Construction of algebraic correspondences between hyperelliptic function fields using Deuring's theory

Georg Kux

Vom Fachbereich Mathematik
der Universität Kaiserslautern
zur Verleihung des akademischen Grades
Doktor der Naturwissenschaften
(Doctor rerum naturalium, Dr. rer. nat.)
genehmigte Dissertation.

1. Gutachter: Dr. habil. Andreas Guthmann
2. Gutachter: Prof. Dr. Hans-Georg Rück

Disputation: 4. Februar 2004

D 386

Für Mara Louisa

Acknowledgement
I would like to thank my supervisor Privat-Dozent Dr. Andreas Guthmann for introducing me to the topic and giving good advice and encouragement. Moreover I thank Professor Hans-Georg Rück and Dr. Steven Galbraith for several comments and discussions.
Special thanks go to Dr. Bernd Kuhlmann and the BGS Systemplanung AG, who provided the financial support for this work as well as Professor Damian Weber, who initiated the project and has always been a good advisor. I would also like to thank the ITWM and in particular the department MAB headed by Dr. Ronald Rösch for their support and the pleasant working atmosphere. Furthermore I want to express my gratitude to all people that had the ambition to read this thesis completely and gave me useful suggestions concerning its content and diction.
Finally I wish to thank my family including my godmother and godfather as well as all of my friends who supported me during my studies.

Contents

CHAPTER 0

Introduction

1. Motivation

Nowadays we cannot imagine secure electronic communication without the help of public key cryptosystems. Many protocols make use of this technique and would be impossible without it. One of the first and still the most popular of these asymmetric encryption algorithms is RSA (named after its inventors Rivest, Shamir and Adleman). Its security relies on the fact that factoring a ´large´ integer which is known to be the product of two primes of similar size is supposed to be a computationally difficult problem.
Nevertheless good progress has been made in factoring due to the so-called number field sieve algorithm. The current factoring record lies at 158 decimal digits for the composite number, which means that RSA-keys of a length of 512 Bits can no longer guarantee security.
Considering this development, it is important to have alternatives available. Many proposals have been made, most of which are not competitive to RSA concerning running time and security per key-length.
Elliptic curves, however, have proved to be a good choice for building public key cryptosystems which can seriously compete with RSA. Their security relies on the problem of computing logarithms in the group of points of an elliptic curve. Since this is supposed to be hard for relative small parameters, they offer high grade security even for small keys and are therefore the optimal choice for smart cards and other environments that provide only a very limited storage space.
As generalisations, hyperelliptic curves have been proposed for cryptographic purposes by Koblitz in 1988 [**Kob89**]. Although the set points of a hyperelliptic curve itself in general does not allow a group structure, we can use the so-called Jacobi group instead and it is assumed that the discrete logarithm problem (DLP) in this group is, at least for hyperelliptic curves of small genus $g = 2, 3$ and 4, as secure as the elliptic case.
Although many cryptographers did not believe in the practability of hyperelliptic curve cryptosystems the last years have shown that the arithmetic can be sped up considerably ([**GLS01**], [**PWGP03**] [**PWP03**], [**BCLW02**]) and they represent an alternative to elliptic curve systems and RSA indeed.
To solve the discrete logarithm problem in the Jacobi group several techniques have been developed. Firstly, there are the generic squareroot attacks such as the Pollard Rho, kangaroo and baby step giant step algorithms, which can be applied to any abelian group. As their name says, they all have a running time of $O(\sqrt{n})$ where n is the order of the respective group. For more details see [**Tes01**].
Another generic method is the one of Pohlig and Hellman [**Poh78**]. Here the DLP of the whole group is reduced to the DLP in smaller subgroups using the Chinese remainder theorem. The running time depends on the largest prime factor of the number of elements of the group. If the group order splits into small primes, this algorithm performs better than the squareroot attacks.
Frey and Rück [**FR94**] showed that there is an additional class of curves we have to

avoid, namely those for which the cardinality of the field $q = p^n$ has a small order modulo the large prime l dividing the group order. In this case with the help of the Tate pairing the DLP in the Jacobian can be reduced to a DLP in the multiplicative group of the finite field $\mathbb{F}_{p^n}$, which is much easier to solve due to index calculus methods. This means that in particular supersingular curves are cryptographically not suitable. Moreover Rück [**Rüc99**] showed that the DLP in Jacobians defined over a finite field of characteristic p and having a cyclic group structure of order p^n can be solved in time $O(n^2 log p)$.
If the Jacobian has an automorphism of the order m, Duursma, Gaudry and Morain proved that one can speed up the discrete logarithm computation by a factor of $\sqrt{m}$. As a consequence one should not choose curves with many automorphisms.
Gaudry [**Gau00**] was able to show the somewhat surprising fact that there exists an algorithm to solve the DLP in Jacobians of curves of genus greater than 4, that is faster than the generic squareroot attacks. He developed a variant of the Adleman DeMarrais Huang algorithm [**ADH94**] which in original form computes discrete logarithms in subexponential time, assuming the genus is sufficiently large compared to the size of the ground field. Moreover, he makes use of automorphisms of order m to speed up his computations even by a factor m^2, which becomes very significant in practice. To demonstrate his method, Gaudry broke a cryptosystem based on a genus 6 curve formerly supposed to be secure by Koblitz.
To construct a secure cryptosystem we have to choose the Jacobian of a curve of genus 2 or 3 (and maybe even 4) that resists all known attacks and the group order of which can be computed in an acceptable time. The latter condition is the main reason why hyperelliptic curve cryptosystems have not yet established in practice. Unlike the elliptic case, where we have Schoof's algorithm [**Sch95**] and extensions, in the hyperelliptic case a technique to compute in reasonable time the number of elements of the Jacobian of a randomly chosen curve over a field of large characteristic has not yet been found up to now. Nevertheless, there are several possibilities to construct curves which resist all known attacks.
First there is the method to compute the cardinality of the Jacobian over some finite field $\mathbb{F}_p$, where p is a small prime. Using the zeta function we obtain the cardinality over an extension $\mathbb{F}_{p^n}$. Those were the first examples for cryptographically suited hyperelliptic curves. Koblitz proposed them in his original paper [**Kob89**] and they are named after him.
Another way is to use the theory of complex multiplication. The idea is to choose a suitable large prime, a group order and a number field, the maximal order of which is isomorphic to the endomorphism ring of the Jacobian we want to construct. Using several invariants and an algorithm of Mestre we can compute the defining equation of a hyperelliptic curve with the above property. More details can be found in [**Wen03**] or [**CMT00**]. Although this kind of curves seems to be special in some sense, an attack on them is not known yet.
If we want to compute the cardinality of the Jacobian of a randomly chosen hyperelliptic curve, there are several possibilities. During the last years many improvements have been made concerning ground fields of characteristic 2 culminating in the algorithm of Harley. Mestre showed that Richelot's isogeny can be used to generalise Satoh's canonical lift algorithm to genus 2. In this case the running time is almost the same as for elliptic curves. Another point counting algorithm has been proposed by Kedlaya [**Ked01**]. He uses the so-called Monsky-Washnitzer cohomology and with a trick Matsuo, Chao and Tsujii [**MCT02**] have been able to obtain cryptographically relevant sizes for medium characteristics. In large characteristics the best algorithms are similar to Schoof's [**Sch95**]. Actually Gaudry holds the record with a computation time of one week for a genus 2 curve with a Jacobian of

cardinality $\sim 2^{164}$. Up to now no practible method is known for curves of higher genus. So there is still a lot of research to be done in this area.

2. Outline

The aim of this thesis is to construct new classes of non-trivial homomorphisms between the Jacobi groups of hyperelliptic function fields. To achieve this we apply the classical theory of algebraic correspondences introduced by Max Deuring in [**Deu37**]. Finding such non-trivial homomorphisms automatically yields connections between the structure and consequently also the security of the respective Jacobians in cryptographical applications.
In the first chapter we introduce the reader to the basic objects we deal with. We differentiate between ideal theory, valuation theory and algebraic geometry and show how to translate the objects from one language to the other.
The second part summarises the theory of algebraic correspondences in the classical language given by Deuring specialised to hyperelliptic function fields. These are the foundations the rest of this thesis relies on.
In the following chapter we derive algorithms that enable us to perform multiplication and composition of correspondences. It is not surprising that these are not practicable in general. Note that already in the elliptic case for example a general expression for the m-th multiple of a point can only be described by division polynomials, the degree of which increases quadratically in m. Nevertheless they can be used under certain assumptions.
Chapter 4 covers several construction methods for non-trivial algebraic correspondences. First we take advantage of what is known about the factorisation of a certain kind of bivariate polynomials in order to find hyperelliptic function fields the Jacobians of which have some special properties. Afterwards we illuminate the well known Richelot isogeny for genus 2 curves in the sense of an algebraic correspondence and show how to generalise it to higher genus. For genus 3 to 5 we give an explicit sufficient criterion for the existence of a generalised Richelot isogeny in terms of the coefficients of the defining equation. Finally we derive an explicit method to construct genus 2 hyperelliptic function fields, the endomorphism ring of which allows a multiplication by $\sqrt{2}$ using Cholesky decomposition.

Notation

$\mathbb{N}$	natural numbers
$\mathbb{Z}$	rational integers
$\mathbb{Q}$	rational numbers
$\mathbb{R}$	real numbers
$\mathbb{C}$	complex numbers
$\mathbb{H}$	quaternion algebra
$\mathbb{F}_q$	finite field with $q = p^m$ elements
$\mathrm{char}(k)$	characteristic of a field k
$\bar{k}$	algebraic closure of k
t,x	transcendental variables over some basic field k
$k[t]$	polynomial ring in t over the field k
$k(t)$	quotient field of $k[t]$, rational function field
D	separable polynomial over some field k
lc	leading coefficient of a polynomial
u	placeholder for $\sqrt{D(t)}$, i.e. $u^2 = D(t)$
y	placeholder for $\sqrt{D(x)}$, i.e. $y^2 = D(x)$
$\mathcal{P}$	point on a hyperelliptic curve
$\mathrm{N}_{L\|K}$	norm map
$\mathrm{Tr}_{L\|K}$	trace map
$L\|k$	algebraic function field over k
$[L : K]$	degree of the field extension $L\|K$
$\mathrm{PDiv}(L\|k)$	set of prime divisors of $L\|k$
$\mathrm{Jac}(L\|k)$	Jacobi group of $L\|k$
$\mathrm{Div}(L\|k)$	divisor group of $L\|k$
$\mathrm{cDiv}(L\|k)$	divisor class group of $L\|k$
$\mathrm{Div}_0(L\|k)$	group of degree 0 divisors of $L\|k$
$\mathrm{Princ}(L\|k)$	group of principal divisors of $L\|k$
$\mathrm{Div}^c(\Lambda\|L_1)$	group of coarser divisors in the double field $\Lambda\|L_1$
$\mathrm{cDiv}^c(\Lambda\|L_1)$	class group of coarser divisors in the double field $\Lambda\|L_1$
$v_\mathfrak{p}$, $w_\mathfrak{p}$	discrete valuations corresponding to $\mathfrak{p}$
gcd	greatest common divisor
lcm	least common multiple
$\mathrm{supp}\,\mathfrak{d}$	support of the divisor $\mathfrak{d}$
$\mathrm{Hom}(G_1, G_2)$	group of group-homomorphisms from G_1 to G_2
$\mathrm{ord}_\mathfrak{p}$	order at the place/prime divisor $\mathfrak{p}$
$\mathrm{Val}(L\|k)$	set of valuations of $L\|k$
$\mathrm{End}(L\|k)$	endomorphism ring of the Jacobi group of $L\|k$
$\mathrm{Hom}(L_1, L_2)$	$\mathrm{Hom}(\mathrm{Jac}(L_1), \mathrm{Jac}(L_2))$
$\mathrm{Cor}(L\|k)$	ring of correspondences of $L\|k$
$\mathrm{Aut}(\bar{k}\|k)$	group of automorphisms of $\bar{k}\|k$
$\Lambda\|L_1$	double field L_1L_2 considered as function field over L_1
L_1^*	image of Λ under the residue class map of some non-constant prime divisor
$\overline{L}_2$	isomorphic image of L_2 under the residue class map of some non-constant prime divisor
$\mathcal{R}$	ring compositum of fields L_1 and L_2
$\mathrm{Mat}(m, n, R)$	ring of $m \times n$-matrices over R
$\mathrm{Mat}_n(R)$	ring of $n \times n$-matrices over R
$[m]$	multiplication by m map in the endomorphism ring

General remarks:
Elements of fields $k = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ or $\mathbb{F}_q$ are named with lower case Latin letters $(a, b, c, \dots)$. Polynomials or fractions of polynomials are usually indicated by capital Latin letters $(A, B, C, \dots)$. We denote ideals and divisors by small Gothic letters $(\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{d}, \dots)$. Prime ideals, prime divisors/places are usually called $\mathfrak{p}$ or $\mathfrak{q}$. When we talk of divisors and ideals of double fields in general we use capital Gothic letters $(\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \dots)$ and $(\mathfrak{A}_x, \mathfrak{B}_x, \mathfrak{C}_x, \dots)$ respectively. Here x represents the transcendental element of $L_2 = k(x, \sqrt{D(x)})$. Elements of function fields are sometimes denoted by small Greek letters $(\alpha, \beta, \gamma, \dots)$, whereas capital Greek letters generally represent maps. If some product extends a line, we will mark it with a $\times$ to indicate that the term continues in the next line.

CHAPTER 1

Quadratic function fields

In this chapter we will collect some background material most of which can be found in standard algebra books. We will only supply the reader with proofs of theorems that lead to algorithms or cannot be found in common literature on the topic.
Starting with the arithmetical aspects of ideals in quadratic function fields we continue with some basic facts from valuation theory and finally come to a geometrical interpretation of the objects we have introduced. The ideal theoretic approach applies to every field, whereas the valuation theory and geometry in the first chapter are only considered over perfect fields k.
The basic objects we are dealing with are algebraic extensions L of the rational function field $k(t)$, where t is transcendental over the arbitrary field k of $\mathrm{char}(k) \neq 2$. The set $\tilde{k} = \{x \in L \ : \ x \text{ is algebraic over } k\}$ is a subfield of L and we call it the *constant field* of $L|k$. For our purposes for a function field $L|k$ we will always assume that k is the full constant field of L, i.e. $\tilde{k} = k$.
We are mainly concerned with quadratic extensions.

Let $D \in k[t]$ be a polynomial over k which is squarefree over the algebraic closure $\bar{k}$ and $\deg(D) \geq 1$. For simplicity we assume that $\mathrm{lc}(D) = 1$ (otherwise we extend k to $\tilde{k} = k(\sqrt{\mathrm{lc}(D)})$). We call

$$L = k(t, \sqrt{D}) = k(t)(\sqrt{D}) = k(t)[X]/(X^2 - D)$$

a quadratic function field . We also use the notation $L = k(t, u)$, where $u^2 = D(t)$. An element $\alpha \in L$ can be written as

$$\alpha = A + B\sqrt{D}, \text{ with } A, B \in k(t) \text{ or } \alpha = \tfrac{A+B\sqrt{D}}{C} \text{ with } A, B, C \in k[t]$$

As $L|k(t)$ is a Galois extension with the nontrivial automorphism

$$A + B\sqrt{D} \mapsto A - B\sqrt{D},$$

we define the *conjugate* of $\alpha = A + B\sqrt{D}$ as $\alpha' = A - B\sqrt{D}$. Trace and norm are given by

$$\mathrm{Tr}(\alpha) = \alpha + \alpha', \ \mathrm{N}(\alpha) = \alpha\alpha'$$

Quadratic function fields have interesting arithmetic properties extending the rational case only when $\deg(D) \geq 3$ as the next theorem shows.

Theorem 0.1. *Let $L = k(t, u)$, $u^2 = D(t)$, $\mathrm{lc}(D) = 1$, D squarefree.*

i) *If $\deg(D) = 1$, i.e. $D(t) = t + a$ for some $a \in k$ then $L = k(u)$.*
ii) *If $\deg(D) = 2$, i.e. $D(t) = t^2 + at + b$ then $L = k(x)$ for some $x \in L$*

Proof. i) Obviously $k(u) \subseteq L = k(t, u)$. On the other hand we also have $u^2 - a = D(t) - a = t \Rightarrow t \in k(u) \Rightarrow L \subseteq k(u)$. Together we have $L = k(u)$.
ii) Let $t_1 = t + \frac{a}{2}$ then $u^2 = D(t) = (t + \frac{a}{2})^2 + b - \frac{a^2}{4} = {t_1}^2 + d$ where $d = b - \frac{a^2}{4}$. So without loss of generality we can assume that $D(t) = t^2 + d$ with $d = (u - t)(u + t)$. If we now set $x = u - t$ and $y = u + t$ then $u = \frac{1}{2}(x + y)$ and $t = \frac{1}{2}(y - x)$. We claim that $L = k(x)$.

On the one hand $x = u - t \in k(t,u) = L$ and on the other hand $y = \frac{d}{x}$. So $u = \frac{1}{2}(x+y) = \frac{1}{2}(x + \frac{d}{x}) \in k(x)$ as well as $t = \frac{1}{2}(y-x) = \frac{1}{2}(\frac{d}{x} - x) \in k(x)$. Together we conclude $k(u,t) \subseteq k(x)$ and therefore $L = k(x)$. □

If $\deg(D) = 2g+2$ is even, as we will see below, we obtain two different places at infinity and call $L = k(t, \sqrt{D})$ *real quadratic function field* and if $\deg(D) = 2g+1$ is odd, there exists only one place at infinity and we call it *imaginary quadratic function field* . The names are due to the similarities to real respective imaginary quadratic number fields. The important number g is called genus . In section 3 we will see that quadratic function fields are closely related to hyperelliptic curves. Therefore we also speak of hyperelliptic function fields sometimes.

1. Arithmetic of ideals

We will mainly follow the approach Artin chooses in his dissertation [**Art21**]. Consider the subring $\mathfrak{O}_L$ of all integral elements of L over $k[t]$. Elements $\alpha \in \mathfrak{O}_L$ can simply be written as

$$\alpha = A + B\sqrt{D}, \text{ where } A, B \text{ are polynomials in } k[t].$$

Although $\mathfrak{O}_L$ itself is in general not an UFD (unique factorisation domain) it is at least a Dedekind ring . This means it is a commutative ring which satisfies the following conditions:

a) It is a Noetherian ring (i.e. every ascending chain of ideals terminates after a finite number of steps) and an integral domain.
b) It is the set of algebraic integers in its field of fractions.
c) Every prime ideal is also a maximal ideal.

We now state some well known basic facts about Dedekind rings which we will need for further investigation which can be found for example in [**Lan94**], [**BS66**] or [**FT91**].

Let $\mathfrak{O}$ be a Dedekind ring and L its quotient field. A fractional ideal is an $\mathfrak{O}$-submodule $\mathfrak{a} \neq \{0\}$ of L, such that there exists a $\gamma \in L^*$, for which $\gamma \cdot \mathfrak{a}$ is an ideal in $\mathfrak{O}$. Since $\mathfrak{O}$ is Noetherian it follows that $\mathfrak{a}$ is finitely generated.
The main theorem of Dedekind's ideal theory gives us a slightly weaker version of the prime factorisation. It says that in a Dedekind ring every fractional ideal $\mathfrak{a}$ can be uniquely factored into prime ideals, i.e.

$$\mathfrak{a} = \frac{\mathfrak{p}_1^{i_1} \cdots \mathfrak{p}_r^{i_r}}{\mathfrak{q}_1^{j_1} \cdots \mathfrak{q}_s^{j_s}} \text{ where } i_k, j_l \in \mathbb{N}$$

and the non-zero fractional ideals form a group G_L under multiplication.
Obviously every ideal $\mathfrak{a}$ itself as well as all multiples $\gamma\mathfrak{a}$ where $\gamma \in L^*$ are fractional ideals. Moreover $(\gamma) = \gamma\mathfrak{O}$ is also a fractional ideal for arbitrary $\gamma \in L^*$. We call these ideals *principal (fractional) ideals* . They form a normal subgroup of G_L, that will be denoted by P_L.
We call the power $e_\mathfrak{p}$ a prime ideal $\mathfrak{p}$ appears in the factorisation of $\mathfrak{a}$ the *order* of $\mathfrak{a}$ at $\mathfrak{p}$, written $\operatorname{ord}_\mathfrak{p} \mathfrak{a}$.
As a generalisation of the divisibility of integers we can define divisibility of ideals. We say that an ideal $\mathfrak{a}$ divides $\mathfrak{b}$ if there exists another ideal $\mathfrak{c}$ with $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$, i.e. $\operatorname{ord}_\mathfrak{p} a \leq \operatorname{ord}_\mathfrak{p} \mathfrak{b}$ for all prime ideals $\mathfrak{p}$. By the definition of the module product it is clear that this is the case if and only if $\mathfrak{a} \supseteq b$. Divisibility of elements in $\mathfrak{O}$ can be considered as a special case of ideal divisibility by regarding $\alpha \in \mathfrak{O}$ as the principal ideal $(\alpha) = \alpha\mathfrak{O}$.

In a canonical way we can also define the *greatest common divisor* and the *least common multiple* for ideals. Let $\mathfrak{a}, \mathfrak{b}$ be ideals in $\mathfrak{O}$, then we call $\mathfrak{c} = \gcd(\mathfrak{a}, \mathfrak{b})$ the greatest common divisor of $\mathfrak{a}$ and $\mathfrak{b}$ if

i) $\mathfrak{c}|\mathfrak{a}$ and $\mathfrak{c}|\mathfrak{b}$ and
ii) if $\mathfrak{d}|\mathfrak{a}$ and $\mathfrak{d}|\mathfrak{b}$ then $\mathfrak{d}|\mathfrak{c}$.

An element $\mathfrak{m}$ is called the least common multiple $\mathfrak{m} = \operatorname{lcm}(\mathfrak{a}, \mathfrak{b})$ if

i) $\mathfrak{a}|\mathfrak{m}$ and $\mathfrak{b}|\mathfrak{m}$ and
ii) if $\mathfrak{a}|\mathfrak{d}$ and $\mathfrak{b}|\mathfrak{d}$ then $\mathfrak{m}|\mathfrak{d}$.

Remark. *Because of the unique factorisation of fractional ideals we obtain the formulas*

$$\gcd(\mathfrak{a}, \mathfrak{b}) = \langle \mathfrak{a} \cup \mathfrak{b} \rangle = \mathfrak{a} + \mathfrak{b}, \quad \operatorname{lcm}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} \cap \mathfrak{b}$$

where $\langle \mathfrak{a} \cup \mathfrak{b} \rangle$ *denotes the ideal generated by the set* $\mathfrak{a} \cup \mathfrak{b}$.

We now apply the above to the special ring $\mathfrak{O}_L$. Since $k[t]$ is a Dedekind ring, its integral closure $\mathfrak{O}_L$ in L, is also a Dedekind ring ([**Lan94**]). Here we can even show:

Lemma 1.1. *Every ideal* $\{0\} \neq \mathfrak{a} \subset \mathfrak{O}_L$ *is a finitely generated free* $k[t]$*-module of rank* 2.

Proof. As $\mathfrak{O}_L = [1, \sqrt{D}]$ is a free $k[t]$-module of rank 2 and $k[t]$ is a principal ideal domain, we know from a standard theorem (see for example [**Lan64**]) that every submodule is again free and consequently of rank ≤ 2. Since for an element $\alpha \in \mathfrak{a}$, α and $\alpha\sqrt{D}$ are linearly independent over $k[t]$, the rank is equal to 2. □

We call a $k[t]$-module $\mathfrak{m} \subseteq \mathfrak{O}_L$ *full*, if $\mathfrak{m}$ has rank 2. Thus we can represent every ideal $\mathfrak{a}$ as $[\alpha, \beta]$ with $\alpha, \beta \in \mathfrak{O}_L$ or in other words as $\gcd(\alpha\mathfrak{O}_L, \beta\mathfrak{O}_L)$.
To facilitate computations with modules we define a special kind of basis.

Theorem 1.1. *Every full* $k[t]$*-module* $\mathfrak{m} \subset \mathfrak{O}_L$ *has a uniquely determined basis of the shape*

$$\mathfrak{m} = [R, S + T\sqrt{D}], \ \operatorname{lc}(R) = \operatorname{lc}(T) = 1, \ \deg(S) < \deg(R)$$

which can be computed by the subsequent algorithm. Moreover $\mathfrak{m} \cap k[t] = Rk[t]$.

Algorithm 1.1.

