verify that the decryption indeed returns the original message M, if it was encrypted with the public key $\mathcal{ID}$, i.e. $C = (U, V) = ([t]P, M \oplus H_2(g_{\mathcal{ID}}^t))$. We have

$$\hat{e}(d_{\mathcal{ID}}, U) = \hat{e}([r]Q_{\mathcal{ID}}, [t]P) = \hat{e}(Q_{\mathcal{ID}}, P)^{rt} = \hat{e}(Q_{\mathcal{ID}}, P_{\text{pub}})^t = g_{\mathcal{ID}}^t,$$

i.e. $m = V \oplus H_2(\hat{e}(d_{\mathcal{ID}}, U)) = M \oplus H_2(g_{\mathcal{ID}}^t) \oplus H_2(g_{\mathcal{ID}}^t) = M$, since $H_2(g_{\mathcal{ID}}^t) \oplus H_2(g_{\mathcal{ID}}^t)$ is just the word in $\{0,1\}^n$ that consists only of zeros.

VII.3 Attacks with Pairings

In the two previous sections, we explained ways to use pairings on elliptic curves in cryptography, positively. But there are also ways to use them in a destructive manner. In chapter I, we introduced the discrete logarithm problem for a given cyclic group G. Here, we consider $G = \langle P \rangle$ for a point P of prime order m on some elliptic curve E/k defined over $k = \mathbb{F}_q$. The DLP in such a group (at least in the most general situation) is believed to have exponential complexity (see section I.1.1). We want to give examples of curves for which the DLP has a complexity that is at most subexponential. If E is supersingular, there is a non-degenerate pairing

$$\tau : \langle P \rangle \times \langle P \rangle \to \mu_m,$$

which is either derived from the Weil or the Tate pairing. This means that we are actually looking at a DL system with bilinear structure.

At this point, we would like to remind the reader of the *index calculus* algorithm, which is a mean to attack the DLP in certain finite groups efficiently. Important to us is the fact that this is the case for the multiplicative group of a finite field, as long as its number of elements is not "too big". The interested reader is refered to [ACD+06, Ch. 20, p. 495] for the actual algorithm and other details. Here, we only want to state the fact that the index calculus algorithm runs in subexponential time in the multiplicative group of a finite field.

Since μ_m is a subgroup of the multiplicative group of some finite field, one might ask whether it is possible to "transfer" the DLP in G to a DLP in μ_m. In this section, we want to show how this works for certain elliptic curves.

VII.3.1 The MOV Attack

We want to use the Weil pairing to attack a DLP in the group of points on an elliptic curve. Recall from section VI.2 that we need to work over a "big enough" field l in order for the Weil pairing to be non-degenerate over l. Therefore, let E/k be an elliptic curve over $k = \mathbb{F}_q$ with a prime number $m \mid |E(k)|$, coprime to q. As we just recalled, the Weil pairing is not necessarily defined over k, and so we let $l := k(E[m]) = \mathbb{F}_{q^s}$, where $s \in \mathbb{Z}_{\geq 0}$, be the smallest field extension of k generated by the coordinates of all the points of $E[m]$, i.e. $E[m] \subseteq E(l)[m]$. Note that s is not necessarily the embedding degree as we have defined it in section VI.3. Moreover, let $P, Q \in E(k)[m]$ be k-rational points of order m.

We want to determine $r \in \mathbb{Z}_m^*$ such that $Q = [r]P$ (while assuming that such r exists). The MOV attack, which is named after its inventors Menezes, Okamoto and Vanstone, transfers this problem to a DLP in l^*. We present this method as described in [MOV91], summarized in algorithm 10.

Algorithm 10 The MOV attack

INPUT: $P, Q \in E(k)$ of order m with $Q = [r]P$ for some unknown $r \in \mathbb{Z}_m^*$.
OUTPUT: $r = \log_P(Q)$.