Input: *Module* $\mathfrak{m} = [A_0 + A_1\sqrt{D}, B_0 + B_1\sqrt{D}]$.
Output: *Canonical basis* $[R, S + T\sqrt{D}]$ *of* $\mathfrak{m}$, *if* $\mathfrak{m}$ *full module, else "*$\mathfrak{m}$ *not a full module".*

begin
If $A_1 = 0$ *and* $B_1 = 0$ *then Output "*$\mathfrak{m}$ *not a full module"*
if $\deg(A_1) > \deg(B_1)$ *interchange* $A_0 + A_1\sqrt{D}$ *and* $B_0 + B_1\sqrt{D}$
while $\deg(A_1) \geq 0$ *do*
  $R := B_1 \bmod A_1$; $Q := B_1 \operatorname{div} A_1$;
  $C_0 := A_0$; $C_1 := B_1$;
  $A_0 := B_0 - QA_0$; $A_1 := R$; $B_0 := C_0$; $B_1 := C_1$;
od;
$R := \operatorname{lc}(A_0)^{-1}A_0$; $S := \operatorname{lc}(B_1)^{-1}B_0$; $T := \operatorname{lc}(B_1)^{-1}B_1$
end.

Observe that in the while loop we have $R := B_1 \bmod A_1$ and $A_1 := R$, so the degree of A_1 decreases in each step and the algorithm terminates. Moreover it does not

change the module that is generated by A_0, A_1, B_0 and B_1 , since for $B_1 = QA_1+R$, $\deg(R) < \deg(A_1)$ we have

$$\begin{aligned}
\mathfrak{m} &= [A_0 + A_1\sqrt{D}, B_0 + B_1\sqrt{D}] \\
&= [A_0 + A_1\sqrt{D}, B_0 + B_1\sqrt{D} - Q(A_0 + A_1\sqrt{D})] \\
&= [A_0 + A_1\sqrt{D}, B_0 - QA_0 + R\sqrt{D}] \\
&= [B_0 - QA_0 + R\sqrt{D}, A_0 + A_1\sqrt{D}] \\
&= [A_0^{(1)} + A_1^{(1)}\sqrt{D}, B_0^{(1)} + B_1^{(1)}\sqrt{D}],
\end{aligned}$$

where $A_i^{(1)}$, $B_i^{(1)}$ are the values of A_i respectively B_i at the end of the loop. The uniqueness of the canonical basis follows from the normalisation of R, S and T as can be seen by some computation.
The canonical basis is nothing else but the usual *hermite normal form* for general modules over principal ideal domains.
As Lemma 1.1 states, every ideal is a full module, so we can compute its canonical basis with algorithm 1.1. However, not every full module given in canonical form defines an ideal. The next theorem characterises them completely.

Theorem 1.2. *Let $\mathfrak{m} = [R, S + T\sqrt{D}]$, $R, S, T \in k[t]$ be a full module given in canonical basis. Then $\mathfrak{m}$ is an ideal if and only if there exist $A, B, C \in k[t]$, such that*

$$R = AT,\ S = BT,\ D = B^2 - AC$$

Proof. "⇒" Let $\mathfrak{m} = [R, S + T\sqrt{D}]$ be an ideal. Then $R \in \mathfrak{m}$ and $R\sqrt{D} \in \mathfrak{m}$. So we can write $R\sqrt{D} = -BR + (S + T\sqrt{D})A$, $A \neq 0$, for suitable polynomials A, B. It follows that $AS - BR = 0$ and $R = AT$. Inserting the second equation into the first implies $AS = BR = BAT$. Hence $S = BT$ and we have proved the first two assertions.
Next we have $T(B + \sqrt{D}) = BT + T\sqrt{D} = S + T\sqrt{D} \in \mathfrak{m}$. Therefore $T(B^2 - D) = T(B + \sqrt{D})(B - \sqrt{D}) \in \mathfrak{m}$. Since $T(B^2 - D) \in k[t] \cap \mathfrak{m}$ it follows that we have $RC = T(B^2 - D)$ for some $C \in k[t]$ (see last assertion of theorem 1.1). Thus $AC = B^2 - D$, proving the last assertion.
"⇐" Let the three conditions of theorem 1.2 be true. We have to show that $\mathfrak{m}\mathfrak{O}_L \subseteq \mathfrak{m}$. Obviously, it suffices to verify that $R\alpha \in \mathfrak{m}$ and $(S+T\sqrt{D})\alpha \in \mathfrak{m}$ for any $\alpha \in \mathfrak{O}_L$ since in this case $(RX + (S + T\sqrt{D})Y)\alpha = R\alpha \cdot X + (S + T\sqrt{D})\alpha \cdot Y \in \mathfrak{m}$ for all $X, Y \in k[t]$, $\alpha \in \mathfrak{O}_L$.
Let $\alpha = A_1 + A_2\sqrt{D}$. Then

$$\begin{aligned}
R\alpha &= RA_1 + RA_2\sqrt{D} = RA_1 + AA_2T\sqrt{D} \\
&= RA_1 - SAA_2 + AA_2(S + T\sqrt{D}) \\
&= RA_1 - BRA_2 + AA_2(S + T\sqrt{D}) \in \mathfrak{m}.
\end{aligned}$$

Similarly

$$\begin{aligned}
(S + T\sqrt{D})\alpha &= T(B + \sqrt{D})(A_1 + A_2\sqrt{D}) \\
&= T\left[A_1B + A_2D + (A_1 + BA_2)\sqrt{D}\right] \\
&= T\left[A_1B + A_2D + (A_1 + BA_2)(B + \sqrt{D}) - (A_1 + BA_2)B\right] \\
&= T\left[A_2D - B^2A_2 + (A_1 + BA_2)(B + \sqrt{D})\right] \\
&= T\left[-ACA_2 + (A_1 + BA_2)(B + \sqrt{D})\right] \\
&= -A_2CR + (A_1 + BA_2)(S + T\sqrt{D}).
\end{aligned}$$

Thus $(S + T\sqrt{D})\alpha \in \mathfrak{m}$, as was to be shown. □

As a consequence every ideal $\mathfrak{a}$ can be written as

$$\begin{aligned} \mathfrak{a} &= T \cdot [A, B + \sqrt{D}], \text{ where } T, A, B \in k[t],\ \mathrm{lc}(A) = \mathrm{lc}(T) = 1 \\ & \quad B^2 \equiv D \bmod A,\ \deg(B) < \deg(A). \end{aligned}$$

In case $T = 1$, we call the corresponding ideal *primitive* .
If $\mathfrak{a}$ is an ideal in $\mathfrak{O}_L$ we define $\mathfrak{a}'$ to be the set of conjugated elements of $\mathfrak{a}$, i.e. $\mathfrak{a}' = \{\alpha' : \alpha \in \mathfrak{a}\}$. The norm of an ideal will be denoted by $\mathrm{N}(\mathfrak{a}) = \mathfrak{a}\mathfrak{a}'$. In this section we will think of the norm as an $\mathfrak{O}_L$-module.

Theorem 1.3. *Let $\mathfrak{a} = [R, S + T\sqrt{D}]$ be an ideal, then $\mathrm{N}(\mathfrak{a}) = RT\mathfrak{O}_L$. In particular, $\mathrm{N}(\mathfrak{a})$ is a principal ideal.*

Proof. The proof is just an easy computation, using the special conditions of theorem 1.2 an ideal fulfils. □

How to multiply ideals with canonical bases will be answered by the next theorem, which follows from elementary computations.

Theorem 1.4. *Let $\mathfrak{a} = [A_0, B_0 + \sqrt{D}]$ and $\mathfrak{b} = [A_1, B_1 + \sqrt{D}]$ be two primitive ideals given in their canonical basis. Compute $T, R, S \in k[t]$ as follows:*

a) *Let $T = \gcd(A_0, A_1, B_0 + B_1)$ and determine $X, Y, Z \in k[t]$ such that $A_0X + A_1Y + (B_0 + B_1)Z = T$.*
b) *Let $R = A_0A_1T^{-1}$.*
c) *Define $S \equiv A_0B_1X + A_1B_0Y + (B_0B_1 + D)Z \bmod R$, $\deg(S) < \deg(R)$*

Then the product $\mathfrak{a} \cdot \mathfrak{b}$ has the canonical basis representation $\mathfrak{a} \cdot \mathfrak{b} = [R, S + T\sqrt{D}]$.

Algorithm 1.2.

Input: *ideals $\mathfrak{a} = [A_0, B_0 + \sqrt{D}]$, $\mathfrak{b} = [A_1, B_1 + \sqrt{D}]$*
Output: *product $\mathfrak{c} = \mathfrak{a} \cdot \mathfrak{b} = [R, S + T\sqrt{D}]$ in canonical basis.*

begin
$T := A_0X + A_1Y + (B_0 + B_1)Z = gcd(A_0, A_1, B_0 + B_1)$;
$R := A_0A_1T^{-1}$;
$S := A_0B_1X + A_1B_0Y + (B_0B_1 + D)Z \bmod R$
end.

We will now study the prime ideals in more detail.

Theorem 1.5. *Let $\mathfrak{p} \neq \{0\}$ be a prime ideal then there exists a unique prime polynomial $P \in k[t]$, such that $\mathfrak{p} | P\mathfrak{O}_L$. Moreover we have $\mathfrak{p} \cap k[t] = Pk[t]$.*

Proof. As already mentioned

$$\mathfrak{p}\mathfrak{p}' = \mathrm{N}(\mathfrak{p}) = A\mathfrak{O}_L = \prod_{i=1}^{s} (P_i\mathfrak{O}_L)^{e_i}.$$

So $\mathfrak{p}$ divides at least one factor $P_i\mathfrak{O}_L$. This factor is unique since if $\mathfrak{p}$ divided $P\mathfrak{O}_L$ and $Q\mathfrak{O}_L$, it would divide their sum which is equal to $\mathfrak{O}_L$ as P and Q are prime, which is a contradiction.
In addition $\mathfrak{p} \cap k[t]$ is an ideal, so $\mathfrak{p} \cap k[t] = P_0k[t]$ for some polynomial P_0 of positive degree. Since $P_0 \in \mathfrak{p}$, it follows that $P_0\mathfrak{O}_L \subseteq \mathfrak{p}$, i.e. $\mathfrak{p} \mid P_0\mathfrak{O}_L$. From the above it then follows $P_0 = P$. □

This means that in order to find prime ideals we only need to look at the ideal factorisation of $P\mathfrak{O}_L$, where P is a prime polynomial. But first we will have a look at a special injection a prime ideal induces. Observe that since every prime ideal

$\mathfrak{p}$ in a dedekind domain is maximal, the residue class ring $\mathfrak{O}_L \bmod \mathfrak{p}$ is a field. A straightforward computation leads us to a representation of this quotient field.

Lemma 1.2. *Let $\mathfrak{p} = [R, S + T\sqrt{D}]$ be a prime ideal given in canonical basis, then a complete system of distinct residue classes modulo $\mathfrak{p}$ is given by the set*

$$\mathfrak{R} = \left\{ A + B\sqrt{D} \,:\, A, B \in k[t], \deg(A) < \deg(R), \deg(B) < \deg(T) \right\}.$$

Definition. *Let $\mathfrak{p} \neq \{0\}$ be a prime ideal with $\mathfrak{p} | P\mathfrak{O}_L$, then we define the embedding*

$$\iota : k[t]/Pk[t] \to \mathfrak{O}_L/\mathfrak{p} \text{ by } A + Pk[t] \mapsto A + \mathfrak{p}$$

With this obviously well defined and injective embedding we can view $\mathfrak{O}_L/\mathfrak{p}$ as a field extension of $k[t]/Pk[t]$. We call the degree of this extension *relative degree* of $\mathfrak{p}$. In addition we can also view $\mathfrak{O}_L/\mathfrak{p}$ as a finite field extension of k itself. Its degree will be called *absolute degree* of $\mathfrak{p}$. We will write

$$\deg^r(\mathfrak{p}) = [\mathfrak{O}_L/\mathfrak{p} : \iota(k[t]/Pk[t])] \text{ and } \deg(\mathfrak{p}) = [\mathfrak{O}_L/\mathfrak{p} : \iota(k)]$$

The next theorem characterises all possible types of prime ideals in $\mathfrak{O}_L$.

Theorem 1.6. *Let $\mathfrak{p} \neq \{0\}$ be a prime ideal with $\mathfrak{p} | P\mathfrak{O}_L$ and $P \in k[t]$ a prime polynomial.*

1) *$P \nmid D$ and $X^2 \equiv D \bmod P$ is unsolvable then $\mathfrak{p} = P\mathfrak{O}_L$ has relative degree 2.*
2) *$P \nmid D$ and U solves $X^2 \equiv D \bmod P$, then $P\mathfrak{O}_L = \mathfrak{p}\mathfrak{p}'$ where $\mathfrak{p} = [P, U + \sqrt{D}]$, $\mathfrak{p}' = [P, -U + \sqrt{D}]$ and $\mathfrak{p}, \mathfrak{p}'$ have relative degree 1.*
3) *$P \mid D$, then $P\mathfrak{O}_L = \mathfrak{p}^2$ and $\mathfrak{p} = [P, \sqrt{D}]$ has relative degree 1.*

PROOF. Assume $\mathfrak{p}$ is a prime ideal with $\mathfrak{p} \mid P\mathfrak{O}_L$, i.e. $\mathfrak{p}\mathfrak{a} = P\mathfrak{O}_L$ for some ideal $\mathfrak{a}$. Taking norms yields $\mathrm{N}(\mathfrak{p})\mathrm{N}(\mathfrak{a}) = \mathrm{N}(P\mathfrak{O}_L) = P^2\mathfrak{O}_L$. So $\mathrm{N}(\mathfrak{p}) = P\mathfrak{O}_L$ or $\mathrm{N}(\mathfrak{p}) = P^2\mathfrak{O}_L$.

1) Let $\mathfrak{p} = T[A, B + \sqrt{D}]$, $\mathrm{lc}(A) = \mathrm{lc}(T) = 1$, $\deg(B) < \deg(A)$, $B^2 \equiv D \bmod A$. Since $\mathrm{N}(\mathfrak{p}) = AT^2$, we conclude $AT^2 = P$ or $AT^2 = P^2$. If P divides A, we have $B^2 \equiv D \bmod P$. So $P \nmid A$ and $P \mid T^2$. Thus $P = T$, $A = 1$ and consequently $B = 0$ (observe that $\deg(B) < \deg(A)$). Together we obtain
$$\mathfrak{p} = T[A, B + \sqrt{D}] = P[1, \sqrt{D}] = P\mathfrak{O}_L$$
By the representation of the corresponding residue class field of Lemma 1.2, we obtain $\deg^r(\mathfrak{p}) = 2$.
2) Let $P \nmid D$ and $X^2 \equiv D \bmod P$, where $X \in k[t]$ with $\deg(X) < \deg(P)$. If we define $\mathfrak{p} = [P, X + \sqrt{D}]$, then $\mathfrak{p}$ is an ideal and
$$\begin{aligned} \mathrm{N}(\mathfrak{p}) &= [P, X + \sqrt{D}] \cdot [P, X - \sqrt{D}] \\ &= [P^2, PX - P\sqrt{D}, PX + P\sqrt{D}, X^2 - D] \\ &= P[P, X - \sqrt{D}, X + \sqrt{D}, (X^2 - D)/P] = P\mathfrak{a} \end{aligned}$$
for some module $\mathfrak{a}$. Then $\mathfrak{a}$ contains P and $2X$. Since $P \nmid X$ we have $1 \in \mathfrak{a}$ and therefore $\mathfrak{a} = \mathfrak{O}_L$. Together we have
$$\mathrm{N}(\mathfrak{p}) = \mathfrak{p}\mathfrak{p}' = P\mathfrak{O}_L.$$
Since $X \neq 0$, $\mathfrak{p} \neq \mathfrak{p}'$.
By Lemma 1.2 we get $\deg^r(\mathfrak{p}) = 1$.
3) Finally let $P \mid D$. Define $\mathfrak{p} = [P, \sqrt{D}]$, then $\mathfrak{p} = \mathfrak{p}'$ and
$$\mathrm{N}(\mathfrak{p}) = \mathfrak{p}^2 = [P^2, 2P\sqrt{D}, D] = P[P, 2\sqrt{D}, Q].$$
P and Q are coprime because D is squarefree, so $\mathfrak{p}^2 = P\mathfrak{O}_L$. Moreover $\deg^r(\mathfrak{p}) = 1$.

□

A prime ideal of type 1) is called *inert*, of type 2) *split* and of type 3) *ramified*. We now describe an algorithm to compute the prime factorisation of an ideal.

Algorithm 1.3.

Input: *ideal* $\mathfrak{a} = T[A, B + \sqrt{D}]$.
Output: *prime factorisation* $\mathfrak{a} = \prod_{i=0}^{n} \mathfrak{p}_i^{e_i}$.

begin
Factor $T = P_i^{e_i}$ *over* $k[t]$;
compute $\left(\frac{D}{P_i}\right)$;
factor $P_i\mathfrak{O}_L$ *corresponding to the three cases*
$P_i\mathfrak{O}_L = \mathfrak{p}$, $P_i\mathfrak{O}_L = \mathfrak{p}\mathfrak{p}'$ *or* $P_i\mathfrak{O}_L = \mathfrak{p}^2$;
factor $A = Q_i^{e_i}$ *(only* Q_i *of cases* 2) *and* 3) *possible);*
compute $X_i = B \bmod Q_i$;
if $X_i = 0$ *then*
  $e_i = 1$ *(prime ideal factor of type* 3)*);*
else
  prime ideal factor of type 2) *to the power* e_i *(confer theorem 1.7);*
end.

Remark. *To compute the quadratic residue symbol we can either use an analogue of Euler's criterion for polynomials over* $GF(q)$ *namely*

$$\left(\frac{D}{P}\right) = D^{\frac{|P|-1}{2}}$$

where $|P| = q^{\deg(P)}$, *or we can make use of the quadratic reciprocity theorem for polynomials (see* [**Ros02**]*).*

The canonical basis representation of the general multiple of an ideal is given by

Theorem 1.7. *Let* $\mathfrak{a} = [A, B + \sqrt{D}] \in \mathrm{Div}(L)$ *be an ideal given in canonical basis with* $\gcd(A, D) = 1$ *and* $m \in \mathbb{N}$. *Then* $\mathfrak{a}^m = [A^m, B_m + \sqrt{D}]$, *where* B_m *is uniquely determined by the conditions*

$$B_m^2 \equiv D \bmod A^m, \quad \deg(B_m) < \deg(A^m), B_m \equiv B \bmod A$$

Proof. We prove the assertion by induction on m. It is clearly true for $m = 1$. Assume it holds for m then

$$\mathfrak{a}^{m+1} = [A^m, B_m + \sqrt{D}] \cdot [A, B + \sqrt{D}],$$

where B_m satisfies the conditions of the theorem. By theorem 1.4 we obtain $\mathfrak{a}^{m+1} = [R, S + T\sqrt{D}]$, where

$$T = \gcd(A^m, A, B_m + B) = \gcd(A, B_m + B) = \gcd(A, 2B),$$

since $B_m \equiv B \bmod A$ by induction hypothesis. Moreover, $(A, D) = 1$ implies $(A, B) = 1$ because $B^2 \equiv D \bmod A$. So we have $T = 1$. Consequently we obtain $R = A^{m+1}$. Since the basis is canonical, we must have $S^2 \equiv D \bmod A$ and $\deg(S) < \deg(A^{m+1})$. It remains to show that $S \equiv B \bmod A$.
Let $Y, Z \in k[t]$ such that $AY + (B_m + B)Z = 1$, then $S \equiv AB_mY + (B_mB + D)Z \bmod A^{m+1}$. Since $B_m \equiv B \bmod A$ we obtain $S \equiv (B^2 + D)Z \equiv 2B^2Z \bmod A$. But $1 = AY + (B_m + B)Z \equiv 2BZ \bmod A$ and we conclude that $S \equiv B \bmod A$. □

Observe that in case $\gcd(A, D) \neq 1$, $\mathfrak{a}$ can be divided by a ramified prime ideal $\mathfrak{p}$, which is easily powered by regarding $\mathfrak{p}^2 = P\mathfrak{O}_L$.
Having now provided the most important algorithms, we come back to the group of fractional ideals G_L. Observe that G_L itself is not finite even if k is a finite field.

But if we cancel all principal ideals P_L of G_L we obtain the so-called *ideal class group* $C_L = G_L/P_L$ which is finite if k is.
We can summarise the construction of C_L by the following exact sequence:

$$1 \longrightarrow \mathfrak{O}_L^* \longrightarrow L^* \longrightarrow G_L \longrightarrow C_L \longrightarrow 1.$$

Here the map from L^* to G_L is given by $\gamma \mapsto (\gamma)$, the corresponding principal ideal. Observe that a fractional ideal $\mathfrak{a}$ is always equivalent to some integral ideal since there exists a $\gamma \in L^*$, such that $\gamma \cdot \mathfrak{a} = \mathfrak{b} \subseteq \mathfrak{O}_L$.
For computational purposes in the ideal class group we define a special type of ideal, namely the reduced one.

Definition. *An ideal of the form* $\mathfrak{a} = [A, B + \sqrt{D}]$, *where* $\mathrm{lc}(A) = 1$, $\deg(B) < \deg(A) \leq g$ *and* $B^2 \equiv D \bmod A$ *holds, is called a reduced ideal.*

The next algorithm can be used to find a reduced representative in the same class as the given ideal.

Algorithm 1.4.

Input: *Primitive ideal* $\mathfrak{a} \subseteq \mathfrak{O}_L$ *given in canonical basis* $\mathfrak{a} = [A, B + \sqrt{D}]$, $\mathrm{lc}(A) = 1$, $\deg(B) < \deg(A)$, $B^2 \equiv D \bmod A$
Output: *Reduced ideal* $\mathfrak{b} = [U, V + \sqrt{D}]$ *in the same class as* $\mathfrak{a}$ *and* $\mathrm{lc}(U) = 1$, $\deg(V) < \deg(U)$, $V^2 \equiv D \bmod U$, $\deg(U) \leq g$.

begin
$U := A; V := B \bmod U;$
while $2\deg(U) > \deg(D)$ *do*
$U := (V^2 - D)/U;$
$U := \mathrm{lc}(U)^{-1} \cdot U;$
$V := -V \bmod U$
od;
end.

It is easy to see that the algorithm terminates (the degree of U decreases in each step) and yields a reduced basis. Moreover the given basis lies in the same class as the reduced, since

$$\begin{array}{rcccl} [U, V + \sqrt{D}] & \sim & [1, (V + \sqrt{D})/U] & \sim & [V - \sqrt{D}, U^{(1)}] \\ & \sim & [U^{(1)}, -V + \sqrt{D}] & \sim & [U^{(1)}, V^{(1)} + \sqrt{D}], \end{array}$$

where $U^{(1)}$ and $V^{(1)}$ are the values for U and V at the end of the loop.
The second equivalence holds because a multiplication by the principal ideal $(V - \sqrt{D})\mathfrak{O}_L$ does not change the class.
Number of steps n of this algorithm:
If $2\deg(A) > \deg(D)$, then n is minimal with respect to $2n \geq 2\deg(A) - \deg(D)$, i.e. $n = \deg(A) - (g+1)$ if $\deg(D) = 2g+2$ and $n = \deg(A) - g$ if $\deg(D) = 2g+1$.
Unfortunately reduced ideals are not always unique representatives of ideal classes. This is only the case when L is an imaginary quadratic function field. The reason for this is that in real quadratic function fields the subring of units of $\mathfrak{O}_L$ is not equal to k^*. In order to compute with ideal classes in this case, one has to define a distance function and compute the regulator. For further details on real quadratic function fields see [**Ste99**], [**PR99**] or [**Sch96**].
However, we will restrict ourselves mainly to the case of imaginary quadratic function fields, i.e. $\deg(D)$ is assumed to be $2g + 1$. As the next lemma shows this is only a constraint if D has no zero in k.

Lemma 1.3. *Let $L = k(t, \sqrt{D_1(t)})$ be a real quadratic function field where we have $\deg(D_1) = 2g+2 > 3$, and let $\alpha \in k$ be a zero of $D_1(t) = d_0 + \cdots + d_{2g+1}t^{2g+1} + t^{2g+2}$. Then $L = k(x, \sqrt{D_2(x)})$ where $x = (t-\alpha)^{-1}$ and $D_2(x) = D_1(x^{-1}+\alpha)x^{2g+2} \in k[x]$ with $\deg(D_2) = 2g+1$.*

PROOF. Note first that $k(x) = k(t)$ and $\sqrt{D_2(x)} = (t-\alpha)^{-1}\sqrt{D_1(t)}$. What remains to be shown is that $\deg(D_2(x)) = 2g+1$. We obtain $D_2(x) = D_1\left(\frac{1+\alpha x}{x}\right) =$

$$\begin{aligned} &= x^{2g+2}(d_0 + d_1\left(\tfrac{1+\alpha x}{x}\right) + \cdots + d_{2g+1}\left(\tfrac{1+\alpha x}{x}\right)^{2g+1} + \left(\tfrac{1+\alpha x}{x}\right)^{2g+2}) \\ &= d_0x^{2g+2} + d_1(1+\alpha x)x^{2g+1} + \cdots + d_{2g+1}(1+\alpha x)^{2g+1}x + (1+\alpha x)^{2g+2} \end{aligned}$$

The leading coefficient of the above polynomial is nothing else but $D_1(\alpha) = 0$, so $\deg(D_2) < 2g+2$. The coefficient of x^{2g+1} is equal to

$$d_1 + d_2(2\alpha) + \cdots + d_{2g+1}(2g+1)\alpha^{2g} + (2g+1)\alpha^{2g+1} = D_1'(\alpha)$$

Since D_1 is assumed to be squarefree, $D_1(\alpha) \neq 0$, so $\deg(D_2) = 2g+1$. □

Remark. *Since inert prime ideals are principal ideals they will not occur in the prime ideal factorisation of a reduced ideal (otherwise it would not be unique). Moreover a split prime ideal $\mathfrak{p}$ and its conjugate $\mathfrak{p}'$ cannot contain a reduced ideal simultaneously, because their product is again a principal ideal as we have already seen in theorem 1.6.*

We are now able to perform the group operation in the ideal class group. To compute the product of two reduced ideals $\mathfrak{a}, \mathfrak{b} \in C_L$, we compute their product by algorithm 1.2 and then reduce the result applying algorithm 1.4. A detailed analysis of the complexity can be found in [**Ste01**]. His main result is the following

Theorem 1.8. *Let $L = k(t, \sqrt{D(t)})$, k finite field with $\mathrm{char}(k) \neq 2$, be a hyperelliptic function field of genus g then composition of two classes in the ideal class group of L (real or imaginary quadratic model) can be performed in*

$$\tfrac{47}{2}g^2 + O(g)$$

field operations.