1: **repeat**
2: choose $S \in_R E(l) \setminus E(k)$
3: **until** $e_m(P, S) \neq 1$
4: $\zeta_1 \leftarrow e_m(P, S)$
5: $\zeta_2 \leftarrow e_m(Q, S)$
6: compute $r \leftarrow \log_{\zeta_1}(\zeta_2)$ by using index calculus
7: **return** r

Proof of algorithm 10. First of all, the repeat-loop terminates after finitely many steps, since e_m is non-degenerate, i.e. it certainly exists a point $S \in E(l)$ such that $e_m(P, S) \neq 1$.

Now assume that we computed $r = \log_{\zeta_1}(\zeta_2)$ in step 6, then:

$$e_m([r]P, S) = e_m(P, S)^r = e_m(Q, S),$$

so $e_m([r]P - Q, S) = 1$, but P and Q are $\mathbb{Z}_m$-linearly dependent by assumption and so $[r]P = Q$ by the choice of S (cf. corollary VI.2.15). Obviously, this only works because m is prime. □

Remark VII.3.1. We want to remark that the repeat-loop usually terminates after one time, since the probability of a random point $S \in E(l)$ satisfying $e_m(P, S) \neq 1$ is overwhelmingly high (see [Was03, Ch. 5, remark 5.2, p. 156]).

VII.3.2 The Frey-Rück Attack

While the MOV attack uses the Weil pairing, it seems natural to ask for a version using the Tate pairing. In fact, a translation for the Tate pairing turns out to be

trivial, as Frey and Rück pointed out in [FR94]. It is the same algorithm as algorithm 10 by interchanging the Weil pairing with the Tate pairing. So instead of stating the algorithm again, we want to slightly modify it to run more efficiently in certain cases.

We are assuming the following situation: Let E/k be an elliptic curve over $k = \mathbb{F}_q$ with a prime number $m \mid |E(k)|$ (coprime to q) and $m^2 \nmid |E(k)|$ such that the embedding degree of E and m is $s > 1$.

By proposition VI.4.7, we know that for points $\mathcal{O}_E \neq P \in E(k)[m]$ and $S \in E(l)[m] \setminus E(k)$, with $l := k(\mu_m)$, we have $e(P, S) \neq 1$, whereas e denotes the Tate pairing. In this situation, the Frey-Rück attack looks as follows:

Algorithm 11 The Frey-Rück attack

INPUT: $P, Q \in E(k)$ of order m with $Q = [r]P$ for some unknown $r \in \mathbb{Z}_m^*$.
OUTPUT: $r = \log_P(Q)$.

1: choose $S \in_R E(l)$ with $S \notin mE(l)$
2: $\zeta_1 \leftarrow e_m(P, S)$
3: $\zeta_2 \leftarrow e_m(Q, S)$
4: compute $r \leftarrow \log_{\zeta_1}(\zeta_2)$ by using index calculus
5: **return** r

Proof of algorithm 11. Recall that, in our situation, we have an isomorphism

$$E(l)[m] \cong E(l)/mE(l).$$

So, since $S \notin mE(l)$, this means that it is a point of order m, and we have $e(P, S) \neq 1$ by the above. Choosing S is trivial by picking a random point $S \in E(l)$ and then check whether $[\frac{q^s-1}{m}]S \neq \mathcal{O}_E$. The rest of the proof works exactly like the proof of algorithm 10. □

VII.4 Pairing-Friendly Elliptic Curves

In the previous section, we have met a method to attack a DLP on an elliptic curve. This attack was only efficient, if the pairing could be computed efficiently, and if the index calculus algorithm worked fast enough. A natural question is, whether there are certain curves for which the pairing can be computed quickly, and whether there are curves for which the attacks of section VII.3 run fast. In the latter case, an elliptic curve is said to be *weak*, and in the former, it is called *pairing-friendly*. In terms of Miller's algorithm, an elliptic curve is pairing-friendly, if it has an embedding degree of moderate size. As a consequence of theorem IV.3.2, we have the following result, which was first proved by Menezes, Okamoto and Vanstone in [MOV91].

Corollary VII.4.1. Supersingular elliptic curves are pairing-friendly, since they have an embedding degree $s \leq 6$.