2. Valuation rings

In this section we give a short introduction to valuations in function fields and relate it to the preceding theory of ideals. First we collect some basics which can be found for example in [**Lan94**], [**Koc97**], [**Sti93**] or [**Iwa93**].

As in section 1, k will be assumed to be an arbitrary field, $\mathrm{char}(k) \neq 2$ *!*

A function $v : L \to \mathbb{Z} \cup \{\infty\}$, where $L|k$ is a function field, is called a *discrete valuation* if it has the following properties:

a) $v(x) = \infty \Leftrightarrow x = 0$
b) $v(xy) = v(x) + v(y)$ for all $x, y \in L$
c) $v(x+y) \geq \min\{v(x), v(y)\}$ for all $x, y \in L$
d) $\exists\, \pi \in L$ such that $v(\pi) = 1$. Such an element is called uniformising variable.
e) $v(a) = 0 \quad \forall\, a \in k \setminus \{0\}$

The set of all valuations of $L|k$ will be denoted by $\mathrm{Val}(L|k)$. The symbol ∞ represents some element not in $\mathbb{Z}$ with the usual properties $\infty+\infty = \infty+n = n+\infty = \infty$ and $\infty > n$ for all $n \in \mathbb{Z}$. Property *c)* is often called *Triangle Inequality*. It can be made strict, for if $v(x) \neq v(y)$, then $v(x+y) = \min\{v(x), v(y)\}$. Let v be a discrete valuation of a function field $L|k$.

$$\mathfrak{O}_v = \{x \in L \,:\, v(x) \geq 0\}$$

is called *valuation ring* of $L|k$.
A *prime divisor (place)* is the maximal ideal of some valuation ring $\mathfrak{O}_v$

$$\mathfrak{p}_v = \{x \in L \mid v(x) > 0\}.$$

The set of all prime divisors of $L|k$ will be denoted by $\mathrm{PDiv}(L|k)$. The claim that $\mathfrak{O}_v$ is a ring follows directly from the properties of a valuation. $\mathfrak{p}_v$ is obviously an ideal. If $xy \in \mathfrak{p}_v$ then $v(xy) = v(x) + v(y) > 0$. By property $c)$ we have $v(x) > 0$ or $v(y) > 0$ and therefore $x \in \mathfrak{p}_v$ or $y \in \mathfrak{p}_v$, so $\mathfrak{p}_v$ is a prime ideal. Moreover $\mathfrak{O}_v \setminus \mathfrak{p}_v = \mathfrak{O}_v^*$ is the set of units and consequently $\mathfrak{p}_v$ is even a maximal ideal.
If π is a *uniformising variable* , i.e. $v(\pi) = 1$ we can also write $\mathfrak{O}_v = \pi\mathfrak{p}_v$. In addition, one can even represent every ideal $\{0\} \neq \mathfrak{a} \subseteq \mathfrak{O}_v$ by $\mathfrak{a} = \pi^n\mathfrak{O}_v$ where $n \in \mathbb{N}_0$. So we obtain the descending chain

$$\mathfrak{O}_v \supset \pi\mathfrak{O}_v \supset \pi^2\mathfrak{O}_v \supset \cdots$$

and $\mathfrak{O}_v$ is a principal ideal domain.
Since $\mathfrak{p}_v$ is a maximal ideal for every valuation v the residue class ring $\mathfrak{O}_v/\mathfrak{p}_v$ is even a field. As $v(x) = 0$ for all $x \in k$ we can embed k into $\mathfrak{O}_v/\mathfrak{p}_v$ in a canonical way. We call $\deg(\mathfrak{p}_v) = [\mathfrak{O}_v/\mathfrak{p}_v : k]$ the *degree* of the place $\mathfrak{p}_v$. For $x \in \mathfrak{O}_v$ we define $\mu_\mathfrak{p} : x \mapsto x \bmod \mathfrak{p}$ to be the *residue class map* and for $x \in L \setminus \mathfrak{O}_v$ we put $\mu(x) := \infty$.

As our next goal is to determine all valuations of a hyperelliptic function field, we will now investigate the behaviour of valuations in algebraic extensions. An algebraic function field $L|k'$ is called an *algebraic extension* of $K|k$ if $L \supseteq K$ is an algebraic field extension and $k' \supseteq k$. We call it *constant field extension* if $L = Kk'$, the compositum of L and k'.
A place $\mathfrak{p}_w$ of $L|k'$ is said to *lie over* $\mathfrak{p}_v$ of $K|k$, if $\mathfrak{p}_v \subseteq \mathfrak{p}_w$. We often also write $\mathfrak{p}_w \mid \mathfrak{p}_v$. It is a standard result of valuation theory that there exists an integer $e \geq 1$ such that $w(x) = e \cdot v(x)$ for all $x \in K$. We call the integer e *ramification index* of the valuation. We say $\mathfrak{p}_w \mid \mathfrak{p}_v$ is *ramified* , if $e(\mathfrak{p}_w|\mathfrak{p}_v) > 1$ and $\mathfrak{p}_w \mid \mathfrak{p}_v$ is *unramified* if $e(\mathfrak{p}_w \mid \mathfrak{p}_v) = 1$. Moreover, if $\mathfrak{p}_w \mid \mathfrak{p}_v$ then $\mathfrak{p}_v = \mathfrak{p}_w \cap L$ and $\mathfrak{O}_v = \mathfrak{O}_w \cap L$. So we have a canonical embedding of the residue class fields given by $x + \mathfrak{p}_v \mapsto x + \mathfrak{p}_w$. The degree of this field extension $f(\mathfrak{p}_w|\mathfrak{p}_v) = [\mathfrak{O}_w/\mathfrak{p}_w : \mathfrak{O}_v/\mathfrak{p}_v]$ is called *relative degree* of $\mathfrak{p}_w$ over $\mathfrak{p}_v$.
We now cite the well known theorem of Ostrowski about valuations of rational function fields $K = k(t)$.

Theorem 2.1. *Let $k(t)$ be a rational function field, then the only possible discrete valuation functions that exist are the P-adic valuations and the ∞-valuation, i.e.: For every prime polynomial there exists a valuation v_P with $v_P(U) = \infty$ iff $U = 0$ and $v_P(U) = n$ when $U = P^n\frac{R}{S}$, $n \in \mathbb{Z}$, $R \cdot S \neq 0$, $P \nmid RS$. In addition there is the valuation v_∞ with $v_\infty(0) = \infty$ and for $U = \frac{R}{S} \in k(t)^*$ we have $v_\infty(U) = -\deg(S) + \deg(R)$. These valuations are pairwise disjoint and there exists no other valuation on $k(t)$.*

Proof. See for example [**vdW93**] □

We now consider extensions of these valuations to the quadratic function field $L|k$.

Theorem 2.2. *The following table characterises all extensions of the valuations from $K = k(t)$ to $L|k$.*

$P \mid D$	$w_{\mathfrak{p}}(\alpha) = v_P(\alpha\alpha')$
$\left(\frac{D}{P}\right) = -1$	$w_{\mathfrak{p}}(\alpha) = \frac{1}{2}v_P(\alpha\alpha')$
$\left(\frac{D}{P}\right) = 1$	$w_{\mathfrak{p}}(A + B\sqrt{D}) = v_P(A + B\delta)$ $w_{\mathfrak{p}'}(A + B\sqrt{D}) = v_P(A - B\delta)$
$\infty, \deg(D) = 2g + 1$	$w_\infty(\alpha) = v_\infty(\alpha\alpha')$
$\infty, \deg(D) = 2g + 2$	$w_\infty(\alpha) = v_\infty(\alpha)$ $w_{\infty'}(\alpha) = v_\infty(\alpha')$

Here δ is defined to be a squareroot of D in the completion field $\hat{K}_v$ of the corresponding valuation, i.e. $\delta = \sum_{j=0}^{\infty} d_j P^j$, $d_0^2 \equiv D \bmod P$ and $v_P(A + B\delta) = v_P(\sum_{j=0}^{\infty} s_j P^j) = \min\{n \in \mathbb{N} \ : \ s_n \neq 0\}$.

Proof. We will only sketch the proof. It is just a specialisation of the general theory of extensions of valuations for which we will refer to [**vdW93**]. We have to look at the completion $\hat{K}$ of $K = k(t)$ with respect to a valuation v in K. Elements of $\hat{K}$ can be written as formal power series in the uniformising variable of the valuation.

$$\hat{K} = \left\{ \sum_{j=n}^{\infty} a_j \pi^j \ : \ n \in \mathbb{Z}, a_j \in \mathfrak{R} \right\}$$

Here $\mathfrak{R}$ is a residue class system mod π. In our case, when $\pi = P \in k[t]$ is a prime polynomial, then for example $\mathfrak{R} = \{U \in k[t] \ : \ \deg(U) < \deg(P)\}$ and for the $\infty-$valuation $\pi = \frac{1}{t}$ and $\mathfrak{R} = k$ (Observe, that $\mathfrak{R}$ is finite if k is finite itself).
If $P \mid D$, we have

$$w_{\mathfrak{p}}(A + B\sqrt{D}) \quad = \quad v_P(A^2 - B^2 D).$$

If $\left(\frac{D}{P}\right) = -1$, we obtain

$$w_{\mathfrak{p}}(A + B\sqrt{D}) \quad = \quad \tfrac{1}{2}v_P(A^2 - B^2 D).$$

If $\left(\frac{D}{P}\right) = 1$, this leads us to

$$\begin{aligned} w_{\mathfrak{p}}(A + B\sqrt{D}) &= v_P(A + B\delta) \\ w'_{\mathfrak{p}}(A + B\sqrt{D}) &= v_P(A - B\delta). \end{aligned}$$

The splitting properties of the $\infty-$valuation depend on the degree of the defining polynomial D. By Hensel's Lemma (see for example [**vdW93**]) one shows that $X^2 - D \in \hat{K}[X]$ splits if and only if $\deg(D)$ is even. As a consequence we obtain the two cases

$$\begin{array}{lll} \deg(D) = 2g + 1 & : & w_\infty(A + B\sqrt{D}) = v_\infty(A^2 - B^2 D) \\ \deg(D) = 2g + 2 & \prec & \begin{array}{ll} w_\infty(A + B\sqrt{D}) &= v_\infty(A + B\delta) \\ w_{\infty'}(A + B\sqrt{D}) &= v_\infty(A - B\delta) \end{array} \end{array}$$

□

In our example we have ramification index $e = 1$ in the cases 2, 3 and 5 and $e = 2$ in the cases 1, and 4.
An algorithm to compute the valuations of an element $\alpha \in \mathfrak{O}_L$ at a place $\mathfrak{p}$ can be formulated as follows.

Algorithm 2.1.

Input: $\alpha = A + B\sqrt{D} \in \mathfrak{O}_L$, $\mathfrak{p} \subseteq \mathfrak{O}_L$ *prime ideal.*
Output: $m = w_{\mathfrak{p}}(\alpha)$, *where* $w_{\mathfrak{p}}$ *is the corresponding valuation.*

begin
If $\alpha = 0$ *then* $m = \infty$
else consider the three cases
1) $\mathfrak{p} = [P, \sqrt{D}]$, *then* $m := 2l$, *where* $l := \max\{n \in \mathbb{N} \,:\, P^n \mid A \text{ and } P^n \mid B\}$.
2) $\mathfrak{p} = P\mathfrak{O}_L$, *then* $m := \max\{n \in \mathbb{N} \,:\, P^n \mid A \text{ and } P^n \mid B\}$.
3) $\mathfrak{p} = [P, X + \sqrt{D}]$ *with* $\delta = \sum_{i=0}^{\infty} a_i P^i$ *and* $X = -a_0$.
Then $m := \max\{n \in \mathbb{N} \,:\, P^n \mid A - B\delta\}$
end.

Observe that it suffices to know the P-adic expansion of $\sqrt{D}$ only up to some fixed $k \geq \max\{\deg(A), \deg(B)\}$.
As the previous theorem suggests, there is a connection between prime ideals in $\mathfrak{O}_L$ and the valuations of $L|k$.

Theorem 2.3. *Every prime ideal of* $\mathfrak{O}_L$ *can be extended in a unique way to the maximal ideal of some valuation ring. Moreover, every maximal ideal of a valuation ring intersected with* $\mathfrak{O}_L$ *is a prime ideal in* $\mathfrak{O}_L$.

Proof. We consider again the three cases:
a) Let $P \in k[t]$ be a prime polynomial with $\left(\frac{D}{P}\right) = 0$, i.e. $P \mid D$. Then we obtain the valuation $w_{\mathfrak{p}}(\alpha) = v_P(\alpha\alpha')$. The corresponding valuation ring and maximal ideal are:

$$\begin{aligned} \mathfrak{O}_{w_{\mathfrak{p}}} &= \left\{\tfrac{A+B\sqrt{D}}{C} \,:\, \gcd(A,B,C) = 1,\, P \nmid C\right\} \\ \mathfrak{p}_w &= \left\{\tfrac{A+B\sqrt{D}}{C} \,:\, \gcd(A,B,C) = 1,\, P \nmid C,\, P \mid A\right\} \end{aligned}$$

Note that $D \equiv 0 \bmod P$.
A uniformising variable is for example $\sqrt{D}$, for $w_{\mathfrak{p}}(\sqrt{D}) = 1$. So $\mathfrak{p}_w = \sqrt{D}\mathfrak{O}_{w_{\mathfrak{p}}}$.
In addition we have $\mathfrak{p}_w \cap \mathfrak{O}_L = [P, \sqrt{D}]$ because

$$\begin{aligned} \alpha \in \mathfrak{p}_w \cap \mathfrak{O}_L &\Leftrightarrow \exists\, A, B \in k[t] \text{ such that } \alpha = A + B\sqrt{D} \text{ and } P \mid A \\ &\Leftrightarrow \exists\, B, U \in k[t] \text{ such that } \alpha = UP + B\sqrt{D} \\ &\Leftrightarrow \alpha \in [P, \sqrt{D}]. \end{aligned}$$

We obtain an isomorphism $\mathfrak{O}_{w_{\mathfrak{p}}}/\mathfrak{p}_w \to \mathfrak{O}_L/\mathfrak{p}$ by $A + \mathfrak{p}_w \mapsto A + \mathfrak{p}$. Observe that $\frac{A+B\sqrt{D}}{C} + \mathfrak{p}_w = \tilde{A} + \mathfrak{p}_w$, where $\tilde{A} \equiv AC^{-1} \bmod P$ and $B\sqrt{D} \in \mathfrak{p}_w$.

b) Let $P \in k[t]$ be a prime polynomial with $\left(\frac{D}{P}\right) = -1$, i.e. D is no quadratic residue modulo P.

$$\begin{aligned} \mathfrak{O}_{w_{\mathfrak{p}}} &= \left\{\alpha = \tfrac{A+B\sqrt{D}}{C} \in L \,:\, w_{\mathfrak{p}}(\alpha) = v_P\left(\tfrac{A^2-B^2D}{C^2}\right) \geq 0\right\} \\ \mathfrak{p}_w &= \left\{\alpha = \tfrac{A+B\sqrt{D}}{C} \in L \,:\, w_{\mathfrak{p}}(\alpha) = v_P\left(\tfrac{A^2-B^2D}{C^2}\right) > 0\right\} \end{aligned}$$

To find an explicit representation for the elements of $\mathfrak{O}_{w_{\mathfrak{p}}}$ and $\mathfrak{p}_w$, we need to examine the numerator and denominator $A^2 - B^2D$ for divisibility by P.

$$A^2 - B^2D \equiv 0 \bmod P \iff A^2 \equiv B^2D \bmod P \iff P \mid A \text{ and } P \mid B$$

The last equivalence holds because $P \nmid D$ and $B \equiv 0 \bmod P$, otherwise AB^{-1} would be a squareroot modulo P.

As a consequence we obtain:

$$\begin{aligned}\mathfrak{O}_{w_\mathfrak{p}} &= \left\{\tfrac{A+B\sqrt{D}}{C} \,:\, \gcd(A,B,C)=1,\, P\nmid C\right\}\\ \mathfrak{p}_w &= \left\{\tfrac{A+B\sqrt{D}}{C} \,:\, \gcd(A,B,C)=1,\, P\nmid C,\, P\mid A,\, P\mid B\right\}\end{aligned}$$

A uniformising variable is for example P, since $w_\mathfrak{p}(P)=1$, so $\mathfrak{p}_w = P\mathfrak{O}_{w_\mathfrak{p}}$. Moreover $\mathfrak{p}_w \cap \mathfrak{O}_L = P\mathfrak{O}_L$, i.e. the maximal ideal of the valuation $w_\mathfrak{p}$ restricted to $\mathfrak{O}_L$ is exactly the prime ideal $P\mathfrak{O}_L$.
The isomorphism $\mathfrak{O}_{w_\mathfrak{p}}/\mathfrak{p}_w \to \mathfrak{O}_L/\mathfrak{p}$ is given by $A+B\sqrt{D}+\mathfrak{p}_w \mapsto A+B\sqrt{D}+\mathfrak{p}$. Observe that $\frac{A+B\sqrt{D}}{C}+\mathfrak{p}_w = \tilde{A}+\tilde{B}\sqrt{D}$, where $\tilde{A}\equiv AC^{-1} \bmod P$ and $\tilde{B}\equiv BC^{-1} \bmod P$.

c) Let $P\in k[t]$ be a prime polynomial with $\left(\frac{D}{P}\right)=1$. Let $X=d_0\in k[t]$, where d_0 is the constant term of the P-adic expansion $\delta=\sum_{j=0}^{\infty} d_jP^j$ of $\sqrt{D}$ in $\hat{K}$. Then this leads us to the two valuations $w_\mathfrak{p}(\frac{A+B\sqrt{D}}{C}) = v_P(\frac{A+B\delta}{C})$ and $w_{\mathfrak{p}'}\left(\frac{A+B\sqrt{D}}{C}\right) = v_P\left(\frac{A-B\delta}{C}\right)$.
The corresponding valuation rings and maximal ideals can be written as:

$$\begin{aligned}\mathfrak{O}_{w_\mathfrak{p}} &= \left\{\tfrac{A+B\sqrt{D}}{C} \,:\, \gcd(A+B\delta,C)=1,\, P\nmid C\right\}\\ \mathfrak{p}_w &= \left\{\tfrac{A+B\sqrt{D}}{C} \,:\, \gcd(A+B\delta,C)=1,\, P\nmid C,\, P\mid (A+B\delta)\right\}\\ \mathfrak{O}_{w_{\mathfrak{p}'}} &= \left\{\tfrac{A+B\sqrt{D}}{C} \,:\, \gcd(A-B\delta,C)=1,\, P\nmid C\right\}\\ \mathfrak{p}'_w &= \left\{\tfrac{A+B\sqrt{D}}{C} \,:\, \gcd(A-B\delta,C)=1,\, P\nmid C,\, P\mid (A-B\delta)\right\}\end{aligned}$$

A uniformising variable for $\mathfrak{O}_{w_\mathfrak{p}}$ is $-X+\sqrt{D}$, since $w_\mathfrak{p}(-X+\sqrt{D}) = v_P(-X+\delta) = v_P(\sum_{j=1}^{\infty} d_jP^j)=1$. Similarly a uniformising variable for $\mathfrak{O}_{w_{\mathfrak{p}'}}$ is $X+\sqrt{D}$, since $v_P(X-\delta)=v_P(\sum_{j=1}^{\infty} d_jP^j)=1$.
Note that $P\mid A+B\delta$ is equivalent to $P\mid A+BX$, since

$$A+B\delta = \sum_{i=0}^{l} a_iP^i + \sum_{i=0}^{m} b_iP^i \cdot \sum_{i=0}^{\infty} d_iP^i$$

In addition $\mathfrak{p}_w\cap\mathfrak{O}_L = [P,-X+\sqrt{D}]$, for

$$\begin{aligned}\alpha\in\mathfrak{p}_w\cap\mathfrak{O}_L &\Leftrightarrow \exists\, A,B\in k[t], \text{ such that } \alpha = A+B\sqrt{D} \text{ and } P\mid A+BX\\ &\Leftrightarrow \exists\, A,B,U\in k[t], \text{ such that } \alpha = A+B\sqrt{D} \text{ and } UP = A+BX\\ &\Leftrightarrow \exists\, A,B,U\in k[t], \text{ such that } \alpha = A+B\sqrt{D} \text{ and } A = UP-BX\\ &\Leftrightarrow \exists\, B,U\in k[t], \text{ such that } \alpha = UP+B(-X+\sqrt{D})\\ &\Leftrightarrow \alpha\in[P,-X+\sqrt{D}].\end{aligned}$$

Similarly one shows that $\mathfrak{p}'_w\cap\mathfrak{O}_L=[P,X+\sqrt{D}]$.
The isomorphism $\mathfrak{O}_{w_\mathfrak{p}}/\mathfrak{p}_w\to\mathfrak{O}_L/\mathfrak{p}$ is given by $A+\mathfrak{p}_w\mapsto A+\mathfrak{p}$. Observe that $\frac{A+B\sqrt{D}}{C}+\mathfrak{p}_w = E+\mathfrak{p}_w$, where $E\equiv AC^{-1}-BC^{-1}X \bmod P$ and the same way $E\equiv AC^{-1}+BC^{-1}X \bmod P$ for $\mathfrak{O}_{w_{\mathfrak{p}'}}/\mathfrak{p}'_w\to\mathfrak{O}_L/\mathfrak{p}'$.

□

In the following we will call prime divisors (places, maximal ideals of valuation rings) *ramified, inert* or *split* depending on the corresponding prime ideal.
As we easily see, $\mathfrak{O}_L = \cap_{w\neq w_\infty}\mathfrak{p}_w$.

Next we will investigate the residue class map for the $\infty-$valuations.
Let $\deg(D) = 2g+1$, then $w_\infty(\frac{A+B\sqrt{D}}{C}) = \frac{1}{2}v_\infty(\frac{A^2-B^2D}{C^2})$. So we can write

$$\begin{aligned}\mathfrak{O}_{w_\infty} &= \left\{\tfrac{A+B\sqrt{D}}{C} \ : \ 2\deg(C) \geq \deg(A^2-B^2D)\right\}\\ \mathfrak{p}_{w_\infty} &= \left\{\tfrac{A+B\sqrt{D}}{C} \ : \ 2\deg(C) > \deg(A^2-B^2D)\right\}\end{aligned}$$

The isomorphism $\mathfrak{O}_{w_\infty}/\mathfrak{p}_{w_\infty} \to k$ is given by $a+\mathfrak{p}_{w_\infty} \mapsto a$. Observe that $\frac{A+B\sqrt{D}}{C} + \mathfrak{p}_{w_\infty} = \frac{\mathrm{lc}(A)}{\mathrm{lc}(C)} + \mathfrak{p}_{w_\infty}$, since $\deg(D)$ is odd, so $\deg(D)+2\deg(B)$ must be greater than $2\deg(C)$ to lie in $\mathfrak{p}_{w_\infty}$.
Let $\deg(D) = 2g+2$ and $\delta \in \hat{K}$ with $\delta^2 = D$, then $w_{\infty_1}(\frac{A+B\sqrt{D}}{C}) = v_\infty(\frac{A+B\delta}{C})$ and

$$\begin{aligned}\mathfrak{O}_{w_{\infty_1}} &= \left\{\tfrac{A+B\sqrt{D}}{C} \ : \ \deg(C) \geq \deg(A+B\delta)\right\}\\ \mathfrak{p}_{w_{\infty_1}} &= \left\{\tfrac{A+B\sqrt{D}}{C} \ : \ \deg(C) > \deg(A+B\delta)\right\}\end{aligned}$$

The isomorphism $\mathfrak{O}_{w_{\infty_1}}/\mathfrak{p}_{w_{\infty_1}} \to k$ is given by $a+\mathfrak{p}_{w_{\infty_1}} \mapsto a$. Observe, that $\frac{A+B\sqrt{D}}{C} + \mathfrak{p}_{w_{\infty_1}} = \frac{\mathrm{lc}(A+B\delta)}{\mathrm{lc}(C)} + \mathfrak{p}_{w_{\infty_1}}$.
Similarly we obtain

$$\begin{aligned}\mathfrak{O}_{w_{\infty_2}} &= \left\{\tfrac{A+B\sqrt{D}}{C} \ : \ \deg(C) \geq \deg(A-B\delta)\right\}\\ \mathfrak{p}_{w_{\infty_2}} &= \left\{\tfrac{A+B\sqrt{D}}{C} \ : \ \deg(C) > \deg(A-B\delta)\right\}\end{aligned}$$

and the corresponding isomorphism where $\frac{A+B\sqrt{D}}{C} + \mathfrak{p}_{w_{\infty_2}} = \frac{\mathrm{lc}(A-B\delta)}{\mathrm{lc}(C)} + \mathfrak{p}_{w_{\infty_2}}$.
Combined with lemma 1.2 we can write down explicit isomorphisms from the residue class fields to finite algebraic extensions of the constant field k.

Definition. *We define the free abelian group on the set of prime divisors as*

$$\mathrm{Div}(L|k) = \left\{\mathfrak{d} \ : \ \mathfrak{d} = \sum_{\mathfrak{p}\in \mathrm{PDiv}(L|k)} m_\mathfrak{p}\mathfrak{p}\right\}$$

and $\deg(\mathfrak{d}) = \sum_{\mathfrak{p}\in\mathrm{supp}(\mathfrak{d})} m_\mathfrak{p}\cdot\deg(\mathfrak{p})$, *where* $\deg(\mathfrak{p})$ *is the absolute degree of the corresponding prime ideal and* $\mathrm{supp}(\mathfrak{d})$ *the support, i.e. the set of prime divisors that occur in* $\mathfrak{D}$.
Since the degree map $\deg : \mathrm{Div}(L|k) \to \mathbb{Z}$ *is a homomorphism, its kernel is a normal subgroup of* $\mathrm{Div}(L|k)$, *that will be denoted by* $\mathrm{Div}_0(L|k)$.

For the rest of this section we assume L to be an imaginary quadratic function field. As shown in Lemma 1.3 this will not be a major restriction.

Definition. *In the case* $\deg(D) = 2g+1$ *the* ∞*-place does not split, so we can define an isomorphic map from the set of fractional ideals* G_L *to* $\mathrm{Div}_0(L|k)$ *by*

$$\begin{array}{rccl}\Phi : & G_L & \to & \mathrm{Div}_0(L|k)\\ & \mathfrak{a} = \mathfrak{p}_1^{m_1}\cdots\mathfrak{p}_r^{m_r} & \mapsto & m_1\mathfrak{p}_1+\cdots+m_r\mathfrak{p}_r - \deg(\mathfrak{a})\infty, \ \ \textit{where } m_j\in\mathbb{Z}\end{array}$$

Here $\deg(\mathfrak{a}) = \sum_{j=1}^{r} m_j\deg(\mathfrak{p}_j)$ *and* $\deg(\mathfrak{p}) = [\mathfrak{O}_L/\mathfrak{p} : k] = [\mathfrak{O}_{w_\mathfrak{p}}/\mathfrak{p}_w : k]$. *The neutral element* $\mathfrak{O}_L$ *in* G_L *is mapped to the zero divisor* $\mathfrak{o}$.
The inverse map is given by

$$\begin{array}{rcl}\mathrm{Div}_0(L|k) & \to & G_L\\ m_1\mathfrak{p}_1+\cdots+m_r\mathfrak{p}_r+m_\infty\infty & \mapsto & \mathfrak{a} = \mathfrak{p}_1^{m_1}\cdots\mathfrak{p}_r^{m_r}\end{array}$$

Definition. *Every $\alpha \in L$ defines a divisor as follows*

$$(\alpha) = \sum_{v \in \mathrm{Val}(L|k)} v(\alpha)\mathfrak{p}_v$$

which we call principal divisor of α.

Theorem 2.4. *The set of principal divisors* $\mathrm{Princ}(L|k)$ *is a normal subgroup of* $\mathrm{Div}_0(L|k)$.

Proof. See [**Sti93**] p. 18. □

Definition. *We define the divisor class group to be the factor group*

$$\mathrm{cDiv}(L|k) = \mathrm{Div}(L|k)/\mathrm{Princ}(L|k)$$

and the Jacobi group (or Jacobian) to be the factor group

$$\mathrm{Jac}(L|k) = \mathrm{Div}_0(L|k)/\mathrm{Princ}(L|k).$$

The next theorem shows that, as one may expect, principal ideals correspond to principal divisors.

Theorem 2.5. *Let $\mathfrak{a} = \gamma\mathfrak{O}_L \in G_L$ be a principal ideal with $\gamma = \gamma_1/\gamma_2 \in L^*$, then the powers of the prime ideals in the prime decomposition are exactly the valuations $w_\mathfrak{p}(\gamma)$ at the corresponding places, i.e. the isomorphism Φ maps principal ideals to principal divisors and consequently* $\mathrm{Jac}(L|k) \cong C_L$.

Proof. Without loss of generality we investigate just the prime decomposition of the numerator $\gamma_1 = A + B\sqrt{D}$ of $\gamma\mathfrak{O}_L$.
Let m be the exponent in the prime decomposition of $\gamma_1\mathfrak{O}_L$. We have to show that $m = w_\mathfrak{p}(\gamma_1)$. As usual we distinguish between the three kinds of prime ideals.

1) $\mathfrak{p} \mid P\mathfrak{O}_L$ with $P \mid D$, i.e. $\mathfrak{p}^2 = P\mathfrak{O}_L$ and $\mathfrak{p} = [P, \sqrt{D}]$.
Since $\gamma_1\mathfrak{O}_L$ is principal and $\mathfrak{p}$ itself is not, $m = 2l$, where $l = \max\{n \in \mathbb{N} : P^n \mid A \text{ and } P^n \mid B\} = v_P(A^2 - B^2D) = w_\mathfrak{p}(\gamma_1)$.
2) $\mathfrak{p} \mid P\mathfrak{O}_L$ where $\left(\frac{D}{P}\right) = -1$, thus $\mathfrak{p} = P\mathfrak{O}_L$.
Obviously $m = \max\{n \in \mathbb{N} : P^n \mid A \text{ and } P^n \mid B\}$. Due to $\left(\frac{D}{P}\right) = -1$, m is the same as $w_\mathfrak{p}(\gamma_1) = \frac{1}{2}v_P(\gamma_1\gamma_1') = v_P(A^2 - B^2D) = \frac{1}{2} \cdot 2m$. (Note that $A^2 \equiv B^2D \bmod P$ implies $P \mid A$ and $P \mid B$ because $\left(\frac{D}{P}\right) = -1$.)
3) $\mathfrak{p} \mid P\mathfrak{O}_L$ where $\left(\frac{D}{P}\right) = 1$.
i) $\mathfrak{p} = [P, X + \sqrt{D}]$, with $X^2 \equiv D \bmod P$ and $\delta = \sum_{i=0}^{\infty} a_i P^i$ the $P-adic$ expansion of $\sqrt{D}$ as an element of $\hat{K}$ with $a_0 = -X$. Let $l = v_P(A - B\delta)$. We show that $\mathfrak{p}_1^m \mid \gamma_1\mathfrak{O}_L$, $\mathfrak{p}^{m+1} \nmid \gamma_1\mathfrak{O}_L$, i.e $\mathfrak{p}^m \supseteq \gamma_1\mathfrak{O}_L$, $\mathfrak{p}^{m+1} \not\supseteq \gamma_1\mathfrak{O}_L$.
Let $\alpha \in \gamma_1\mathfrak{O}_L \Rightarrow \alpha = (A + B\sqrt{D})(U + V\sqrt{D}) = AU + BVD + (AV + BU)\sqrt{D}$.
We define $X_m = a_0 + \cdots + a_{m-1}P^{m-1}$, then $X_m^2 \equiv D \bmod P^m$. So we get

$$\begin{aligned} P^m \parallel A - B\delta &\Rightarrow P^m \parallel A - BX_m \\ &\Rightarrow A - BX_m \equiv 0 \bmod P^m \\ &\Rightarrow (U - VX_m)(A - BX_m) \equiv 0 \bmod P^m \\ &\Rightarrow AU + BVD - (AV + BU)X_m \equiv 0 \bmod P^m \\ &\Rightarrow AU + BVD \equiv (AV + BU)X_m \bmod P^m \end{aligned}$$

If we define K_1 by $K_1P^m = AU + BVD - (AV + BU)X_m$ and $K_2 = AV + BU$,

$$\alpha = K_1P^m + K_2(X_m + \sqrt{D}), \text{ so by theorem 1.7 } \alpha \in \mathfrak{p}_1^m.$$

Since m is chosen maximal such that $P^m \mid (A - B\delta)$, we have $m = l$.

ii) $\mathfrak{p}' = [P, -X + \sqrt{D}]$.
In the same way as in i) we obtain $m = v_P(A + B\delta)$.

□

Theorem 2.5 allows us to compute the prime factorisation of a principal ideal $\gamma\mathfrak{O}_L$ by simply evaluating γ at the corresponding primes (i.e. those that occur in the factorisation of the first generator of its canonical basis).

Remark. *As already mentioned, in the case of $L = k(x, y)$ being a real quadratic function field, the ∞-place splits into two places ∞_1 and ∞_2. In order to obtain a similar relation as in the imaginary quadratic case, we have to choose generators x' and y' of L with the properties $L = k(x', y')$ and only one of the two ∞-places occurs in the denominator of x' (i.e. either $v_{\infty_1}(x') < 0$ or $v_{\infty_2} < 0$ but not both at the same time). This is always possible due to the Riemann part of the Riemann-Roch-theorem (see for example* [**Sti93**] *page 22 et seqq). Then every principal divisor $\mathfrak{p}$ corresponds to a principal ideal $\mathfrak{p}_{x'}$. This will be important for the next chapter.*

3. Hyperelliptic curves

The last section of this chapter gives a geometric interpretation for the results obtained in sections 1 and 2. A more detailed and general approach to hyperelliptic curves can be found for example in the books [**HS00**], [**Lan87**] or [**Mum70**].
Let k be an arbitrary field with $\mathrm{char}(k) \neq 2$. A hyperelliptic curve C of genus $g \geq 1$ over k is an equation of the form

$$C : u^2 = D(t) \quad \text{in } k[t, u],$$

where $D \in k[t]$ is a monic polynomial of degree $2g + 1$. Moreover, there exist no points $(x, 0) \in \bar{k} \times \bar{k}$, such that $D(x) = 0$, and $D'(x) = 0$. Points of that kind are called singular or singularities. A hyperelliptic curve, therefore, does not have any singular points.
We will only consider the case $\deg(D)$ is odd, since if $\deg(D)$ is even we can transform C into $\tilde{C}$ as we have done it in lemma 1.3 with function fields.
We define the set of points on C as

$$C_{\bar{k}} = \{\mathcal{P} = (x, y) \in \bar{k} \times \bar{k}, \text{ where } y^2 = f(x)\} \cup \{\infty\}$$

Here ∞ is a symbol for the special point at infinity which arises from the transition from projective to affine coordinates.
Let $\mathcal{P} = (x, y)$ be a finite point in $C_{\bar{k}}$. Then the opposite point $\mathcal{P}' = (x, -y)$ also lies in $C_{\bar{k}}$.
A finite point $\mathcal{P} = (x, y)$ is called *special* , if $\mathcal{P} = \mathcal{P}'$, i.e. $y = 0$. Otherwise $\mathcal{P}$ is called *ordinary*. The *coordinate ring* $k[C]$ of C over k is defined as

$$k[C] = k[t, u]/(u^2 - D(t)).$$

Elements of $k[C]$ are called polynomial functions on C.
The function field $k(C)$ of C over k is the quotient field of the coodinate ring $k[C]$. Obviously $k(C)$ is a quadratic function field and $k[C]$ is the integral closure of $k[t]$ as defined at the beginning of this chapter.
First we only consider hyperelliptic curves over the algebraic closure $\bar{k}$. These have the advantage that every prime polynomial in $\bar{k}[t]$ has degree 1. Later we will show the extension to the general case.

Definition. *Let $\bar{k}$ be an algebraically closed field and $C_{\bar{k}}$ a hyperelliptic curve over $\bar{k}$. We denote by* $\mathrm{Div}(C_{\bar{k}})$ *the free abelian (additive) group on the set of points of C. An element $\mathfrak{d} \in \mathrm{Div}(C_{\bar{k}})$ is called divisor and can be written as*

$$\mathfrak{d} = \sum_{\mathcal{P} \in C_{\bar{k}}} m_{\mathcal{P}} \mathcal{P} \ , \ m_{\mathcal{P}} \in \mathbb{Z},$$

where only finitely many integers $m_{\mathcal{P}}$ are not equal to 0.
The degree of $\mathfrak{d}$ noted by $\deg(\mathfrak{d})$ *is the integer number* $\sum_{\mathcal{P}\in C_{\bar{k}}} m_{\mathcal{P}}$. *The order of $\mathfrak{d}$ at a point $\mathcal{P}$, written* $\mathrm{ord}_{\mathcal{P}}(\mathfrak{d})$, *is $m_{\mathcal{P}}$.*

Definition. *Let $\mathcal{P} \in C_{\bar{k}}$ be a point on the hyperelliptic curve $C_{\bar{k}}$ and $\alpha = A(t) + B(t)\sqrt{D(t)} \in \bar{k}[C]$.*

1) *If $\mathcal{P} = (x, y)$ is a finite point, we attach the prime polynomial $P = (t-x) \in \bar{k}[t]$ to $\mathcal{P}$ and define* $\mathrm{ord}_{\mathcal{P}}(\alpha) = w_{\mathfrak{p}}(\alpha)$.
If $\mathcal{P}$ is a special point , i.e. $y = 0$, we have $D(t) \equiv D(x) = y^2 = 0 \bmod P$, so $P(t) = t - x$ divides $D(t)$ and we obtain $\mathrm{ord}_{\mathcal{P}}(\alpha) = v_P(\alpha\alpha')$. *(confer theorem 2.2). The corresponding prime ideal is* $[t - x, \sqrt{D}]$.
If $\mathcal{P}$ is an ordinary point, then $D(t) \equiv D(x) = y^2 \bmod x - t$. Thus $D(t)$ is a quadratic residue $\bmod P$ *and we obtain* $\mathrm{ord}_{\mathcal{P}}(\alpha) = w_{\mathfrak{p}}(\alpha)$ *and* $\mathrm{ord}_{\mathcal{P}}(\alpha) = w_{\mathfrak{p}'}(\alpha)$, *where $\mathfrak{p}$ and $\mathfrak{p}'$ correspond to* $[t - x, -y + \sqrt{D}]$ *and* $[t - x, y + \sqrt{D}]$.
Here y and $-y$ are the constant terms in the P-adic expansion of $\sqrt{D}$ in $\hat{K}_v$.
2) *If $\mathcal{P} = \infty$, we define* $\mathrm{ord}_{\infty}(\alpha) = w_{\infty}(\alpha)$.

Since $\bar{k}$ is algebraically closed the case $\left(\frac{D}{P}\right) = -1$ does not occur. Otherwise $\sqrt{D(x)} \notin \bar{k}$, which is a contradiction.
In order to extend the above to non-algebraically closed fields, we need the group of automorphisms.

Definition. *Let k be an arbitrary field* $\mathrm{char}(k) \neq 2$ *and $\bar{k}$ its algebraic closure. Moreover let $C_{\bar{k}}$ be a hyperelliptic curve over $\bar{k}$. If $\mathcal{P} = (x, y) \in C_{\bar{k}}$ and σ is an automorphism of $\bar{k}$ over k, then let $\mathcal{P}^{\sigma} = (\sigma(x), \sigma(y))$ and $\infty^{\sigma} = \infty$.*
A divisor $\mathfrak{d} = \sum m_{\mathcal{P}}\mathcal{P}$ is called rational over k, if $\mathfrak{d}^{\sigma} := \sum_{m_{\mathcal{P}}} \mathcal{P}^{\sigma} = \mathfrak{d}$ for every automorphism $\sigma \in \mathrm{Aut}_k(\bar{k})$. The group of k-rational divisors will be denoted by

$$\mathrm{Div}(C_k) := \{\mathfrak{d} \in \mathrm{Div}(C_{\bar{k}}) \,:\, \mathfrak{d} = \mathfrak{d}^{\sigma} \ \forall \sigma \in \mathrm{Aut}_k(\bar{k})\}$$

Obviously the generators of the k-rational divisors are formal sums of points, which are fixed by every automorphism. We call them *k-rational prime divisors* and denote them by $\mathrm{PDiv}(C_k)$. In case $k = \bar{k}$, we have $\mathrm{PDiv}(C_k) = C_{\bar{k}}$.
The degree of a k-rational prime divisor $\mathfrak{p} = \sum_{i=1}^{r} m_i\mathcal{P}_i$ is defined as $\deg(\mathfrak{p}) = \sum_{i=1}^{r} m_i$. A k-rational divisor $\mathfrak{d}$ can be written as

$$\mathfrak{d} = \sum_{\mathfrak{p}\in\mathrm{PDiv}(C_k)} m_{\mathfrak{p}} \cdot \mathfrak{p}\ ,\ m_{\mathfrak{p}} \in \mathbb{Z},$$

where only finitely many $m_{\mathfrak{p}}$ are $\neq 0$.
The degree of a k-rational divisor $\mathfrak{d}$ is defined as the natural number

$$\deg(\mathfrak{d}) = \sum_{\mathfrak{p}\in\mathrm{PDiv}} m_{\mathfrak{p}} \cdot \deg(\mathfrak{p})$$

and the order of $\mathfrak{d}$ at a prime divisor $\mathfrak{p}$ is $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{d}) = m_{\mathfrak{p}}$. Similarly to the algebraically closed case we want to attach a valuation to every prime divisor and vice versa.

For the rest of this section we assume k to be a perfect field, i.e. prime polynomials in $k[X]$ do not have any multiple roots in $\bar{k}[X]$, but split into prime factors of exponent 1.

For prime divisors $\mathfrak{p} = \sum_{i=1}^{r} m_i\mathcal{P}_i$ this means that all $m_i = 1$, otherwise there would be a prime polynomial in $k[X]$ with a multiple root in $\bar{k}[X]$. Note that every finite field as well as all fields of characteristic 0 are perfect (see for example [**vdW93**]).

Definition. *Let* $\mathfrak{p} = \sum_{i=1}^{r} m_i \mathcal{P}_i$ *be a* k*-rational prime divisor* $\neq \infty$ *with* $\mathcal{P}_i = (x_i, y_i) \in \bar{k} \times \bar{k}$ *and* $P_i = t - x_i$. *As usual we distinguish between the following cases:*

1) $\mathfrak{p}$ *is the sum of pairwise distinct finite special points, i.e.* $\mathfrak{p} = \sum_{i=1}^{r} \mathcal{P}_i$, *where* $\mathcal{P}_i = (x_i, 0)$. *Then we attach the prime polynomial* $P = \prod_{i=1}^{r}(t - x_i) \in k[u]$ *to* $\mathfrak{p}$. *Obviously it divides* $D(t)$ *and we obtain the valuation* $w_{\mathfrak{p}}$ *for the case* $P \mid D$. *The corresponding prime ideal is* $\mathfrak{p} = [P, \sqrt{D}]$.
   So we define $\operatorname{ord}_{\mathfrak{p}}(\alpha) = w_{\mathfrak{p}}(\alpha) = v_P(\alpha\alpha')$.
2) $\mathfrak{p} = \sum_{i=1}^{r} \mathcal{P}_i$ *with* $\mathcal{P}_i = (x_i, y_i)$, *not all* $y_i = 0$ *and the polynomial* $X \in \bar{k}[t]$ *with the property* $X \equiv y_i \mod P_i$ *for* $i = 1, \ldots, r$, *which can be obtained by the chinese remainder theorem lies in* $k[t]$. *Then this leads us to the case* $\left(\frac{D}{P}\right) = 1$
   The corresponding prime ideal is $\mathfrak{p} = [P, -X + \sqrt{D}]$ *or* $[P, X + \sqrt{D}]$ *and we define* $\operatorname{ord}_{\mathfrak{p}}(\alpha) = w_{\mathfrak{p}}(\alpha) = v_P(A - BX)$ *or* $\operatorname{ord}_{\mathfrak{p}'}(\alpha) = w_{\mathfrak{p}}(\alpha) = v_P(A + BX)$ *respectively.*

3) $\mathfrak{p} = \sum_{i=1}^{r} \mathcal{P}_i$ *with* $\mathcal{P}_i = (x_i, y_i)$, *not all* $y_i = 0$ *and the polynomial* $X \in \bar{k}[t]$ *with the property* $X \equiv y_i \mod P_i$ *for* $i = 1, \ldots, r$, *which can be obtained by the chinese remainder theorem does not lie in* $k[t]$. *Then we define* $P = \prod_{i}^{r}(u - x_i)$ *and have the case* $\left(\frac{D}{P}\right) = -1$. *The corresponding ideal is* $P[1, \sqrt{D}]$.
   So we define $\operatorname{ord}_{\mathfrak{p}}(\alpha) = w_{\mathfrak{p}}(\alpha) = \frac{1}{2} v_P(\alpha\alpha')$.
4) $\mathfrak{p} = \infty$, *then we define* $\operatorname{ord}_{\mathfrak{p}}(\alpha) = w_{\infty}(\alpha)$.

Note that, because of $\mathfrak{p} = \mathfrak{p}^{\sigma}$ for every automorphism $\sigma \in \operatorname{Aut}_k(\bar{k})$, the polynomial $P(t)$ must lie in $k[t]$ and in addition has to be prime because of the property of being a generator.

Now that we have defined prime divisors, places and valuations we also obtain the group of degree 0 divisors $\operatorname{Div}_0(C_k)$ and its subgroup of principal divisors $\operatorname{Princ}(C_k)$ as well as the Jacobian $\operatorname{Jac}(C_k)$.
To conclude the first chapter we collect the introduced objects that correspond to each other.

ideal theory	valuation theory / geometrical view
prime ideal $\mathfrak{p}$ of degree 1,	place $\mathfrak{p}_v$, point $\mathcal{P}$ on C_k
prime ideal $\mathfrak{p}$	prime divisor $\mathfrak{p}$
order at a prime ideal $\operatorname{ord}_{\mathfrak{p}}(\mathfrak{a})$	valuation at a place $w_{\mathfrak{p}}(\mathfrak{a})$
if $\deg(D) = 2g + 1$:	
ideal group G_L	divisor group of degree 0 $\operatorname{Div}_0(L)$, $\operatorname{Div}_0(C_k)$
principal ideal group P_L	principal divisor group $\operatorname{Princ}(L)$, $\operatorname{Princ}(C_k)$
ideal class group C_L	Jacobi group $\operatorname{Jac}(L)$, $\operatorname{Jac}(C_k)$
reduced ideal	reduced divisor

CHAPTER 2

Algebraic Correspondences between Quadratic Function Fields

In this chapter we specialise Deuring's theory of algebraic correspondences between function fields to hyperelliptic function fields. At first we introduce the so-called double fields which are the basis for the definition of the correspondences. Subsequently we turn to the main statements the proof of which utilises the fact that algebraic correspondences are equivalent to the description by algebraic equations in algebraic geometry. Finally we show how to compute the image of a divisor class under a correspondence. The theory can also be found in the dissertation of Peter Roquette [**Roq51**], where he proves Riemann's hypothesis for general function fields of characteristic > 0, as well as in the book of Eichler [**Eic63**].
As in chapter 1 section 1 k is an arbitrary (constant) field with $\operatorname{char} k \neq 2$.

1. Divisors of double fields

Definition. *Let $L_1 = k(t,u)$ with $u^2 = D_1(t)$, $D_1 \in k[t]$ and $L_2 = k(x,y)$ where $y^2 = D_2(x)$, $D_2 \in k[x]$ be two quadratic function fields over k, x transcendent over $k(t)$. We call*

$$\Lambda = L_1 L_2 = k(t,u,x,y)$$

a doublefield.

Λ can be considered as a constant field extension of $L_1|k$ from k to L_2 or as a constant field extension of $L_2|k$ from k to L_1. In the following we will mainly deal with $\Lambda|L_1$.
We distinguish between two kinds of prime divisors in the doublefield.

Definition. *Prime divisors $\mathfrak{P}$ of $\Lambda|L_1$ are called non-constant if the respective valuation $w_{\mathfrak{P}}$ evaluates not only the elements of L_1 but also all elements of L_2 to zero. So they also represent non-constant prime divisors of $\Lambda|L_2$.*
Prime divisors of $\Lambda|L_1$ are called constant if there exists an element $\alpha \in L_2$ with $w_{\mathfrak{P}}(\alpha) \neq 0$. A divisor of $\Lambda|L_1$ that only consists of constant divisors is called constant.