Proof. Trivial by theorem IV.3.2. □

We want to give another example of a pairing-friendly elliptic curve. Frey, Müller and Rück proved in [FMR99] that there are elliptic curves (not necessarily supersingular) with embedding degree 1. We need the following definition.

Definition VII.4.2. Let E/k be an elliptic curve over $k = \mathbb{F}_q$. By the Hasse-Weil bound (see theorem III.4.4), we know that

$$|E(k)| = q + 1 - t,$$

where $t \in \mathbb{Z}$ with $|t| \leq 2\sqrt{q}$. This value t is called the *trace* of E over k.

Proposition VII.4.3. Let E/k be an elliptic curve over $k = \mathbb{F}_q$ with an integer $m \mid |E(k)|$, coprime to q. If the trace t of E over k is congruent to 2 modulo m, then the embedding degree of E and m is $s = 1$, i.e. E is pairing-friendly.

Proof. Assume that $t \equiv 2 \pmod{m}$, i.e. it exists $a \in \mathbb{Z}$ with $a \cdot m = t - 2$. Furthermore, it exists $b \in \mathbb{Z}$ with $b \cdot m = |E(k)|$ by assumption. By definition, we have

$$t - 2 = q - 1 - |E(k)|,$$

i.e. $(a + b)m = q - 1$, which means that $s = 1$. □

Appendix A

Galois Cohomology

In this short appendix, we would like to give a very brief summary of results on Galois cohomology. We mostly rely on [Sil86], although the reader is better off by consulting books like [Ser01] or [Ser79].

Let k be a perfect field with a fixed algebraic closure K, and let $G_{K/k}$ denote the Galois group of the Galois extension K/k. Recall that $G_{K/k}$ is a profinite group (see e.g. [Bos04, Ch. 4, Satz 2.7, p. 153]).

Definition A.0.4. Let M be an additively written Abelian group on which $G_{K/k}$ acts. If the $G_{K/k}$-action on M is continuous with respect to the profinite topology on $G_{K/k}$ and the discrete topology on M, we say that M is a *(discrete) $G_{K/k}$-module*.

Example A.0.5.

1. K and K^* certainly are $G_{K/k}$-modules with the natural action of $G_{K/k}$ on K resp. K^* (cf. [Sil86, Example B.2.1.1, p. 333]).

2. If $V \subseteq \mathbb{A}^n$ is an affine variety defined over k, then $I(V/K)$ is an ideal of $K[X_1, \ldots, X_n]$, generated by finitely many elements of $k[X_1, \ldots, X_n]$, and so, in particular, an (additive) Abelian group on which $G_{K/k}$ acts. That the action of $G_{K/k}$ is continuous follows immediately from example 1. So $I(V/K)$ is a $G_{K/k}$-module.

Definition A.0.6. Let M be a $G_{K/k}$-module. The group of $G_{K/k}$-invariant elements of M,

$$H^0(G_{K/k}, M) := \{m \in M \mid \sigma(m) = m \text{ for all } \sigma \in G_{K/k}\},$$

is called the 0*-th cohomology group of* M.

Using the additional property of $G_{K/k}$ being profinite, we can define the following:

Definition A.0.7. Let M be a $G_{K/k}$-module.

1. Whenever a map $\xi : G_{K/k} \to M$ is continuous with respect to the profinite topology on $G_{K/k}$ and the discrete topology on M, we simply say that ξ is *continuous*.

2. The *group of contiuous 1-cocycles (from $G_{K/k}$ to M)* is defined by

$$\begin{aligned} Z^1_{\text{cont}}(G_{K/k}, M) := \{\xi : G_{K/k} \to M \mid \xi \text{ continuous map,} \\ \xi(\sigma \circ \tau) = \sigma(\xi(\tau)) + \xi(\sigma) \text{ for all } \sigma \in G_{K/k}\}. \end{aligned}$$

This is indeed a group, as one easily verifies.

3. The *group of (continuous) 1-coboundaries (from $G_{K/k}$ to M)* is defined by

$$B^1(G_{K/k}, M) := \{\xi : G_{K/k} \to M \mid \exists m \in M : \\ \xi(\sigma) = \sigma(m) - m \text{ for all } \sigma \in G_{K/k}\}.$$

Clearly, $B^1(G_{K/k}, M)$ is a subgroup of $Z^1_{\text{cont}}(G_{K/k}, M)$.