Remark. *Note that the residue class map of a non-constant prime divisor $\mathfrak{P}$ maps L_2 isomorphic to a subfield $\overline{L}_2$ of the finite algebraic extension $L_1^* = \mathfrak{O}_v/\mathfrak{P}_v$ of L_1 since all elements of L_2 are evaluated to 0, whereas the residue class map of a constant prime divisor maps the elements $x \in L_2$ with $v(x) \geq 0$ into L_1^* and the rest to ∞.*

The next Lemma gives a simple characterisation of constant divsiors.

Lemma 1.1. *A prime divisor $\mathfrak{P} \neq \infty$ of $\Lambda|L_1$ is constant if and only if the corresponding prime polynomial $P \in L_1[x]$ with $\mathfrak{P} \mid P$ is an element of $k[x]$.*

Proof. Assume $\mathfrak{P}$ is constant and for some $\alpha = (A(x)+B(x)\sqrt{D_2(x)})/C(x) \in L_2$ we have $w_{\mathfrak{P}}(\alpha) > 0$. According to the three cases of theorem 2.2 of chapter 1, $P(x)$ divides either $A(x)^2 - B(x)^2 D(x) \in L_1[x]$, $A(x) + B(x)\delta$ or $A(x) - B(x)\delta$. Since

$A(x)$, $B(x) \in k[x]$, we must also have $P(x) \in k[x]$.
If $P(x) \notin k[x]$, then $w_{\mathfrak{P}}(\alpha) = 0$ for all $\alpha \in L_2$. □

Another important characterisation is given by the next theorems for the proof of which we need the following lemma.

Lemma 1.2. *Let $x, y = \sqrt{D(x)}$ be the generators of the function field $L|k$. Every prime divisor $\mathfrak{p}$ with $v_{\mathfrak{p}}(x) \geq 0$ corresponds one-to-one to generators x_0, y_0 uniquely up to algebraic conjugacy over k in a way that the residue class map* $\bmod \mathfrak{p}$ *maps $(x, y) \mapsto (x_0, y_0)$. We then have*

$$k^* = k(x_0, y_0)$$

is the residue class field $\bmod \mathfrak{p}$ *and* $\deg(\mathfrak{p}) = \deg(k^*|k)$.

Proof. If $v_{\mathfrak{p}}(x) \geq 0$ then we also have $v_{\mathfrak{p}}(y) \geq 0$ since y is integrally dependent on x. By the extension theory of prime divisors (cf. theorem 2.2 of chapter 1) the images $\bar{x}$ and $\bar{y}$ form a basis of $k^*|k$. □

Theorem 1.1. *There is a one-to-one correspondence of constant prime divsiors of $\Lambda|L_1$ and of prime divisors $\mathfrak{p}$ of $L_2|k$, i.e. the residue class map of Λ induces the residue class map of L_2. Moreover we have $L_1^* = L_1 k^*$, where k^* is the residue class field of $\mathfrak{p}$.*

Proof. Restricting the residue class map from Λ to L_2 we obviously obtain the residue class map of a prime divisor $\mathfrak{p}$ of $L_2|k$.
Conversely let $(x, y = \sqrt{D(x)})$ be generators of $L_2|k$, i.e. $L_2 = k(x, y)$, which are $\mathfrak{p}$-integral. The prime divisor $\mathfrak{p}$ corresponds to a finite field extension of k which can be extended to an extension of L_1. By lemma 1.2 this extension corresponds to a prime divisor $\mathfrak{P}$ of $\Lambda|L_1$ the restriction to L_2 of which is in fact nothing else but $\mathfrak{p}$. Moreover we have $\overline{\mathfrak{P}} = \mathfrak{P}$ (conjugacy over L_1) if and only if $\bar{\mathfrak{p}} = \mathfrak{p}$ (conjugacy over k). □

Theorem 1.2. *The non-constant prime divisors $\mathfrak{P}$ of $\Lambda|L_1$ correspond one-to-one to the non-conjugated isomorphisms from $L_2|k$ onto subfields $\overline{L}_2|k$ of finite algebraic extensions L_1^* of L_1. The residue class map $\mu_{\mathfrak{P}}$ induces the isomorphism from L_2 to $\overline{L}_2$.*

$$\mu_{\mathfrak{P}}: \quad \begin{array}{ccccc} \Lambda & \longrightarrow & L_1^* & = & \mathfrak{O}_v/\mathfrak{P}_v \\ \cup & & \cup & \nwarrow & \\ L_2 & \xrightarrow{\sim} & \overline{L}_2 & & L_1 \end{array}$$

Moreover L_1^* can be considered as the compositum $L_1\overline{L}_2$.

Two isomorphisms φ and φ' of $L_2|k$ to subfields $\overline{L}_2|k$, $\overline{L}_2'|k$ of finite algebraic extensions of L_1^* and ${L_1'}^*$ of L_1 are called conjugated, if there is an isomorphism from $L_1^*|L_1$ to ${L_1'}^*|L_1$ that fixes L_1.

$$\begin{array}{ccccccc} & & L_1^* & \overset{\exists\psi}{\longleftrightarrow} & {L_1'}^* & & \\ & \nearrow & & \searrow \quad \swarrow & & \searrow & \\ L_2 & \overset{\varphi}{\longleftrightarrow} & \overline{L}_2 & & L_1 & & \overline{L}_2' \overset{\varphi'}{\longleftrightarrow} L_2 \end{array}$$

Proof. As already mentioned in the remark above, the residue class map of non-constant prime divisors defines an isomorphism from L_2 to some $\overline{L}_2$, which is *per definitionem* a subfield of the finite algebraic extension L_1^* of L_1.
Conversely, we choose generators $x, y = \sqrt{D(x)}$ of $L_2|k$. The given isomorphism corresponds to some generators x_0, y_0 of L_1^* over L_1, so it defines a prime divisor of $\Lambda|L_1$. By lemma 1.2 $\overline{\mathfrak{P}} = \mathfrak{P}$ if and only if the isomorphisms from L_2 are conjugated in the sense defined above. □

The constant prime divisors $\tilde{\mathfrak{p}}$ of $\Lambda|L_2$, i.e. those who correspond to prime divisors $\mathfrak{p}$ of L_1 are also important for the double field $\Lambda|L_1$.

Theorem 1.3. *Let $\tilde{\mathfrak{p}}$ be the prime divisor in the double field $\Lambda|L_2$ that corresponds to the prime divisor $\mathfrak{p}$ of L_1. For an element*

$$\alpha = \frac{A(x)+B(x)\sqrt{D_2(x)}}{C(x)} \in \Lambda|L_1$$

with $A(x) = \sum_{i=0}^{k} a_i x^i$, $B(x) = \sum_{i=0}^{l} b_i x^i$ and $C(x) = \sum_{i=0}^{m} c_i x^i$, $a_i, b_i, c_i \in L_1$ we have

$$v_{\tilde{\mathfrak{p}}}(\alpha) = \min_i(v_{\tilde{\mathfrak{p}}}(a_i), v_{\tilde{\mathfrak{p}}}(b_i)) - \min_i(v_{\tilde{\mathfrak{p}}}(c_i))$$

PROOF. By factoring out the multiples of $\mathfrak{p}$ the assertion is reduced to the following:

If $A(x) + B(x)\sqrt{D(x)}$ and $C(x)$ are $\mathfrak{p}$-primitive (i.e. a uniformising variable of $\mathfrak{p}$ does not divide them), then α is prime to $\tilde{\mathfrak{p}}$.

Assume $A(x) + B(x)\sqrt{D(x)}$ and $C(x)$ are not prime to $\tilde{\mathfrak{p}}$. Since x and $\sqrt{D(x)}$ are $\tilde{\mathfrak{p}}$-integral, $A(x) + B(x)\sqrt{D(x)}$ and $C(x)$ are at least $\tilde{\mathfrak{p}}$-integral. So

$$C(x) \equiv 0 \bmod \tilde{\mathfrak{p}} \text{ and } A(x) + B(x)\sqrt{D(x)} \equiv 0 \bmod \tilde{\mathfrak{p}}$$

In these congruences we now substitute the coefficients of the polynomials $A(x) + B(x)\sqrt{D(x)}$ and $C(x)$ that lie in L_1 by their residues mod $\mathfrak{p}$ in k. For these residues we put $a(x), b(x)$ and $c(x)$ and we obtain congruences mod $\tilde{\mathfrak{p}}$ between elements of L_2. Since elements of L_2 that are different from 0 are units for $\tilde{\mathfrak{p}}$, these congruences are indeed equations

$$c(x) = 0 \text{ and } a(x) + b(x)\sqrt{D(x)} = 0$$

So all coefficients of $a(x), b(x)$ and $c(x)$ must be equal to zero which contradicts the assumed primitivity of $A(x) + B(x)\sqrt{D(x)}$ and $C(x)$. □

Remark. *¿From now on we will denote the constant prime divisors $\tilde{\mathfrak{p}}$ of $\Lambda|L_2$ by the same letter $\mathfrak{p}$ as the corresponding prime divisor of $L_1|k$.*

2. Definition of an algebraic correspondence

For this section we will assume $k = \bar{k}$ to be an algebraically closed field. This means that all prime divisors of $L_1|k$ and $L_2|k$ as well as constant divisors of $\Lambda|L_1$ will have degree 1. Later we will see how to apply the results to the non-algebraically closed case. To define a correspondence we need to introduce the norm of a divisor.

Definition. *Let $L|k$ be a finite algebraic field extension of $L_0|k$ and L' the smallest normal extension of L_0 that contains L, i.e.*

$$L_0 \subseteq L \subseteq L'$$

Let $\bar{k}$ be the algebraic closure of k in L'. Then $L'|\bar{k}$ is an algebraic function field with constant field $\bar{k}$. Moreover let $G = Gal(L'|L_0)$ be the galois group of L' over L_0 and H the subgroup of the automorphisms of L' that keep the elements of L_0 fixed. G/H are the left cosets of G modulo H. For elements $\alpha \in L'$ the norm of α over L_0 is given by

$$N_{L|L_0}(\alpha) = \left(\prod_{\bar{\sigma} \in G/H} \sigma(\alpha) \right)^{[L|L_0]_i}$$

Here $[L|L_0]_i$ is the degree of inseparability of L over L_0.
It is well known (see for example [**Koc97**]*) that the norm is nothing else but the*

determinant of the matrix $A = (a_{ij})$ *representing the multiplication map by* $[\alpha]$ *when considering* L' *as an* L*-vector space, i.e.*

$$N_{L|L_0}(\alpha) = \det((a_{ij})).$$

In a similar way we now introduce the norm of a divisor of L*. If* $\mathfrak{a}$ *is a divisor of* L*, we set*

$$N_{L|L_0}(\mathfrak{a}) = \left(\prod_{\bar{\sigma} \in G/H} \sigma(\mathfrak{a}) \right)^{[L|L_0]_i}.$$

This definition is independent of the choice of the representative σ *of* $\bar{\sigma}$*, because* $\sigma(\mathfrak{a}) = \mathfrak{a}$ *for* $\sigma \in H$*.*

The following theorem lists the essential properties of the norm.

Theorem 2.1.

1) *The norm of a divisor of* L *is a divisor of* L_0*. Hence the norm map is a homomorphism of* $\mathrm{Div}(L|k)$ *into* $\mathrm{Div}(L_0|k)$*.*
2) *If* $\mathfrak{P}$ *is a prime divisor of* L *lying above the prime divisor* $\mathfrak{p}$ *of* L_0*, we have*

$$\mathrm{N}_{L|L_0}(\mathfrak{P}) = \mathfrak{p}^f,$$

   where f *is the relative degree of* $\mathfrak{P}$ *over* $\mathfrak{p}$*.*
3) *If* $\alpha \in L$*,*

$$\mathrm{N}_{L|L_0}((\alpha)) = \left(\mathrm{N}_{L|L_0}(\alpha)\right)$$

4) *If* $\mathfrak{a} \in \mathrm{Div}(L_0|k)$

$$\mathrm{N}_{L|L_0}(\mathfrak{a}) = \mathfrak{a}^{[L:L_0]}$$

5) *If* $\tilde{L} \supset L \supset L_0$ *is a tower of extensions of algebraic function fields, and* $\mathfrak{a} \in \mathrm{Div}(\tilde{L})$*, then*

$$\mathrm{N}_{\tilde{L}|L_0}(\mathfrak{a}) = \mathrm{N}_{\tilde{L}|L}\mathrm{N}_{L|L_0}(\mathfrak{a})$$

Proof. See [**Deu73**] p. 108 ff. □

Definition. *Let* $\mathfrak{D}$ *be a divisor of* $\Lambda|L_1$*. We define a map of the divisor group of* $L_1|k$ *to the divisor group of* $L_2|k$ *by:*

$$\Phi_{\mathfrak{D}} : \mathrm{Div}(L_1|k) \to \mathrm{Div}(L_2|k)$$

Here we have to distinguish between the two cases:

a) $\mathfrak{P}$ *is a constant prime divisor of* $\Lambda|L_1$ *and* $\mathfrak{p}$ *is the associated prime divisor of* $L_2|k$*. In this case we define*

$$\Phi_{\mathfrak{P}}(\mathfrak{a}) := \mathfrak{p}^f \text{ where } f = \deg(\mathfrak{a})$$

b) $\mathfrak{P}$ *is a non-constant prime divisor that maps all* $x \in \Lambda$ *with* $v_{\mathfrak{P}}(x) \geq 0$ *to* L_1^* *and* L_2 *isomorphic to* $\overline{L}_2 \subseteq L_1^*$ *via the residue class map* μ*. Then we define*

$$\Phi_{\mathfrak{P}}(\mathfrak{a}) := \mu^{-1}\left(\mathrm{N}_{L_1^*|\overline{L}_2}(\iota(\mathfrak{a}))\right)$$

   where ι *is the conorm map.*
c) *In general we put*

$$\Phi_{\mathfrak{D}}(\mathfrak{a}) := \prod_{i=1}^{n} \Phi_{\mathfrak{P}_i}(\mathfrak{a}_i)^{r_i} \text{ if } \mathfrak{D} = \textstyle\prod_{i=1}^{n} \mathfrak{P}_i^{r_i}$$

This map $\mathfrak{a} \mapsto \Phi_{\mathfrak{D}}(\mathfrak{a})$ *is called correspondence from* L_1 *to* L_2. *If* $\mathfrak{D}$ *is a prime divisor, we speak of a prime correspondence.*
For non-constant prime divisors we obtain the following diagram:

$$\begin{array}{ccccc} \mathrm{Div}(\Lambda) & \xrightarrow{\mu} & & & \mathrm{Div}(L_1^*) \\ & & & N \swarrow & \qquad\qquad \nwarrow \iota \\ \mathrm{Div}(L_2) & \xrightarrow{\mu} & \mathrm{Div}(\overline{L}_2) & & \mathrm{Div}(L_1) \end{array}$$

Remark. *For simplicity, when talking about correspondences we will omit the* Φ. *So instead of* $\Phi_{\mathfrak{D}}(\mathfrak{a})$ *from now on we will write* $\mathfrak{D}(\mathfrak{a})$.

Correspondences are in fact *per definitionem* homomorphisms from the divisor group of $L_1|k$ to the divisor group of $L_2|k$. As we will see they also map degree zero divisors to degree zero divisors. To show that, let $\mathfrak{P}$ be a non-constant prime divisor of $\Lambda|L_1$ with $\deg \mathfrak{P} = m$ and $\mathfrak{a}$ a divisor of $L_1|k$ of degree f. Then $\mathfrak{a}$ has degree mf in L_1^* because $\deg \mathfrak{P} = [L_1^* : L_1] = m$. Therefore $\mathrm{N}(\mathfrak{a})$ also has degree mf in $\overline{L}_2$. So we have

$$\deg(\mathfrak{P}(\mathfrak{a})) = \deg(\mathfrak{P}) \deg(\mathfrak{a})$$

Per definitionem this also holds for constant prime divisors where $\deg(\mathfrak{p}) = 1$.
For general divisors we obtain

$$\deg(\mathfrak{D}(\mathfrak{a})) = \deg(\mathfrak{D}) \deg(\mathfrak{a})$$

We conclude that a correspondence is also a homomorphic map from $\mathrm{Div}_0(L_1|k)$ to $\mathrm{Div}_0(L_2|k)$.

Remark. *In a geometric context an algebraic correspondence between two hyperelliptic curves given by* $C_1 : u^2 = D_1(t)$ *and* $C_2 : y^2 = D_2(x)$ *is defined to be a subvariety of the Cartesian product* $C_1 \times C_2$, *where the corresponding function fields are* $L_1 = k(t,u)$, $L_2 = k(x,y)$ *and* $\Lambda = L_1 L_2$. *So it can be described as the set of points* $(t,u,x,y) \in k^4$ *that fulfil the equations*

$$\begin{aligned} u^2 - D_1(t) &= 0 \\ y^2 - D_2(x) &= 0 \\ F_1(t,u,x,y) &= 0 \\ &\vdots \\ F_n(t,u,x,y) &= 0 \end{aligned}$$

We first assume $n = 1$.
Since $y^2 = D_2(x)$ *instead of* $F(t,u,x,y) = 0$ *we can write*

$$F(t,u,x,y) = G(t,u,x) + H(t,u,x)y = 0.$$

Multiplication by $G(t,u,x) - H(t,u,x)y$ *yields*

$$A(t,u,x) = G^2(t,u,x) - H^2(t,u,x)D_2(x) = 0.$$

We first assume $\gcd(A,H) = 1$. *The map* Φ *that maps a point of* C_1 *to a sum of points of* C_2 *given by this correspondence is defined to be*

$$(t_0,u_0) \mapsto \mathfrak{a} = [A(t_0,u_0,x), -G(t_0,u_0,x)H(t_0,u_0,x)^{-1} \bmod A(t_0,u_0,x)]$$

So the equations above define a divisor of $\Lambda|L_1$

$$\mathfrak{A} = [A(t,u,x), -G(t,u,x)H(t,u,x)^{-1} \bmod A(t,u,x)].$$

If $\gcd(A,H) = P(t,u,x)$, *then we define*

$$F'(t,u,x,y) = P(t,u,x)(G'(t,u,x) + H'(t,u,x)y)$$

and

$$A'(t,u,x) = G'^2(t,u,x) - H'^2(t,u,x)D_2(x).$$

The map Φ *is then defined by*

$$(t_0,u_0) \mapsto \mathfrak{a}' + \mathfrak{p},$$

where $\mathfrak{p}$ *is the principal divisor of* L_2 *given by* $P(t_0,u_0,x)$.
If $n > 1$ *then we only consider the* $\gcd(A_1(t,u,x),\ldots,A_n(t,u,x))$ *in* $L_1[x]$ *and if it is not equal to* 1, *check if the* F_ν *all define the same* y.
The residue ideal theorem 2.3 will show that the correspondence map defined by Deuring is equivalent to that in algebraic geometry.

As the next theorem shows a correspondence yields even a homomorphism of the corresponding class groups and Jacobi groups.

Theorem 2.2. *If* $\mathfrak{a} \sim 1$ *then* $\mathfrak{D}(\mathfrak{a}) \sim 1$.

PROOF. It suffices to prove the assertion for a prime divisor $\mathfrak{P}$, i.e. to show that $\mathfrak{P}(\mathfrak{a}) \sim 1$ if $\mathfrak{a} \sim 1$.
If $\mathfrak{P}$ is constant, then $\mathfrak{P}(a) = 1$ by definition since $\mathfrak{a}$, being a principal divisor, has degree 0. If $\mathfrak{P}$ is non-constant, then the property of being principal goes through the definiton of $\mathfrak{P}(\mathfrak{a})$: $\mathfrak{a}$ is also principal in L_1^*, therefore $\mathrm{N}(\mathfrak{a})$ principal in $\overline{L}_2$ and hence the preimage $\mathfrak{P}(\mathfrak{a})$ is also a principal divisor in L_2. □

In the following we consider special subgroups of the divisor group $\mathrm{Div}(\Lambda|L_1)$.

Definition. *We define the group of coarser divisors of* $\Lambda|L_1$ *to be the group of the divisors of* $\Lambda|L_1$ *modulo the constant divisors.*

$$\mathrm{Div}^c(\Lambda|L_1) := \mathrm{Div}(\Lambda|L_1)/(\mathrm{Div}(L_2|k))$$

and analogously

$$\mathrm{cDiv}^c(\Lambda|L_1) := \mathrm{cDiv}(\Lambda|L_1)/(\mathrm{Div}(L_2|k))$$

Remark. *When talking about non-trivial correspondences we think of correspondences given by a degree* 0 *divisor of the double field that is in a coarser sense not equivalent to the trivial class.*
Note that we can always find a representative of a coarser divisor class of degree 0, *since the* ∞*-prime divisors are constant divisors. This is also the reason why we do not need to distinguish between imaginary and real quadratic double fields when talking about the ideal class group. The constant* ∞*-prime divisors do not play a role for the coarser divisor class, so the coarser divisor class group is in both the real and imaginary quadratic case isomorphic to the coarser ideal class group.*

We will now provide the reader with some notions and facts about ideals in $\Lambda|L_1$. Let $\mathfrak{A} \in \mathrm{Div}(\Lambda|L_1)$ be a divisor of $\Lambda|L_1$, then we denote by $\mathfrak{A}_x$ the unique corresponding (fractional) ideal in the ideal group G_Λ given by the isomorphism Φ (cf. the definitions above theorem 2.5 of chapter 2) in the imaginary quadratic case and in the real case we define it to be the ideal that consists of the product of all prime ideals that correspond to prime divisors with $v_\mathfrak{p}(x) > 0$. In the real case $\mathfrak{A}$ is not uniquely determined by $\mathfrak{A}_x$ but for our purposes it is enough to know that, as already remarked after theorem 2.5, we can choose an x such that only one prime divisor $\mathfrak{p}_\infty$ occurs in the denominator of $\mathfrak{A}$ and then principal divisors correspond to principal ideals.

Definition. *Let* $\frac{1}{A(x)} \cdot [R(x), S(x) + T(x)\sqrt{D_2(x)}]$ *be a canonical* $L_1[x]$*-basis of the fractional ideal* $\mathfrak{A}_x$, *where* $R(x), S(x), T(x) \in L_1[x]$. *Without loss of generality we can assume that* $A(x)$ *is* $\mathfrak{p}$*-primitive. We call such a canonical basis* $\mathfrak{p}$*-regular if*

1. $R(x), S(x)$ *and* $T(x)$ *are* $\mathfrak{p}$*-integral and*

2. *the polynomials $A(x)$ and $R(x)T(x)$ have the highest coefficients prime to $\mathfrak{p}$. We call an ideal $\mathfrak{A}_x$ uncombined to $\mathfrak{p}$ if it has a $\mathfrak{p}$-regular $L_1[x]$-basis.*

Obviously every canonical basis $\frac{1}{A(x)}[R(x), S(x)+T(x)\sqrt{D_2(x)}]$ of a fractional ideal $\mathfrak{A}_x$ is $\mathfrak{p}$-regular for almost all (i.e. all but finitely many) $\mathfrak{p}$ and $\mathfrak{A}_x$ is uncombined to almost all $\mathfrak{p}$.
Notice also that all $\mathfrak{p}$-integral elements $\alpha \in \mathfrak{A}_x$ are given exactly by

$$\alpha = \frac{1}{A(x)}(F_1(x)R(x) + F_2(x)(S(x) + T(x)\sqrt{D_2(x)}))$$

with $\mathfrak{p}$-integral polynomials $F_1(x)$ and $F_2(x)$ in $L_1[x]$. This can be seen by the following argumentation. On the one hand, these α are $\mathfrak{p}$-integral. On the other hand, $A(x)\mathfrak{A}_x \subseteq \mathfrak{O}_\Lambda$, so α can be represented by $\alpha = \frac{H_1(x)+H_2(x)\sqrt{D_2(x)}}{A(x)}$ with $H_i(x) \in L_1[x]$. If α is $\mathfrak{p}$-integral, then because of theorem 1.3 the $H_i(x)$ are $\mathfrak{p}$-integral. $F_1(x), F_2(x)$ can be computed by solving the linear equation system

$$\begin{array}{rcl} F_1(x)R(x) + F_2(x)S(x) & = & H_1(x) \\ F_2(x)T(x) & = & H_2(x) \end{array}$$

with determinant $R(x)T(x) \in L_1[x]$. Since the highest coefficient of this determinant is $\mathfrak{p}$-prime, the polynomials $F_1(x), F_2(x)$ are in fact $\mathfrak{p}$-integral.
We now consider residues $\bmod \mathfrak{p}$ in L_2 of $\mathfrak{p}$-integral elements of $\mathfrak{A}_x$.

Definition. *If $\frac{1}{A(x)}[R(x), S(x) + T(x)\sqrt{D_2(x)}]$ is a $\mathfrak{p}$-regular $L_1[x]$-basis of $\mathfrak{A}_x$ then $\mathfrak{A}_x \bmod \mathfrak{p} = \frac{1}{A_0(x)}[R_0(x), S_0(x) + T_0(x)\sqrt{D_2(x)}]$ is defined to be the corresponding residue ideal, where $R_0(x) \equiv R(x) \bmod \mathfrak{p}$, $S_0(x)+T_0(x)\sqrt{D_2(x)} \equiv S(x) + T(x)\sqrt{D_2(x)} \bmod \mathfrak{p}$ and $A_0(x) \equiv A(x) \bmod \mathfrak{p}$.*

Since $\deg(\mathfrak{p}) = 1$ (k is algebraically closed), the corresponding prime polynomial $P(t) = t - a \in k[t]$ is of degree 1 and $\mathfrak{p}$ is split or ramified. So we only have to substitute t by a and $\sqrt{D_1(t)}$ by $\pm\sqrt{D_1(a)} \in k$ to obtain $R_0(x) \in L_2$ from $R(x)$ and $S_0(x) + T_0(x)\sqrt{D_2(x)} \in L_2$ from $R(x) + T(x)\sqrt{D_2(x)}$. As a consequence $\frac{1}{A_0(x)}[R_0(x), S_0(x) + T_0(x)\sqrt{D_2(x)}]$ is a canonical $k[x]$-basis of a fractional ideal of L_2. So we have shown

Lemma 2.1. *Let $\mathfrak{A}_x$ be an uncombined ideal of $\Lambda|L_1$, then by the residue class map a $\mathfrak{p}$-regular $L_1[x]$-basis $A_1(x), A_2(x)$ of $\mathfrak{A}_x$ is mapped to a $k[x]$-basis a_1, a_2 of $\mathfrak{A}_x \bmod \mathfrak{p}$.*

As an immediate implication of the second property of a $\mathfrak{p}$-regular basis we obtain: if $\mathfrak{A}_x$ is a $\mathfrak{p}$-regular fractional $\mathfrak{O}_\Lambda$-ideal, then $\deg(\mathfrak{A}_x) = \deg(\mathfrak{A}_x \bmod \mathfrak{p})$. Moreover we state

Lemma 2.2. *If $\mathfrak{A}_x, \mathfrak{B}_x, \mathfrak{A}_x\mathfrak{B}_x$ are uncombined to $\mathfrak{p}$, then*

$$\mathfrak{A}_x\mathfrak{B}_x \bmod \mathfrak{p} = \mathfrak{A}_x \bmod \mathfrak{p} \cdot \mathfrak{B}_x \bmod \mathfrak{p}$$

PROOF. By the definition of the residue ideal it follows that

$$\mathfrak{A}_x\mathfrak{B}_x \bmod \mathfrak{p} \subseteq \mathfrak{A}_x \bmod \mathfrak{p} \cdot \mathfrak{B}_x \bmod \mathfrak{p}$$

Since $\mathfrak{A}_x, \mathfrak{B}_x, \mathfrak{A}_x\mathfrak{B}_x$ are uncombined to $\mathfrak{p}$, both ideals on the left and right hand side have the same degree and therefore must be equal. □

Assume $L_1^*|k$ to be an algebraic function field in one variable with $L_1^* = L_1\overline{L}_2$. Let $S_1, S_2, \mathrm{N}_1, \mathrm{N}_2$ be the trace and norm to L_1 and $\overline{L}_2$ respectively.

Lemma 2.3. *The least multiple in $\overline{L}_2$ of a prime divisor $\mathfrak{p}_1$ of L_1 is equal to $\mathrm{N}_2(\mathfrak{p}_1)$ and the least multiple of a prime divisor $\mathfrak{p}_2$ of $\overline{L}_2$ that lies in L_1 is equal to $\mathrm{N}_1(\mathfrak{p}_2)$, if we only consider all but finitely many $\mathfrak{p}_1, \mathfrak{p}_2$.*

PROOF. See [**Deu37**] □

Remark. *More precisely, Deuring shows that if* $\omega_1, \ldots, \omega_r$ *is a basis for* $L_1^*|L_1$ *that lies in* $\overline{L}_2$*, then the assertion is true for all prime divisors* $\mathfrak{p}$ *that lie neither in the support of the numerator divisor of the discriminant* $\det(\omega_i\omega_j)$ *nor in the support of the denominator divisors of the* ω_i*.*

As a consequence of lemma 2.3 we can conclude

$$\begin{array}{rcl} \alpha_2 \equiv 0 \mod \mathfrak{p}_1 \text{ in } \overline{L}_2 & \Rightarrow & \alpha_2 \equiv 0 \mod \mathrm{N}_2(\mathfrak{p}_1) \\ \alpha_1 \equiv 0 \mod \mathfrak{p}_2 \text{ in } L_1 & \Rightarrow & \alpha_1 \equiv 0 \mod \mathrm{N}_1(\mathfrak{p}_2) \end{array}$$

The next theorem is the basis for Deuring's main result. It shows that the algebraic correspondences defined above are in fact equivalent to the description by algebraic equations in algebraic geometry.

Theorem 2.3 (residue ideal theorem)**.** *Let* $\mathfrak{D} \in \mathrm{Div}(\Lambda|L_1)$ *be a divisor of the double field* $\Lambda|L_1$ *then for all but finitely many prime divisors* $\mathfrak{p} \in \mathrm{Div}(L_1|k)$ *we have*

$$\mathfrak{D}_x \bmod \mathfrak{p} = \mathfrak{D}(\mathfrak{p})_x$$

PROOF. We show the theorem under the following three assumptions which are obviously true for almost all prime divisors $\mathfrak{p}$.

1. $\mathfrak{p}$ is prime to the denominator of the image $\bar{x}$ of x in $\overline{L}_2$ when applying the residue class homomorphism $\bmod \mathfrak{P}$, i.e. $\bar{x}$ is $\mathfrak{p}$-integral.
2. lemma 2.3 can be applied to $\mathfrak{p}$ (cf. the remark above).
3. $\mathfrak{P}_x$ is uncombined to $\mathfrak{p}$, i.e. $\mathfrak{P}_x \bmod \mathfrak{p}$ has the same degree as $\mathfrak{P}$.

We will prove the assertion in three steps:

a) for a prime divisor $\mathfrak{D} = \mathfrak{P}$ with 1. and 2. we have $\mathfrak{P}_x \bmod \mathfrak{p} \subseteq \mathfrak{P}(\mathfrak{p})_x$,
b) if 3. holds, we even obtain $\mathfrak{P}_x \bmod \mathfrak{p} = \mathfrak{P}(\mathfrak{p})_x$,
c) the assertion is also true for composite $\mathfrak{D} = \prod_{i=1}^{n} \mathfrak{P}_i^{e_i}$.

If $\mathfrak{P} = \mathfrak{P}_\infty$, then $\mathfrak{P}_\infty(\mathfrak{a}) = \mathfrak{p}_\infty^{\deg(\mathfrak{a})}$. Since $\mathfrak{P}_\infty \bmod \mathfrak{p} = \mathfrak{p}_\infty$, a) is true at least for a prime divisor $\mathfrak{P}_\infty$. Now let $\mathfrak{P} \neq \mathfrak{P}_\infty$, i.e. x is $\mathfrak{P}$-integral, and

$$\alpha = F_1(x) + F_2(x)\sqrt{D_2(x)} \in \mathfrak{P}_x,$$

in other words

$$\alpha \equiv 0 \bmod \mathfrak{P}_x \text{ in } \Lambda.$$

Applying the residue class map $\bmod \mathfrak{P}$ leads to

$$F_1(\bar{x}) + F_2(\bar{x})\bar{y} \equiv 0 \bmod \mathfrak{P} \text{ in } L_1^*.$$

Since x is assumed to be $\mathfrak{p}$-integral because of 1., $\bar{y}$ as algebraically integral dependent on $\bar{x}$ is also $\mathfrak{p}$-integral. Because of theorem 1.3 we can consider residues $\bmod \mathfrak{p}$, i.e.

$$f_1(\bar{x}) + f_2(\bar{x})\bar{y} \equiv 0 \bmod \mathfrak{p} \text{ in } L_1^*.$$

Moreover, 2. yields

$$f_1(\bar{x}) + f_2(\bar{x})\bar{y} \equiv 0 \bmod \mathrm{N}(\mathfrak{p}) \text{ in } \overline{L}_2.$$

Applying μ^{-1}, by definition of $\mathfrak{P}(\mathfrak{p})$, we finally obtain

$$f_1(x) + f_2(x)\sqrt{D_2(x)} \equiv 0 \bmod \mathfrak{P}(\mathfrak{p}) \text{ in } L_2,$$

which concludes the proof of a). Observe that for constant $\mathfrak{P}$, we immediately get the last congruence by applying the residue class map $\bmod \mathfrak{P}$ on

$$F_1(\bar{x}) + F_2(\bar{x})\bar{y} \equiv 0 \bmod \mathfrak{P} \text{ in } L_1^*.$$

Using assumption 3., we conclude

$$\deg(\mathfrak{P}_x \bmod \mathfrak{p}) = \deg(\mathfrak{P}_x) = \deg(\mathfrak{P}).$$

By the degree rule we have

$$\deg(\mathfrak{P}(\mathfrak{p})_x) = \deg(\mathfrak{P}(\mathfrak{p})) = \deg(\mathfrak{P}) \cdot \deg(\mathfrak{p}) = \deg(\mathfrak{P})$$

so we obtain

$$\deg(\mathfrak{P}_x \bmod \mathfrak{p}) = \deg(\mathfrak{P}(\mathfrak{p})_x)$$

Together with statement a), which has been proved already, this concludes the proof of b).
It remains to show the composite case, i.e.

$$\mathfrak{D} = \prod_{i=1}^{n} \mathfrak{P}_i^{e_i}$$

By the definition of a correspondence

$$\mathfrak{D}(\mathfrak{p}) = \prod_{i=1}^{n} \mathfrak{P}_i(\mathfrak{p})^{e_i},$$

which means

$$\mathfrak{D}(\mathfrak{p})_x = \prod_{i=1}^{n} \mathfrak{P}_i(\mathfrak{p})_x^{e_i}.$$

Now we can apply lemma 2.2 for almost all $\mathfrak{p}$, which yields

$$\mathfrak{D}_x \bmod \mathfrak{p} = \prod_{i=1}^{n} (\mathfrak{P}_{ix} \bmod \mathfrak{p})^{e_i},$$

and have thus proven the last assertion c) and therefore the whole theorem. □

3. Main theorem of the theory of correspondences

The main result which is due to Deuring states the following:

There is a one-to-one correspondence between:

divisor $\mathfrak{D}$	action of the correspondence $\mathfrak{a} \mapsto \mathfrak{D}(\mathfrak{a})$ on $\mathrm{Div}(L_1\|k)$
coarser divisor $\mathfrak{D}$	action of the correspondence on $\mathrm{Div}_0(L_1\|k)$
ordinary class of $\mathfrak{D}$	action of the correspondence on $\mathrm{cDiv}(L_1\|k)$
coarser divisor class of $\mathfrak{D}$	action of the correspondence on $\mathrm{Jac}(L_1\|k)$

For our purposes the last assertion is of special interest, since we will mostly deal with the Jacobi group. It shows that the interesting correspondences (i.e. the non-trivial ones) are those which lie over a splitting $P \in L_1[x]$, i.e. $\left(\frac{D(x)}{P(x)}\right) = 1$ or $D(x)$ is a quadratic residue in $L_1[x] \bmod P(x)$, with $\deg_x(P) \leq g$. Only those play a role for the coarser divisor class group of the doublefield.
We now formulate the above result more explicitly by several theorems. By $\mathfrak{D}_c$ we will always think of a constant divisor of $\Lambda|L_1$ and $\mathfrak{a}_0$ will always be a divisor of degree 0 of $L_1|k$.

Theorem 3.1. *If* $\mathfrak{D} = 1$ *then* $\mathfrak{D}(\mathfrak{a}) = 1$ *for all* $\mathfrak{a} \in \mathrm{Div}(L_1|k)$

Proof. By definition of a correspondence we have for $\mathfrak{D} = \mathfrak{P}^0 = 1$, that $\mathfrak{D}(\mathfrak{a}) = 1(\mathfrak{a}) = 1$ for all $\mathfrak{a} \in \mathrm{Div}(L_1|k)$. □

Theorem 3.2. *If* $\mathfrak{D} = \mathfrak{D}_c$ *then* $\mathfrak{D}(\mathfrak{a}_0) = 1$ *for all* $\mathfrak{a}_0 \in \mathrm{Div}_0(L_1|k)$

PROOF. If $\mathfrak{D}$ is constant then by definition $\mathfrak{P}(\mathfrak{a}_0) = 1$ for every constant prime divisor $\mathfrak{P}$ that divides $\mathfrak{D}$, whence also $\mathfrak{D}(\mathfrak{a}_0) = 1$. □

Theorem 3.3. *If* $\mathfrak{D} \sim 1$ *then* $\mathfrak{D}(\mathfrak{a}) \sim 1$ *for all* $\mathfrak{a} \in \mathrm{Div}(L_1|k)$

PROOF. We can apply the residue ideal theorem for almost all $\mathfrak{p}$ in L_1. Let $\mathfrak{p}$ be such a valid prime divisor of L_1. We normalise $\mathfrak{D}$ by a prime power of $\mathfrak{p}$, such that $\mathfrak{D}$ is prime to $\mathfrak{p}$ (note that we consider $\mathfrak{D}$ as a divisor of $\Lambda|L_1$).
Let $\mathfrak{D}$ be given as the principal ideal of $\Delta \in \Lambda$ and $\Delta \equiv \delta \bmod \mathfrak{p}$, $\delta \neq 0$ in L_2, then

$$\mathfrak{D}_x = \Delta\mathfrak{O}_\Lambda, \ \mathfrak{D}_x \bmod \mathfrak{p} = \delta\mathfrak{O}_{L_2}.$$

So by the residue theorem we obtain

$$\mathfrak{D}(\mathfrak{p})_x = \delta\mathfrak{O}_{L_2}$$

and hence

$$\mathfrak{D}(\mathfrak{p}) \sim 1 \text{ for almost all } \mathfrak{p}$$

and even

$$\mathfrak{D}(\mathfrak{a}) \sim 1 \text{ for all } \mathfrak{a} \text{ that are prime to finitely many } \mathfrak{p}.$$

Since by the homomorphism theorem 2.2, $\mathfrak{D}(\mathfrak{a})$ only depends on the class of $\mathfrak{a}$ and since in every class there is a divisor that is prime to finitely many $\mathfrak{p}$ (strong approximation theorem, cf [**Sti93**] p. 31), we conclude that $\mathfrak{D}(\mathfrak{a}) \sim 1$ for all $\mathfrak{a}$ as was to be shown. □

Theorem 3.4. *If* $\mathfrak{D} \sim \mathfrak{D}_c$ *then* $\mathfrak{D}(\mathfrak{a}_0) \sim 1$ *for all* $\mathfrak{a}_0 \in \mathrm{Div}_0(L_1|k)$.

PROOF. If $\mathfrak{D} \sim \mathfrak{D}_c$, i.e. $\frac{\mathfrak{D}}{\mathfrak{D}_c} \sim 1$, then by the last theorem we have $\frac{\mathfrak{D}}{\mathfrak{D}_c}(\mathfrak{a}) \sim 1$ for all $\mathfrak{a}$, in other words $\mathfrak{D}(\mathfrak{a}) \sim \mathfrak{D}_c(\mathfrak{a})$ for all $\mathfrak{a}$. By definition we have $\mathfrak{D}_c(\mathfrak{a}_0) = 1$ for every $\mathfrak{a}_0$ and therefore $\mathfrak{D}(\mathfrak{a}_0) \sim 1$ for all $\mathfrak{a}_0$. □

Thus we have shown that the action of a correspondence on the respective group only depends on the associated class in the divisor group of the double field. The next 4 theorems show the converse directions.

Theorem 3.5. *If* $\mathfrak{D} \neq 1$ *then* $\mathfrak{D}(\mathfrak{p}) \neq 1$ *for almost all* $\mathfrak{p}$.

PROOF. Let $\mathfrak{D} \neq 1$. If $\mathfrak{D}$ is integral, then $\mathfrak{D}(\mathfrak{p})$ is also integral by definition and hence $\neq 1$ even for all $\mathfrak{p}$.
It remains to be shown that if $\mathfrak{D}$ is fractional, then $\mathfrak{D}(\mathfrak{p})$ is also fractional for almost all $\mathfrak{p}$. Using the residue ideal theorem, it is sufficient to show that

$$\mathfrak{D} \bmod \mathfrak{p} \text{ is fractional for almost all } \mathfrak{p}.$$

For this reason let

$$\tfrac{1}{A(x)}[R(x), S(x) + T(x)\sqrt{D_2(x)}]$$

be a $\mathfrak{p}$-regular (canonical) $L_1[x]$-basis of $\mathfrak{D}_x$. This is possible for almost all $\mathfrak{p}$. Then the assumption that $\mathfrak{D}$ is fractional is equivalent to $A(x) \nmid R(x)T(x)$. Passing to residues $\bmod \mathfrak{p}$ in L_2 by lemma 2.1 this yields a $k[x]$-basis

$$\tfrac{1}{A_0(x)}[R_0(x), S_0(x) + T_0(x)\sqrt{D_2(x)}]$$

of $\mathfrak{D}_x \bmod \mathfrak{p}$, which is fractional for almost all $\mathfrak{p}$ due to the $\mathfrak{p}$-regularity.

□

Theorem 3.6. *If* $\mathfrak{D} \neq \mathfrak{D}_c$ *then* $\mathfrak{D}(\mathfrak{p}\mathfrak{p}_\infty^{-1}) \neq 1$ *for almost all* $\mathfrak{p}$.

PROOF. Let $\mathfrak{D}$ be a non-constant divisor of $\Lambda|L_1$. If $\mathfrak{p}_\infty$ is one of the ∞-divisors of $L_1|k$ and $\mathfrak{D}_c$ is the constant divisor of $\Lambda|L_1$ that corresponds to $\mathfrak{D}(\mathfrak{p}_\infty)$, then

$$\mathfrak{D}\left(\frac{\mathfrak{p}}{\mathfrak{p}_\infty}\right) = \frac{\mathfrak{D}(\mathfrak{p})}{\mathfrak{D}(\mathfrak{p}_\infty)} = \frac{\mathfrak{D}(\mathfrak{p})}{\mathfrak{D}_c(\mathfrak{p})} = \frac{\mathfrak{D}}{\mathfrak{D}_c}(\mathfrak{p}).$$

By assumption $\frac{\mathfrak{D}}{\mathfrak{D}_c} \neq 1$, so theorem 3.5 yields $\mathfrak{D}\left(\frac{\mathfrak{p}}{\mathfrak{p}_\infty}\right) \neq 1$ for almost all $\mathfrak{p}$. □

Theorem 3.7. *If $\mathfrak{D} \not\sim 1$ then $\mathfrak{D}(\mathfrak{p}) \not\sim 1$ for almost all $\mathfrak{p}$.*

PROOF. Let $\mathfrak{D} \not\sim 1$. If $\deg(\mathfrak{D}) \neq 0$, then by the degree rule $\deg(\mathfrak{D}(\mathfrak{p})) \neq 0$ and consequently the assertion is true for all $\mathfrak{p}$.
To prove the claim in the case of $\deg(\mathfrak{D}) = 0$ as well, instead of $\mathfrak{D}$ we can choose any equivalent divisor $\mathfrak{A}$. For simplicity we take a reduced one. Then the assumption that $\mathfrak{A} \not\sim 1$ is equivalent to $\mathfrak{A}_x$ not being a principal ideal. For this reason we deduce a computational criterion to decide whether an ideal is principal or not.
We have $\mathfrak{A}_x \sim \mathfrak{O}_\Lambda$ if and only if there is an elment $\alpha \in \mathfrak{A}_x$ with $\deg_x(\mathrm{N}_{\Lambda|L_1(x)}(\alpha)) = \deg(A_x) = r$. Here the norm of α is considered as a polynomial in x. Since $\deg(\mathrm{N}(\alpha))$ is at least r, we can also postulate the existence of an element $\alpha \in \mathfrak{A}_x$ with $\deg(\alpha) \leq r$. Let $\mathfrak{A}_x = [R(x), S(x) + T(x)\sqrt{D_2(x)}]$ be the canonical basis of $\mathfrak{A}_x$, where $R = AT$, $S = BT$, $D_2 = B^2 - AC$. An element $\alpha \in \mathfrak{A}_x$ can be written as

$$\alpha = T(x)[U_1(x)A(x) + U_2(x)(B(x) + \sqrt{D_2(x)})]$$

with polynomials $U_1, U_2 \in L_1[x]$. As a consequence

$$\mathrm{N}(\alpha) = T(x)^2[(U_1(x)A(x) + U_2(x)B(x))^2 - U_2(x)^2 D_2(x)]$$

Since $\deg(D_2) = 2g_2 + 1$ is odd, to find an integral element in $\mathfrak{A}_x$ of norm r, we only need to consider polynomials $U_1(x), U_2(x)$ of x-degree less than or equal to $M = \lceil \frac{r}{2} \rceil$. We write $U_i(x) = \sum_{j=0}^{M} u_{ij}x^j$ for $i = 1, 2$. If we sort $\mathrm{N}(\alpha)$ for x we obtain

$$\mathrm{N}(\alpha) = \sum_{i=0}^{N} G_i(u)x^i$$

where the G_i are polynomials in the unknowns u_{ij} with coefficients in L_1. The condition $\mathrm{N}(\alpha) \leq r$ is therefore equivalent to

$$G_i(u) = 0, \text{ for } i = r+1, \ldots, N$$

Let $R_i(u)$ be the resultants of the previous homogeneous equation system, then this system is solvable by non-trivial u_{ij} (i.e. not all $u_{ij} = 0$) if and only if $R_i(u) = 0$. (see [**vdW93**] p.166).
For almost all $\mathfrak{p}$, $[R_0(x), S_0(x) + T_0(x)\sqrt{D_2(x)}]$ with $R_0(x) = R(x) \bmod \mathfrak{p}$, $S_0(x) + T_0(x)\sqrt{D_2(x)} = S(x) + T(x)\sqrt{D_2(x)} \bmod \mathfrak{p}$ is again a canonical basis. We further obtain the resultants $\rho_i(u)$ by applying the residue map $\bmod \mathfrak{p}$.
Now if $\mathfrak{A}_x \not\sim \mathfrak{O}_\Lambda$, the R_i are not all equal to 0 for every element of $\mathfrak{A}_x$, therefore the ρ_i are not all equal to 0 either, for almost all $\mathfrak{p}$ and finally $\mathfrak{A}_x \bmod \mathfrak{p} \not\sim \mathfrak{O}_{L_2}$ for almost all $\mathfrak{p}$, which is enough to prove the assertion as the residue ideal theorem states. □

Theorem 3.8. *If $\mathfrak{D} \not\sim \mathfrak{D}_c$ then $\mathfrak{D}(\mathfrak{p}\mathfrak{p}_\infty^{-1}) \not\sim 1$ for almost all $\mathfrak{p}$.*

PROOF. Let $\mathfrak{D}$ be a non-constant divisor of $\Lambda|L_1$. If $\mathfrak{p}_\infty$ is one of the ∞-divisors of $L_1|k$ and $\mathfrak{D}_c$ is the constant divisor of $\Lambda|L_1$ that corresponds to $\mathfrak{D}(\mathfrak{p}_\infty)$, then

$$\mathfrak{D}\left(\frac{\mathfrak{p}}{\mathfrak{p}_\infty}\right) = \frac{\mathfrak{D}(\mathfrak{p})}{\mathfrak{D}(\mathfrak{p}_\infty)} = \frac{\mathfrak{D}(\mathfrak{p})}{\mathfrak{D}_c(\mathfrak{p})} = \frac{\mathfrak{D}}{\mathfrak{D}_c}(\mathfrak{p}).$$

By assumption $\frac{\mathfrak{D}}{\mathfrak{D}_c} \not\sim 1$, so theorem 3.7 yields $\mathfrak{D}\left(\frac{\mathfrak{p}}{\mathfrak{p}_\infty}\right) \not\sim 1$ for almost all $\mathfrak{p}$. □

A correspondence maps the Jacobian of L_1 homomorphic to the Jacobian of L_2. These homomorphisms correspond one-to-one with the coarser divisor/ideal classes of $\Lambda|L_1$. Therefore the x-degree of the relevant $P(x) \in L_1[x]$ can be bound by the genus g_2 of L_2.

Definition. *We call* $\mathrm{Hom}(L_1, L_2)$ *the group of homomorphisms of the Jacobi group of* L_1 *to the Jacobi group of* L_2.

Lemma 3.1. *Let* L *be a finite algebraic extension of* K *with* q *as degree of inseparability, then we have*

$$L|L^q \text{ purely inseparable of degree } q, L^q|K \text{ separable},$$
$$L|K^{q^{-1}} \text{ separable}, K^{q^{-1}}|K \text{ purely inseparable of degree } q.$$

Here $L^q = \{a^q | a \in L\}$ *is the image of* L *under the frobenius map.*

Proof. See [**Has34**] theorem 1. □

As the next theorem shows we can always find a divisor in the double field that represents the composition of two such divisors. For simplicity we will omit the conorm maps.