4. The *1-st cohomology group of M* is defined by

$$H^1(G_{K/k}, M) := Z^1_{\text{cont}}(G_{K/k}, M)/B^1(G_{K/k}, M).$$

The next result will summarize all properties of the cohomology groups that are of importance to our purposes.

Proposition A.0.8. 1. (Hilbert theorem 90) The 1-st cohomology group of the $G_{K/k}$-module K^* is trivial, i.e.

$$H^1(G_{K/k}, K^*) = 0.$$

2. (Additive version of Hilbert theorem 90) The 1-st cohomology group of the $G_{K/k}$-module K is trivial, i.e.

$$H^1(G_{K/k}, K) = 0.$$

Proof. See for instance [Sil86, Proposition B.2.5, p. 335]. □

Bibliography

[ACD+06] Roberto Avanzi, Henri Cohen, Christophe Doche, Gerhard Frey, Tanja Lange, Kim Nguyen, and Frederik Vercauteren, *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Mathematics and its Applications, CRC Press, 2006.

[AM69] M. F. Atiyah and I. G. MacDonald, *Introduction to commutative algebra*, Addison-Wesley, 1969.

[BB96] G. Brassard and P. Bratley, *Fundamentals of algorithmics*, Prentice Hall, 1996.

[BF01] D. Boneh and M. Franklin, *Identity-based encryption from the weil pairing*, Advances in Cryptology - CRYPTO 2001 **2139** (2001), 213–229.

[Bos04] S. Bosch, *Algebra*, fifth ed., Springer-Verlag, 2004.

[Bou59] N. Bourbaki, *Algebrè*, Éléments de Mathématique, Hermann, 1959.

[BSS05] Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart, *Advances in elliptic curve cryptography*, Cambridge University Press, 2005.

[Can87] David G. Cantor, *Computing in the jacobian of a hyperelliptic curve*, Math. Comp. **48** (1987), no. 177, 95–101.

[Coh96] Henri Cohen, *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*, Springer-Verlag, 1996.

[DH76] Whitfield Diffie and Martin E. Hellman, *New directions in cryptography*, IEEE Transactions on Information Theory **22** (1976), no. 6, 644–654.

[Eis99] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, volume 150 of *Graduate Texts in Mathematics*, Springer-Verlag, 1999.

[Eng00] Andreas Enge, *Hyperelliptic cryptosystems: Efficiency and subexponential attacks*, Books on Demand GmbH, 2000.

[FMR99] Gerhard Frey, Michael Müller, and Hans-Georg Rück, *The tate pairing and the discrete logarithm applied to elliptic curve cryptosystems*, IEEE Transactions on Information Theory **45** (1999), no. 5, 1717–1719.

[FR94] G. Frey and H.-G. Rück, *A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves*, Math. Comp. **62** (1994), 865–874.

[Gal01] Steven D. Galbraith, *Supersingular curves in cryptography*, Advances in Cryptology - Asiacrypt 2001 **2248** (2001), 495–513.

[Gar04] Theodoulos Garefalakis, *The generalized weil pairing and the discrete logarithm problem on elliptic curves*, Theor. Comput. Sci. **321** (2004), no. 1, 59–72.

[Gau01] Carl Friedrich Gauß, *Disquisitiones arithmeticae*, Gerh. Fleischer Jun., 1801.

[GHV07] Steven D. Galbraith, Florian Hess, and F. Vercauteren, *Hyperelliptic pairings*, Pairing-Based Cryptography - Pairing 2007 (T. Takagi et al, ed.), Lecture Notes in Computer Science, vol. 4575, Springer-Verlag, 2007, pp. 108–131.

[Har77] R. Hartshorne, *Algebraic geometry*, volume 52 of *Graduate Texts in Mathematics*, Springer-Verlag, 1977.

[Hes04] F. Hess, *A note on the tate pairing of curves over finite fields*, Arch. Math. (Basel) **82** (2004), 28–32.