Theorem 3.9. *Let* L_1, L_2, L_3 *be quadratic function fields over* k.
Given a divisor $\mathfrak{D}_{12}$ *of* $L_1L_2|L_1$ *and a divisor* $\mathfrak{D}_{23}$ *of* $L_2L_3|L_2$ *we can construct a divisor* $\mathfrak{D}_{13}$ *of* $L_1L_3|L_1$ *with*

$$\mathfrak{D}_{23}(\mathfrak{D}_{12}(\mathfrak{a})) = \mathfrak{D}_{13}(\mathfrak{a}) \text{ for all } \mathfrak{a} \in \mathrm{Div}(L_1|K)$$

Proof. Without loss of generality we only consider the case, where $\mathfrak{D}_{12} = \mathfrak{P}$, $\mathfrak{D}_{23} = \mathfrak{Q}$ are both non-constant prime divisors.
Let π be the residue class isomorphism

$$\pi : L_2 \xrightarrow{\mathfrak{P}} \overline{L}_2 = L_2^\pi$$

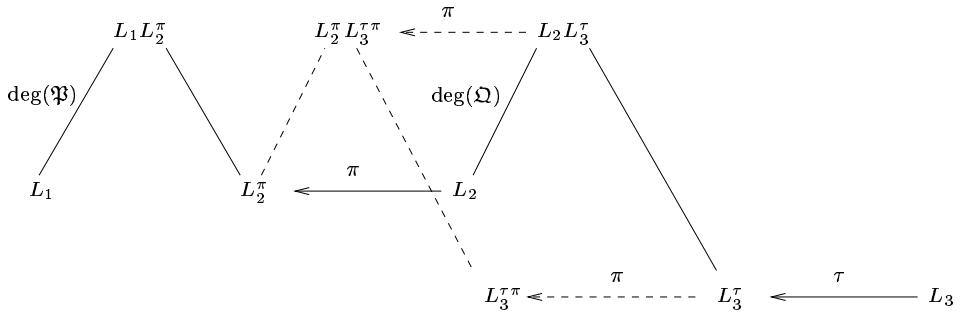
and

$$\tau : L_3 \xrightarrow{\mathfrak{Q}} \overline{L}_3 = L_3^\tau$$

and accordingly

$$\begin{aligned} \pi: \quad L_1L_2 &\xrightarrow{\mathfrak{P}} L_1L_2^\pi = L_1L_2 \mod \mathfrak{P}, \\ \tau: \quad L_2L_3 &\xrightarrow{\mathfrak{Q}} L_2L_3^\tau = L_2L_3 \mod \mathfrak{Q}. \end{aligned}$$

We obtain the following diagram:



For $\mathfrak{a} \in \mathrm{Div}(L_1|k)$ and $\mathfrak{b} \in \mathrm{Div}(L_2|k)$ we have

$$\mathfrak{P}(\mathfrak{a}) = \mathrm{N}_{L_1L_2^\pi|L_2^\pi}(\mathfrak{a})^{\pi^{-1}} \text{ and } \mathfrak{Q}(\mathfrak{b}) = \mathrm{N}_{L_2L_3^\tau|L_3^\tau}(\mathfrak{b})^{\tau^{-1}}.$$

We conclude

$$\mathfrak{Q}(\mathfrak{P}(\mathfrak{a})) = \mathrm{N}_{L_2L_3^\tau|L_3^\tau}(\mathrm{N}_{L_1L_2^\pi|L_2^\pi}(\mathfrak{a})^{\pi^{-1}})^{\tau^{-1}} \quad = \quad \mathrm{N}_{L_2^\pi L_3^{\tau\pi}|L_3^{\tau\pi}}(\mathrm{N}_{L_1L_2^\pi|L_2^\pi}(\mathfrak{a}))^{(\tau\pi)^{-1}}$$

We first consider the case that $\mathfrak{Q}$ is a divisor of degree 1. Then we have $L_3^\tau \leq L_2$, i.e. $L_3^{\tau\pi} \leq L_2^\pi$. As a consequence, $\tau\pi$ defines an isomorphism of L_3 to the subfield $L_3^{\tau\pi}$ of the finite algebraic extension $L_1L_2^\pi$ of L_1. So $\tau\pi$ defines a non-constant prime divisor $\mathfrak{R}$ from $L_1L_3|L_1$ with the residue class field

$$L_1^* = L_1L_3^{\tau\pi} \leq L_1L_2^\pi.$$

If $e = [L_1L_2^\pi : L_1^*]$ then the last equation is simplified to

$$\mathfrak{Q}(\mathfrak{P}(\mathfrak{a})) = \mathrm{N}_{L_2^\pi|L_3^{\tau\pi}}(\mathrm{N}_{L_1L_2^\pi|L_2^\pi}(\mathfrak{a}))^{\pi^{-1}\tau^{-1}} \tag{1}$$

$$= \mathrm{N}_{L_1L_2^\pi|L_3^{\tau\pi}}(\mathfrak{a})^{(\tau\pi)^{-1}} \tag{2}$$

$$= (\mathrm{N}_{L_1^*L_3^{\tau\pi}}(\mathfrak{a})^{(\tau\pi)^{-1}})^e = \mathfrak{R}(\mathfrak{a})^e = \mathfrak{R}^e(\mathfrak{a}) \tag{3}$$

So $\mathfrak{D}_{13} = \mathfrak{R}^e$ satisfies the condition.

To find a divisor $\mathfrak{D}_{13}$ in the general case we need to consider the composition of the two extensions of L_2^π, namely $L_2^\pi L_3^{\tau\pi}$ and $L_1L_2^\pi$. Note that we know $L_2^\pi L_3^{\tau\pi}$ only up to conjugacy (see theorem 1.1) and not as a subfield of an extension of L_2^π that also contains $L_1L_2^\pi$. For simplicity we will assume $L_2^\pi L_3^{\tau\pi}$ to be fixed and $L_1L_2^\pi$ be given only up to conjugacy. This is possible by throwing the isomorphisms to L_1. Therefore we consider $L_1L_2^\pi|L_2^\pi$ as an algebra and perform the constant field extension from L_2^π to $L_2^\pi L_3^{\tau\pi}$.

If the constant field extension is separable the associated algebra is semi simple i.e. it is the direct sum of fields $L^{(i)}$. Every $L^{(i)}$ results from the new constant field $L_2^\pi L_3^{\tau\pi}$ by composition with a field of the type $L_1L_2^\pi|L_2^\pi$. So it contains a subfield $L_1^{\sigma_i}$ that is isomorphic to L_1, such that $L^{(i)} = L_1^{\sigma_i}L_2^\pi L_3^{\tau\pi}$.

Corresponding to the decomposition into a direct sum the norm map is given by

$$\mathrm{N}_{L_1L_2^\pi|L_2^\pi}(\mathfrak{a}) \quad = \quad \prod_i \mathrm{N}_{L^{(i)}|L_2^\pi L_3^{\tau\pi}}(\mathfrak{a}^{\sigma_i}) \tag{4}$$

The isomorphism $\tau\pi$ maps L_3 to a subfield $L_3^{\tau\pi}$ of the finite algebraic extension $L^{(i)}$ of $L_1^{\sigma_i}$. Therefore it defines for every $L^{(i)}$ a non-constant prime divisor $\mathfrak{R}_i^{\sigma_i}$ of $L_1^{\sigma_i}L_3|L_1^{\sigma_i}$ with residue class field

$$L_{1i}^{*\,\sigma_i} = L_1^{\sigma_i}L_3^{\tau\pi} \leq L^{(i)}$$

and

$$e_i = [L^{(i)} : L_{1i}^{*\,\sigma_i}].$$

The latter corresponds to a non-constant prime divisor $\mathfrak{R}_i$ of $L_1L_3|L_1$ with the property

$$\mathfrak{R}_i(\mathfrak{a}) = \mathfrak{R}_i^{\sigma_i}(\mathfrak{a}^{\sigma_i})$$

¿From (1) and (4) we conclude that

$$\mathfrak{Q}(\mathfrak{P}(\mathfrak{a})) = \mathrm{N}_{L_2^\pi L_3^{\tau\pi}|L_3^{\tau\pi}}(\prod_i \mathrm{N}_{L^{(i)}|L_2^\pi L_3^{\tau\pi}}(\mathfrak{a}^{\sigma_i}))^{\pi^{-1}\tau^{-1}} = \prod_i \mathrm{N}_{L^{(i)}|L_3^{\tau\pi}}(\mathfrak{a}^{\sigma_i})^{(\tau\pi)^{-1}},$$

where

$$\mathrm{N}_{L^{(i)}|L_2^\pi L_3^{\tau\pi}}(\mathfrak{a}^{\sigma_i}))^{(\tau\pi)^{-1}} = (\mathrm{N}_{L_{1i}^{*\,\sigma_i}|L_3^{\tau\pi}}(\mathfrak{a}^{\sigma_i})^{(\tau\pi)^{-1}})^{e_i}$$

$$= \mathfrak{R}_i^{\sigma_i}(\mathfrak{a}^{\sigma_i})^{e_i} = \mathfrak{R}_i(\mathfrak{a})^{e_i} = \mathfrak{R}_i^{e_i}(\mathfrak{a}).$$

So $\mathfrak{D}_{13} = \prod_i \mathfrak{R}_i^{e_i}$ satisfies the condition.

What remains is the inseparable case. If both extensions $L_1L_2^\pi|L_2^\pi$ and $L_2^\pi L_3^{\tau\pi}|L_2^\pi$ are inseparable then by lemma 3.1 there exists a unique maximal purely inseparable subfield $(L_2^\pi)^q$, above which one of the extensions is separable. In this case we take

$(L_2^\pi)^q$ instead of L_2^π as constant field for the composition above. The norms of (4) are now

$$\mathrm{N}_{L_1L_2^\pi|(L_2^\pi)^q}(\mathfrak{a}) = \prod_i \mathrm{N}_{L^{(i)}|L_2^\pi L_3^{\tau\pi}}(\mathfrak{a}^{\sigma_i}).$$

Since for all $\mathfrak{b} \in \mathrm{Div}((L_2^\pi)^q|L_2^\pi)$ we have

$$\mathrm{N}_{(L_2^\pi)^q|L_2^\pi}(\mathfrak{b}) = \mathfrak{b}^q,$$

we obtain

$$\mathrm{N}_{L_1L_2^\pi|L_2^\pi}(\mathfrak{a}) = (\prod_i \mathrm{N}_{L^{(i)}|L_2^\pi L_3^{\tau\pi}}(\mathfrak{a}^{\sigma_i}))^q.$$

What has changed is only the additional exponent q and $\mathfrak{D}_{13} = \prod_i \mathfrak{R}_i^{e_i \cdot q}$ satisfies the conditions. □

We are now able to compute the composition of two separable prime divisors at least up to conjugacy. This means that we can compute the polynomial $Q(x) \in L_1[x]$ of the representation of $\mathfrak{R} = [R(x), V(x)]$. Note that $Q(x)$ need not be a prime polynomial. It is given by the defining polynomial of the extension $L_1L_3^\tau|L_3^{\tau\pi}$ and can be determined by the following resultant computation.

Let $L_1 = k(t, \sqrt{D_1(t)})$, $L_2 = k(v, \sqrt{D_2(v)})$, $L_3 = k(x, \sqrt{D_3(x)})$ and $\mathfrak{P}_{12} = [P(v), S(v)]$, $P, S \in L_1[v]$, $\mathfrak{P}_{23} = [Q(x), T(x)]$, $Q, T \in L_2[x]$. The extension $L_1L_2^\pi|L_2^\pi$ is given by the prime polynomial $P(v) \in L_1[v]$ and the extension of $L_1L_2^\pi|L_2^{p^i}$ by the prime polynomial $Q(x) \in L_2[x]$ (assuming that P and Q do not contain any squareroots). The resultant $\mathrm{res}(P, Q)$ factors into the defining polynomials of the fields $L^{(i)}$ of the semi simple algebra. In the next chapter we will give examples for this construction.

Definition. *If L_1 is isomorphic to L_2, where φ is a fixed isomorphism from L_1 to L_2, by attaching φ we can view the correspondences $\mathfrak{a} \mapsto \mathfrak{D}(\mathfrak{a})$ as a map from* $\mathrm{Div}(L_1)$ *to itself. We call the corresponding ring* $(\mathrm{Cor}(L), \cdot, \circ)$.

Remark. *Since every correspondence from L to L defines a homomorphism from the Jacobi group* $\mathrm{Jac}(L)$ *to itself, the restriction of the correspondence ring to the Jacobi group is* per definitionem *a subring of the ring of (group)endomorphisms of the Jacobi group to itself. Weil has proven in the second part of* [**Wei71**] *that there exist no other endomorphisms, so* $(\mathrm{End}(L), +, \cdot) \cong (\mathrm{Cor}(L)_{|\mathrm{Jac}(L)}, \cdot, \circ)$.
Note that we write the group of the endomorphism ring additively whereas the group of the correspondence ring is denoted multiplicatively due to the association to the ideal class group.

Up to now we have not shown how to compute the action of a correspondence given by a reduced prime divisor $\mathfrak{P} \in \mathrm{cDiv}^c(\Lambda|L)$. We will first investigate the case, when the constant field $k = \bar{k}$ is algebraically closed, i.e. all prime divisors of L_1 as well as of L_2 have degree 1.
Let $L_1^* = L_1(\alpha)$, where α is a root of the prime polynomial $P(x) \in L_1[x]$ with $\deg_x(P) \leq g_2$. Multiplying with the denominators we can consider $P(x)$ and $V(x)$ as polynomials in t and u, $u^2 = D_1(t)$ over $k(x)$. Observe that $V(x)^2 \equiv D_2(x) \bmod P(x, t, u)$, so $L_1^* = \overline{L}_2(t, u)$ and if $V(x) \notin k(t)[x]$ then $L_1^* = \overline{L}_2(t)$ since u can be expressed by x, t and $V(x) = \sqrt{D_2(x)}$. Since computing the norm from $\overline{L}_2(t, u)$ to $\overline{L}_2(t)$ if those are not already equal, is easy, namely $\mathrm{N}(A(x,t) + B(x,t)u) = A(x,t)^2 + B(x,t)^2 D(t)$, we will concentrate on the case where $L_1^* = L_2(t)$.
Let $P_t(X) = \sum_{i=0}^{m-1} p_i X^i + X^m$ be the normalised minimal polynomial of t. If we want to compute the norm of some prime polynomial $t - a$, $a \in k$, we have to

evaluate the determinant of the matrix

$$A = \begin{pmatrix} -a & 1 & & & \\ & -a & 1 & & \\ & & \ddots & \ddots & \\ & & & -a & 1 \\ -p_0 & -p_1 & \dots & -p_{m-1} & -a \end{pmatrix}$$

Developing it for the last row, we obtain

$$\mathrm{N}_{L_1^*|\overline{L}_2}(t-a) = \det(A) = (-1)^m P_t(a).$$

To compute the image of a reduced prime divisor $\mathfrak{p} = [t-a, b+\sqrt{D_1(t)}] \in \mathrm{Jac}(L_1)$ under the prime correspondence given by $\mathfrak{P} = [P(x,t), V(x,t)+\sqrt{D_2(x)}] \in \mathrm{Jac}^c(\Lambda|L_1)$, where P, U are polynomials in t, x and u (just multiply with the lcm of the denominators), $\deg_t(P) = m$ we first compute $(-1)^m P(x,a,b)$. As a consequence, the image $\mathfrak{P}(\mathfrak{p})$ lies above $(-1)^m P(x,a,b)$. In order to obtain the 'conjugacy class', we first compute the norm of $V(x,t,u)$ as $(-1)^m V(x,a,b)$.
In the case where k is not algebraically closed, to compute the image of $\mathfrak{p} = [Q(t), R(t)+\sqrt{D_1(t)}]$ under the correspondence given by $\mathfrak{P} = [P(x,t), V(x,t)+\sqrt{D_2(x)}] \in \mathrm{cDiv}^c(\Lambda|L_1)$, we first compute the norm of the polynomial $Q(t) \in k[t]$ with respect to t and then that of V with respect to t, after substituting $u = \sqrt{D_1(t)}$ by $R(t)$.
Alternatively we could extend k to some field k', where $Q(t)$ splits completely and then add the divisors resulting from the computations as in the algebraically closed case.

Example. *Let* $L_1 = \mathbb{F}_{17}(t, \sqrt{t^5+t^3+t})$ *and* $L_2 = \mathbb{F}_{17}(x, \sqrt{x^5+x^3+x})$ *then*

$$\begin{aligned} \mathfrak{P} \;=\; [\; & x^2 + 16\tfrac{13t^{16}+13t^{14}+13t^{12}+13t^{10}+4t^8+5t^6+13t^4+3t^2+4}{t^{15}+3t^{13}+6t^{11}+7t^9+6t^7+3t^5+t^3}x + \\ & 16\tfrac{(15t^{16}+9t^{14}+15t^{12}+4t^{10}+t^8+4t^6+15t^4+15+9t^2)}{t^{14}+3t^{12}+6t^{10}+7t^8+6t^6+3t^4+t^2}, \\ & 9\tfrac{(9t^{24}+5t^{22}+8t^{20}+14t^{18}+11t^{16}+t^{14}+14t^{10}+16t^8+6t^6+11t^4+16t^2+1)}{\sqrt{t^5+t^3+t}(1+t^2+t^4)t^4(1+3t^2+6t^4+7t^6+6t^8+3t^{10}+t^{12})}x + \\ & 16\tfrac{(13+8t^2+14t^4+6t^6+10t^8+12t^{10}+15t^{12}+7t^{14}+12t^{16}+13t^{18}+5t^{20}+9t^{22}+3t^{24})}{\sqrt{t^5+t^3+t}(1+t^2+t^4)t^3(1+3t^2+6t^4+7t^6+6t^8+3t^{10}+t^{12})}] \end{aligned}$$

defines the multiplication by [3] endomorphism on the Jacobi group (see chapter 3 section 2 for a construction method).
Let

$$\mathfrak{p} = [t-8, 6+\sqrt{t^5+t^3+t}],$$

then by substituting $t = 8$ *and* $\sqrt{t^5+t^3+t} = 6$ *we obtain*

$$\mathfrak{P}(\mathfrak{p}) = [x^2+6x+16, 12x+9].$$

Let $\mathfrak{p}$ *be a prime divisor of degree 2, for example*

$$\mathfrak{p} = [t^2+8t+6, 9t+15]$$

then $P(t) = t^2+8t+6$ *is a prime polynomial over* $\mathbb{F}_{17}$ *since* $\left(\frac{10}{17}\right) = -1$. *So we consider the extension field* $F_{17}(\sqrt{10})$. *Here we can write*

$$\mathfrak{p} = \mathfrak{p}_1 \cdot \mathfrak{p}_2 = [t-(-4+\sqrt{10}), 13+9\sqrt{10}] + [t-(-4-\sqrt{10}), 13+8\sqrt{10}]$$

Substituting t *and* $\sqrt{t^5+t^3+t}$ *we obtain*

$$\begin{aligned} \mathfrak{P}(\mathfrak{p}_1) &= [x^2+9\sqrt{10}+15+10x+16x\sqrt{10}, \sqrt{10}+8+16x\sqrt{10}+5x] \\ \mathfrak{P}(\mathfrak{p}_2) &= [x^2+8\sqrt{10}+15+10x+x\sqrt{10}, 16\sqrt{10}+8+x\sqrt{10}+5x] \end{aligned}$$

and consequently

$$\mathfrak{P}(\mathfrak{p}) = \mathfrak{P}(\mathfrak{p}_1) \cdot \mathfrak{P}(\mathfrak{p}_2) = [10+4x+3x^3+x^2+x^4, 9x^3+5x^2+16x+2].$$

CHAPTER 3

Applications of Deuring's Theory

In this chapter we show how to compute with algebraic correspondences. This includes addition and multiplication as well as multiples of coarser divisors. In sections 3 and 4 we introduce the Rosati antiautomorphism and cite a classification theorem for the endomorphism rings of general abelian varieties. The last section provides an algorithm that computes a representation of correspondences as matrices which is even faithful if the constant field has characteristic equal to 0.

1. Computation with correspondences

In chapter 2 we have seen that the action of an algebraic correspondence depends only on the coarser divisor class of the defining divisor of the double field. So if we have two correspondences from $\mathrm{Div}_0(L_1)$ to $\mathrm{Div}_0(L_2)$ given by divisors $\mathfrak{D}_1$ and $\mathfrak{D}_2$ of the double field Λ, then we can compute the addition of these two homomorphisms by adding the two divisors and then reducing them in the coarser divisor class group.
As in chapter 2 section 2 for $\mathfrak{D} \in \mathrm{Div}_0(\Lambda|L_1)$, let $\mathfrak{D}_x$ be the unique corresponding ideal in the ideal group G_Λ. Without loss of generality we only consider the multiplication of integral ideals.

Algorithm 1.1.

Input: *ideals* $\mathfrak{A}_x = [A_0, B_0 + \sqrt{D}]$, $\mathfrak{B}_x = [A_1, B_1 + \sqrt{D}]$
Output: *product* $\mathfrak{C}_x = \mathfrak{a} \cdot \mathfrak{b} = [R, S + T\sqrt{D}]$ *in canonical basis.*

begin
$T := A_0X + A_1Y + (B_0 + B_1)Z = gcd(A_0, A_1, B_0 + B_1)$;
$R := A_0A_1T^{-1}$;
$S := A_0B_1X + A_1B_0Y + (B_0B_1 + D)Z \bmod R$
end.

Observe that all computations are done in the polynomial ring $L_1[x]$. Although the number of field operations is bounded by $\frac{47}{2}g^2 + O(g)$ as in the finite constant field case (compare theorem 1.8), the degree of the polynomials in t occuring in the numerators and denominators increases rapidly in each step, which soon makes computations inefficient. Nevertheless, for small degree divisors $\mathfrak{A}_x$ and $\mathfrak{B}_x$ we can compute their product in acceptable time, even for cryptographically relevant parameters.

Example. *Let* $L_1 = \mathbb{C}(t, \sqrt{t^5 + t + 1})$, $L_2 = \mathbb{C}(x, \sqrt{x^5 + x + 1})$ *and* $\mathfrak{A}_x = [x - t, \sqrt{t^5 + t + 1}]$, $\mathfrak{B}_x = [x - t, \sqrt{t^5 + t + 1}]$ *then*

$$T = 1, R = (x - t)^2, S = \frac{-3t^5 + t + 2 + x + 5t^4x}{2\sqrt{t^5 + t + 1}}.$$

Consequently,

$$\mathfrak{C}_x = [(x - t)^2, \frac{-3t^5 + t + 2 + x + 5t^4x}{2\sqrt{t^5 + t + 1}}].$$

If we consider the constant field $k = GF(p)$ *with* $p = 2^{80} + 13$, *we obtain* $\mathfrak{C}_x = \mathfrak{A}_x \cdot \mathfrak{B}_x =$

$$[(x-t)^2, \frac{60446290980731458735309 5(1208925819614629174706186t^5+t+2+x+5t^4x)}{\sqrt{t^5+t+1}}].$$

Next we show how to reduce the product in the coarser ideal class group.

Algorithm 1.2.

Input: *primitive ideal* $\mathfrak{A}_x = [A(x), B(x) + \sqrt{D_2(x)}] \subseteq \mathfrak{O}_\Lambda$ *given in canonical basis* $\mathrm{lc}(A(x)) = 1$, $\deg_x(B(x)) < \deg_x(A(x))$ *and* $B^2(x) \equiv D_2(x) \bmod A(x)$ *in* $L_1[x]$

Output: *reduced ideal* $\mathfrak{B}_x = [U(x), V(x) + \sqrt{D_2(x)}]$ *in the same class as* $\mathfrak{A}_x$, $\mathrm{lc}(U(x)) = 1$, $\deg_x(V(x)) < \deg_x(U(x))$, $V^2(x) \equiv D_2(x) \bmod U(x)$, $\deg_x(U(x)) \leq g_2$.

begin
$U := A; V := B \bmod U;$
while $2\deg(U) > \deg(D)$ *do*
$U := (V^2 - D)/U;$
$U := \mathrm{lc}(U)^{-1} \cdot U;$
$V := -V \bmod U$
od;
cancel the constant prime ideals;
end.

An example for the above function will be given in the next section.