[Jou02] Antoine Joux, *The weil and tate pairings as building blocks for public key cryptosystems*, ANTS-V: Proceedings of the 5th International Symposium on Algorithmic Number Theory, Springer-Verlag, 2002, pp. 20–32.

[Jou04] ———, *A one round protocol for tripartite diffie-hellman*, Journal of Cryptology **17** (2004), 263–276.

[Kob89] Neal Koblitz, *Hyperelliptic cryptosystems*, Journal of Cryptology **1** (1989), 139–150.

[Kob99] ———, *Algebraic aspects of cryptography*, Algorithms and Computation in Mathematics, vol. 3, Springer-Verlag, 1999.

[KS04] H. Kurzweil and B. Stellmacher, *The theory of finite groups: An introduction*, Springer-Verlag, 2004.

[Kun85] E. Kunz, *Introduction to commutative algebra and algebraic geometry*, Birkhäuser, 1985.

[Lag73] J.-L. Lagrange, *Recherches d'arithmétique*, Nouveaux Mémoires de l'Académie Royale des Sciences et Belles-Lettres (1773), 265–312.

[Lan02] S. Lang, *Algebra*, third ed., volume 211 of *Graduate Texts in Mathematics*, Springer-Verlag, 2002.

[Mat80] Hideyuki Matsumura, *Commutative algebra*, second ed., Benjamin / Cummings, 1980.

[Men93] Alfred J. Menezes, *Elliptic curve public key cryptosystems*, Kluwer Academic Publishers, 1993.

[Mil04] Victor S. Miller, *The weil pairing, and its efficient calculation*, Journal of Cryptology **17** (2004), no. 4, 235–261.

[MOV91] Alfred Menezes, Tatsuaki Okamoto, and Scott Vanstone, *Reducing elliptic curve logarithms to logarithms in a finite field*, STOC '91: Proceedings of the twenty-third annual ACM symposium on Theory of computing, ACM, 1991, pp. 80–89.

[MvOV96] A. J. Menezes, P. van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*, Discrete Mathematics and its Applications, CRC Press, 1996.

[PS98] Sachar Paulus and Andreas Stein, *Comparing real and imaginary arithmetics for divisor class groups of hyperelliptic curves*, Algorithmic Number Theory (J. P. Buhler, ed.), Lecture Notes in Computer Science, vol. 1423, Springer-Verlag, 1998, pp. 576–591.

[Sal06] Gabriel Daniel Villa Salvador, *Topics in the theory of algebraic function fields*, Birkhäuser, 2006.

[Ser79] J.-P. Serre, *Local fields*, Springer-Verlag, 1979.

[Ser01] ———, *Galois cohomology*, Springer-Verlag, 2001.

[Sil86] J. H. Silverman, *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*, Springer-Verlag, 1986.

[Sti93] Henning Stichtenoth, *Algebraic function fields and codes*, Springer-Verlag, 1993.

[Sti95] Douglas Stinson, *Cryptography: Theory and pratice*, Discrete Mathematics and its Applications, CRC Press, 1995.

[vdW71] B. L. van der Waerden, *Algebra*, vol. 1, Springer-Verlag, 1971.

[Ver04] Eric R. Verheul, *Evidence that xtr is more secure than supersingular elliptic curve cryptosystems*, Journal of Cryptology **17** (2004), no. 4, 277–296.

[Was03] Lawrence C. Washington, *Elliptic curves: Number theory and cryptography*, Discrete Mathematics and its Applications, CRC Press, 2003.

[Wat69] E. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. **4** (1969), 521–560.

[ZS75] O. Zariski and P. Samuel, *Commutative algebra*, volume 28 of *Graduate Texts in Mathematics*, vol. 1, Springer-Verlag, 1975.

[ZS76] ———, *Commutative algebra*, volume 29 of *Graduate Texts in Mathematics*, vol. 2, Springer-Verlag, 1976.

Erklärung

Hiermit versichere ich, dass ich diese Arbeit selbständig verfasst und keine anderen als die angegebenen Hilfsmittel und Quellen benutzt habe.