2. General multiples of endomorphisms

The easiest way to find non-trivial correspondences is to take the most obvious prime correspondence, namely the one that represents the identity map, and consider multiples of it. In this section we will describe how this can be done.
Let $L_1 = k(t, \sqrt{D(t)})$, $L_2 = k(x, \sqrt{D(x)})$ be two hyperelliptic function fields of genus $g \geq 1$. We are looking for the reduced divisor in $\mathrm{cDiv}^c(\Lambda|L_1)$ that is associated to the multiplication by $[m]$, $m \in \mathbb{N}$, $m > g$ in the endomorphism ring $\mathrm{End}(L_1)$ of L_1. Let $\mathfrak{P}_{id} \in \mathrm{cDiv}^c$ be the prime divisor that represents the identity endomorphism. Then $\mathfrak{P}_{id}$ is given by the polynomial pair $[x - t, \sqrt{D(t)}]$. So the corresponding ideal can be written as $\mathfrak{P}_x = [x - t, \sqrt{D(t)} + \sqrt{D(x)}]$. Lemma 1.7 of chapter 1 gives us a representation of a general ideal $\mathfrak{A}_x^m$ as an ideal in canonical basis, namely

$$\mathfrak{A}_x^m = [A(x)^m, B_m(x) + \sqrt{D(x)}],$$

where $B_m(x)$ is uniquely determined by the conditions

$$B_m^2(x) \equiv D(x) \bmod A^m, \quad \deg(B_m) < \deg(A^m), B_m \equiv B \bmod A$$

If $\mathfrak{P}_x = [P(x), U(x) + \sqrt{D(x)}]$ is a prime ideal, then we obtain

$$m \cdot \mathfrak{P} = [P^m(x), S_m(x) + \sqrt{D(x)}],$$

where S_m is the $P(x)$-adic expansion of $\sqrt{D(x)}$ in $L_1[x]$ up to m, i.e.

$$\sqrt{D(x)} = \sum_{i=0}^{\infty} a_i \cdot P(x)^i \text{ and } S_m(x) = \sum_{i=0}^{m-1} a_i \cdot P(x)^i$$

and $S_m^2 \equiv \sqrt{D(x)} \bmod P(x)^m$.
To compute S_m we can make use of the fact that $S_1(x) = a_0 = U(x)$ and put

$$a_m = \tfrac{1}{2} \cdot S_m(x)^{-1} \tfrac{D(x) - S_m^2}{P(x)^m} \bmod P(x).$$

If $D(x) = \sum_{k=0}^{2g+l} d_k P(x)^k$, $l = 1, 2$ (imaginary or real quadratic function field), we have the condition

$$\sum_{\substack{i+j=n \\ 0 \le i,j \le n}} a_i a_j = d_n$$

Together with $S_n(x) \equiv a_0 \bmod P(x)$ this leads us to the following formula to compute the a_n:

$$a_n = \frac{1}{2a_0}(d_n - \sum_{\substack{i+j=n \\ 0 < i,j < n}} a_i a_j) \tag{5}$$

where $d_n = 0$ for $n > \deg(D)$.
The case $P(x) = x - t$ is somewhat easier. Here we obtain for the $(x-t)$-adic expansion

$$\sqrt{D(x)} = \sum_{i=0}^{\infty} \frac{1}{i!} \sqrt{D(t)}^{(i)} (x-t)^i$$

where $\sqrt{D(t)}^{(i)}$ denotes the i-th derivative of $\sqrt{D(t)}$ for t.
Now we have to reduce the semi-reduced divisor $[(x-t)^m, S_m]$ using algorithm 1.2 until the degree of the first polynomial is less than or equal to g.
In [**Can94**] Cantor gives recursive formulas to compute the analogue of the division polynomials for hyperelliptic curves with the help of Padé approximation methods. Let $z = x - t$, $\sqrt{D(x)} = \sum_{i=0}^{\infty} s_i z^i$, $s_i \in k(t)$, then instead of reducing the semi-reduced divisor $[z^m, S_m(z)]$ he constructs $A_m(z)$, $B_m(z) \in k(t)[z]$, such that

$$A_m(z) - B_m(z) \sum_{i=0}^{\infty} s_i z^i = -z^m C_r(z)$$

where $C_m(z) = \sum_{i=0}^{\infty} c_i z^i$. Multiplication by $A_m(z) + B_m(z) \sum_{i=0}^{\infty} s_i z^i$ leads to

$$A_m(z)^2 - B_m(z)^2 D(z+t) = -z^m \underbrace{C_m(z)[A_m(z) + B_m(z) \sum_{i=0}^{\infty} s_i z^i]}_{E_m(z)}.$$

This means that $(A_m(z)/B_m(z))^2 \equiv D(x) \bmod z^m$ as well as $\bmod E_m(z)$.
The approximation can be chosen such that

$$\deg_x(A_m) = k_m = \left\lfloor \frac{m+g}{2} \right\rfloor \text{ and } \deg_x(B_m) = l_m = \left\lfloor \frac{m-g-1}{2} \right\rfloor$$

(observe that $\deg(D) = 2g+1$). Then $\deg_x(E_m) = g$ and to obtain a reduced representative we only need to reduce $S_m(x) \bmod E_m(z)$.

Example. *Let $\mathfrak{A}_x$ represent the multiplication by [3] endomorphism of the Jacobian of the function field $k(t, \sqrt{t^5+t+1})$, then $\mathfrak{A}_x = [(x-t)^3, V(x)]$, where $V(x) =$*

$$\frac{(8 + 4x + 36t^5 + 30t^4x^2 - 36t^5x + 40t^3x^2 + 15t^8x^2 - 10t^9x + 12t - x^2 + 3t^2 + 22t^6 + 3t^10 + 6tx - 60t^4x)}{8(t^5+t+1)^{(3/2)}}$$

This divisor can be reduced to

$$[x^2 + \tfrac{F(t)}{64(t^5+t+1)^3}x + \tfrac{G(t)}{64(t^5+t+1)^3}, \tfrac{H(t)}{512\sqrt{t^5+5+1^9}}x + \tfrac{I(t)}{512\sqrt{t^5+5+1^9}}],$$

where $F, G, H, I \in \mathbb{C}[t]$ with $\deg(F) = 17$, $\deg(G) = 16$, $\deg(H) = 25$, $\deg(I) = 24$.

3. The Rosati antiautomorphism

In the last chapter we have seen that homomorphisms from $\mathrm{Jac}(L_1|k)$ to $\mathrm{Jac}(L_2|k)$ correspond one to one to the coarser divisor classes of the double field $\Lambda = L_1L_2$ or if we are talking about imaginary quadratic function fields, they correspond to the ideal classes of the maximal order $\mathfrak{O}_{\Lambda|L_1} = \{A(x) + B(x)\sqrt{D_2(x)} \ : \ A(x), B(x) \in L_1[x]\}$. Since constant divisors/ideals do not play a role in the coarser divisor/ideal class group, instead of $\mathfrak{O}_{\Lambda|L_1}$ we can also consider the ideal classes of the larger ring $\mathcal{R}$ of all elements of Λ, the principal divisors of which only contain constant divisors in the denominator, i.e.

$$\mathcal{R} = \{\alpha \in \Lambda \ : \ v_{\mathfrak{P}}(\alpha) \geq 0 \text{ for all non-constant prime divisors } \mathfrak{P} \ \}.$$

Lemma 3.1. *Let $\mathcal{R}$ be defined as above, then $\mathcal{R}$ is the ring compositum of L_1 and L_2, i.e.*

$$\mathcal{R} = [L_1, L_2] = \{\sum_i u_i v_i\}, \text{ where } u_i \in L_1,\ v_i \in L_2.$$

Proof. Note that $[L_1, L_2] \supseteq \mathfrak{O}_{\Lambda|L_1} = [\mathfrak{O}_{L_2|k}, L_1]$. The denominators of the elements of $[L_1, L_2]$ are constant *per definitionem* (just write them with a common rational denominator). Moreover, every constant prime divisor can occur in the denominator of some element of $[L_1, L_2]$, namely in the denominator of the elements of L_2. So $[L_1, L_2]$ is exactly the ring of all elements of L_1L_2 that are integral for every non-constant prime divisor of $\Lambda|L_1$. □

Obviously the ring $\mathcal{R}$ is symmetric in L_1 and L_2. Therefore swapping L_1 and L_2 leads to an involutoric map from $\mathrm{Hom}(L_1, L_2)$ to $\mathrm{Hom}(L_2, L_1)$ which we denote by $\varphi \mapsto \varphi^*$.
Now if we think of isomorphic L_1 and L_2, we obtain the following result

Theorem 3.1. *The map $\varphi \mapsto \varphi^*$ from $\mathrm{End}(L)$ to itself is an antiautomorphism , i.e. for $\varphi, \psi \in \mathrm{End}(L)$ we have*

$$(\varphi\psi)^* = \psi^*\varphi^*.$$

The proof is straightforward and can be found in [**Deu37**].
We now give explicit examples for the action of the above Rosati involution .

Example. *First we consider the multiplication by $[m]$ endomorphisms. As we have already seen in the last section they are given by ideals of the form*

$$\mathfrak{D}_x = [(x-t)^m, S_m + \sqrt{D(x)}]$$

where S_m is the $(x-t)$-adic expansion of $\sqrt{D(x)}$ in $L_1[x]$. More precisely, we write

$$S_m = \sum_{i=0}^{m} a_i(x-t)^i, \ a_i \in L_1$$

where the denominator of a_i is equal to $D(t)^{2i-\frac{3}{2}}$ for $i > 0$. Let $\frac{1}{D(t)^{m-\frac{3}{2}}}\tilde{S}_m = S_m$ then for $m > 1$, $\tilde{S}_m^2 \equiv D(t)^{2m-3}D(x) = D(t)^{2m-4}D(t)D(x) \bmod (x-t)$. Considering this congruence in $L_2[t]$ now, we conclude

$$D(t) \equiv \frac{\tilde{S}_m^2}{D(x)} \cdot D(t)^{-2(m-2)} \bmod (-t+x)^m \text{ in } L_2[t].$$

If we choose for example $D(t) = t^5 + 1$ and $m = 3$, then we have

$$\mathfrak{P}_x = [(x-t)^3, \sqrt{t^5+1} + \tfrac{5t^4}{2\sqrt{t^5+1}}(x-t) + \tfrac{5t^3(8+3t^5)}{8\sqrt{t^5+1}^3}(x-t)^2].$$

Thus

$$S_3 = \tfrac{3t^{10}+36t^5+8-10t^9x-60t^4x+40t^3x^2+15t^8x^2}{8(t^5+1)^{\frac{3}{2}}},$$

$$\tilde{S}_3 = \tfrac{1}{8}(3t^{10} + 36t^5 + 8 - 10t^9x - 60t^4x + 40t^3x^2 + 15t^8x^2).$$

With the extended Euclidean algorithm we compute the inverse of $D(t) \bmod (x-t)^3$

$$D(t)^{-1} = \tfrac{21x^{10}-35x^9t+15x^8t^2-3x^5+15x^4t-10x^3t^2+1}{(x^5+1)^3} \text{ in } L_2[t]$$

and

$$\tfrac{\tilde{S}_3(D(t))^{-1}}{\sqrt{x^5+1}} = \tfrac{3x^{10}+36x^5+8-10x^9t-60x^4t+40x^3t^2+15x^8t^2}{8\sqrt{x^5+1}^3},$$

so

$$\mathfrak{P}_t^* = [(-t+x)^3, \sqrt{x^5+1} + \tfrac{5x^4}{2\sqrt{x^5+1}}(-t+x) + \tfrac{5x^3(8+3x^5)}{8\sqrt{x^5+1}^3}(-t+x)^2 + \sqrt{D(t)}]$$

and the rosati involution acts as the identity map.

Example. *If we choose* $L_1 = k(t, \sqrt{t^5+5})$ *and* $L_2 = k(x, \sqrt{x^5+x})$, $i \in k$ *with* $i^2 = -1$, *we have the prime correspondence representing multiplication by* $[i]$, *where* $[i^2] = [-1]$ *in the endomorphism ring, given by*

$$\mathfrak{P}_x = [x+t, i\sqrt{t^5+t}]$$

since $x^5 + x \equiv -t^5 - t = (i\sqrt{t^5+t})^2 \bmod (x+t)$ *in* $L_1[x]$.
In $L_2[t]$ *we have* $t^5 + t \equiv (\frac{1}{i}\sqrt{x^5-x})^2 \bmod (t+x)$, *so*

$$\mathfrak{P}_t^* = [t+x, -i\sqrt{x^5+x}]$$

and the Rosati involution acts as the complex conjugation.

In the next section we will see that these two examples are no coincidences.

4. The endomorphism ring of hyperelliptic curves

In this section we will collect some general facts concerning the structure of endomorphism rings of abelian varieties, which can be applied to the Jacobians of hyperelliptic curves. For this reason we have to assume some basic definitions of algebraic geometry to be known, that can be found in every standard book on the topic such as [**Har77**], [**Mum70**] or [**Gor97**]. For our purposes the book of Mumford is especially suited, since he derives the theory over arbitrary algebraically closed fields k.

For the rest of this chapter, let k *be an arbitrary algebraically closed field.*

Definition. *An abelian variety* A *is a complete algebraic variety (irreducible) over some arbitrary algebraically closed field* k *with a group law* $+ : A \times A \to A$ *such that* $+$ *and the inverse map* $-$ *are both morphisms of varieties.*
If a subvariety S *of an abelian variety* A *is a subgroup, then it has a natural structure of an abelian variety and is called an abelian subvariety of* A. *An abelian variety is called simple if it has no abelian subvarieties other than* $\{0\}$ *and itself.*

Definition. *For two abelian varieties* A *and* B *of the same dimension, i.e. the associated function fields of which have the same transcendence degree, there exists a (group) homomorphism of* A *onto* B *if and only if there exists a homomorphism of* B *onto* A, *in which case* A *and* B *are called isogenous. Any such homomorphism is called isogeny.*

Definition. *For an abelian variety* A *let* $\mathrm{End}(A)$ *denote its endomorphism ring. We define* $\mathrm{End}_0(A) = \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(A)$ *to be the endomorphism algebra.*

Lemma 4.1. *If* A *and* A' *are isogenous abelian varieties then* $\mathrm{End}_0(A) \simeq \mathrm{End}_0(A')$.

Theorem 4.1. *Any abelian variety A is isogenous to a product $A_1^{n_1} \times \cdots \times A_k^{n_k}$, where the A_i are simple and not isogeneous to each other. The isogeny type of the A_i and the integers n_i are uniquely determined. Moreover, if $R_i = \mathrm{End}_0(A_i)$ then*

$$\mathrm{End}_0(A) \simeq \mathrm{Mat}_{n_1}(R_1) \oplus \cdots \oplus \mathrm{Mat}_{n_k}(R_k)$$

So we only have to look at simple abelian varieties.

Theorem 4.2. *Let A be a simple abelian variety. Let K be the center of $\mathrm{End}_0(A)$ and K_0 the subfield of elements of K fixed by the Rosati involution. Then $\mathrm{End}_0(A)$ is of one of the following types:*

a) *$\mathrm{End}_0(A) = K = K_0$ is a totally real algebraic number field, and the Rosati involution acts as the identity map.*
b) *$K = K_0$ is a totally real algebraic number field, and $\mathrm{End}_0(A)$ is a division quaternion algebra over K such that every simple component of $\mathrm{End}_0(A) \otimes_{\mathbb{Q}} \mathbb{R}$ is isomorphic to $\mathrm{Mat}_2(\mathbb{R})$; there is an element $\beta \in \mathrm{End}_0(A)$ such that $\beta^T = -\beta$, and $\beta^2 \in K$ is totally negative; moreover, the Rosati involution is given by $\alpha^\iota = \beta^{-1}\alpha^T\beta$.*
c) *$K = K_0$ is a totally real algebraic number field, and $\mathrm{End}_0(A)$ is a division quaternion algebra over K such that every simple component of $\mathrm{End}_0(A) \otimes_{\mathbb{Q}} \mathbb{R}$ is isomorphic to the Hamiltonian quaternion algebra $\mathbb{H}$ over $\mathbb{R}$ and $\alpha^\iota = \alpha^T$.*
d) *K_0 is a totally real algebraic number field, and K is a totally imaginary quadratic extension of K_0. $\mathrm{End}_0(A)$ is a division algebra with center K, and the Rosati involution acts as complex conjugation.*

Thus we have described all possible endomorphism rings.
For our purposes it is sufficient to know that the Jacobian of a hyperelliptic curve of genus g is an abelian variety of dimension g and therefore its endomorphism ring has one of the structures listed above.

5. Representation of correspondences by matrices

A very useful tool that facilitates the computation with correspondences are matrices of differentials. They form a group under addition which can be considered as the image of a homomorphism from the multiplicative subgroup of separable divisors of the double field. Moreover, if we consider correspondences from $\mathrm{Div}(L_1)$ to itself, this map can be extended to a ring homomorphism from $\mathrm{End}(L_1)$ to the ring of matrices over $\bar{k}$. In this section we give some basic facts on these matrices and finally show how to compute them. In the special case of genus 2 function fields an explicit description can be found in [**Ben99**].

Definition. *Let $L_1 = k(t,u)$, $u^2 = D_1(t)$, $L_2 = k(x,y)$, $y^2 = D_2(x)$ be two quadratic function fields. Let $\mathfrak{P}$ be a separable non-constant prime divisor of $\Lambda|L_1$, i.e. $L_1^*|\overline{L}_2$ is separable. If $\mathcal{D}_{L_2}$ is a basis of the integral differentials of L_2, Deuring shows, that $\mathrm{Tr}_{L_1^*|L_1}(\mathcal{D}_{L_2}^\pi)$ is a system of integral differentials of L_1 (note that $\mathcal{D}_{L_2}^\pi$ is the image of $\mathcal{D}_{L_2}$ under the residue class map π). Thus we can define $M_{\mathfrak{P}}$ to be the $g_2 \times g_1$ matrix given by the following equation*

$$\mathrm{Tr}_{L_1^*|L_1}(\mathcal{D}_{L_2}^\pi) \quad = \quad M_{\mathfrak{P}}(\mathcal{D}_{L_1}) \tag{6}$$

where $\mathcal{D}_{L_1}$ is a basis of the integral differentials of L_1
If $\mathfrak{P}$ is constant we define $M_{\mathfrak{P}}$ to be the 0-matrix. For $\mathfrak{D} = \prod \mathfrak{P}_i^{e_i}$ we put $M(\mathfrak{D}) = \sum e_i M(\mathfrak{P}_i)$

The importance of this kind of matrices is exhibited by the following theorem.

Theorem 5.1. *If $\mathfrak{D} \sim \mathfrak{D}_c$ then $M(\mathfrak{D}) = 0$.*

In addition, for the composition of correspondences we have

Theorem 5.2. $M_{\mathfrak{P}_{12}\mathfrak{P}_{23}} = M_{\mathfrak{P}_{23}} \circ M_{\mathfrak{P}_{12}}$.

The proofs can be found in [**Deu37**].
If we consider the special case of correspondences from $\mathrm{Div}(L)$ to itself, we obtain that the map $\mathfrak{D} \mapsto M_{\mathfrak{P}}$ is a ring homomorphism from $\mathrm{End}(L)$ to a ring of matrices over k. If $\mathrm{char}(k) = 0$ this representation is faithful (in case $\mathrm{char}(k) = p$ it cannot be faithful, since the endomorphism ring over $\bar{k}$ has characteristic 0 whereas the ring of matrices has characteristic p).
We will now describe an algorithm to compute the matrix of differentials, given a separable non-constant prime divisor $\mathfrak{P}$.
As usual let $L_1 = k(t,u)$, $u^2 = D_1(t)$, $L_2 = k(x,y)$, $y^2 = D_2(x)$ be two quadratic function fields and $\mathfrak{P}$ be a non-constant prime divisor given by

$$\begin{array}{lllllllll} P(x) & = & x^m & + & A_{m-1}x^{m-1} & + & \ldots & + & A_0 \quad A_i \in L_1, \\ V(x) & = & & & B_{m-1}x^{m-1} & + & \ldots & + & B_0 \quad B_i \in L_1 \end{array}$$

with $V(x)^2 \equiv D_2(x) \bmod P(x)$.
For simplicity as from now we will omit the π's and do not differentiate between L_2 and its image $\overline{L}_2$ under the residue class map.
We assume $x_0, \ldots, x_{m-1}$ to be the zeros of $P(x)$ and $y_0 = V(x_0), \ldots, y_{m-1} = V(x_{m-1})$ the corresponding squareroots of $D_2(x)$.
An integral basis for the differentials of L_1 is given by $t^i \frac{dt}{u}$, $i = 0, \ldots, g_1 - 1$ and for L_2 by $x^i \frac{dx}{y}$, $i = 0, \ldots, g_2 - 1$. So (6) can be written as

$$\begin{pmatrix} \sum_{k=0}^{m-1} \frac{dx_k}{y_k} \\ \vdots \\ \sum_{k=0}^{m-1} x_k^{g_2-1} \frac{dx_k}{y_k} \end{pmatrix} = M_{\mathfrak{P}} \begin{pmatrix} \frac{dt}{u} \\ \vdots \\ t^{g_1} \frac{dt}{u} \end{pmatrix}.$$

Division by dt leads us to the equation system

$$\begin{array}{lllllllll} \sum_{k=0}^{m-1} \frac{1}{y_k} \frac{dx_k}{dt} & = & \frac{1}{u} & (a_{00} & + & a_{01}t & + & \ldots & + \quad a_{0g_1-1}t^{g_1-1}) \\ \vdots & & & & & \vdots & & & \\ \sum_{k=0}^{m-1} \frac{x_k^{g_2-1}}{y_k} \frac{dx_k}{dt} & = & \frac{1}{u} & (a_{g_2-1,0} & + & a_{g_2-1,1}t & + & \ldots & + \quad a_{g_2-1,g_1-1}t^{g_1-1}). \end{array}$$

In a first step we write:

$$x^i \frac{dx}{dt} = I_0^{(i)} + I_1^{(i)}x + I_2^{(i)}x^2 + \cdots + I_{m-1}^{(i)}x^{m-1}, \quad i = 0, \ldots, g_2 - 1.$$

To achieve this, observe that $\frac{dx}{dt} = -\frac{P_t}{P_x}$ for some x with $P(x) = 0$, since

$$P(x) = 0 \Rightarrow \frac{dP}{dx} + \frac{dP}{dt} = 0 \Rightarrow \frac{dP}{dx} = -\frac{dP}{dt}.$$

Since $P(x)$ is a prime polynomial in $L_1[x]$, we can compute inverses by the extended Euclidean algorithm in $L_1[x]$.
Similarly we can write

$$\frac{1}{y} = \frac{1}{V(x)} = J_0 + J_1 x + \cdots + J_{m-1}x^{m-1}.$$

Now let

$$\frac{1}{y} \cdot x^i \frac{dx}{dt} = U_0^{(i)} + U_1^{(i)}x + \cdots + U_{m-1}^{(i)}x^{m-1},$$

then

$$\sum_{k=0}^{m-1} \frac{x_k^i}{y_k} \frac{dx_k}{dt} = mU_0^{(i)} + U_1^{(i)} \sum_{j=0}^{m-1} x_j + \cdots + U_{m-1}^{(i)} \sum_{j=0}^{m-1} x_j^{m-1}$$

for $i = 0, \ldots, g_2 - 1$. This polynomial in $x_0, \ldots, x_{m-1}$ is obviously symmetric in the x_k, so we can develop it into its elementary symmetric functions which are exactly the coefficients of $P(x)$, namely $A_0, \ldots, A_{m-1}$.
To be precise, we only need the elementary symmetric functions for sums of the form $\sum_{j=0}^{m-1} x_j^k$ for $k = 0, \ldots, m-1$. Finally we obtain

$$\sum_{k=0}^{m-1} \frac{x_k^j}{y_k} \frac{dx_k}{dt} = K^{(j)}$$

where $K^{(j)}$ is an integral polynomial in t of degree $\leq g_1 - 1$ and the computation of the matrix $M_{\mathfrak{P}}$ can easily be read off the above equation system.
We summarise the above in the following

Algorithm 5.1.

Input: *Defining squarefree polynomials* $D_1(t) \in k[t]$ *and* $D_2(x) \in k[x]$, *s.t.* $L_1 = k(t, \sqrt{D_1(t)})$, $L_2 = k(x, \sqrt{D_2(x)})$, *reduced separable prime divisor* $\mathfrak{P} = [P(x), V(x)]$, $P, V \in L_1[x]$.
Output: *The* $g_1 \times g_2$ *matrix of differentials* $M_{\mathfrak{P}}$.

begin
$g_1 := genus(L_1)$;
$g_2 := genus(L_2)$;
$m := deg_x(P)$;
for $i = 0$ *to* $g_2 - 1$
  compute $K_i = mU_0^i + U_1^i(\sum_{j=0}^{m-1} x_j) + \cdots + U_{m-1}^i(\sum_{j=0}^{m-1} x_j^{m-1})$
  write $\sum_{j=0}^{m-1} x_j^k$ *for* $k = 0..m-1$ *in terms of coefficients of* $P(x)$
od;
for $i = 0$ *to* $g_1 - 1$
  for j *from* 0 *to* $g_2 - 1$ *do*
   $M_{\mathfrak{P}_{ij}} := coeff(K_i, t, j)$;
  od;
od;
end.

CHAPTER 4

Hyperelliptic Function Fields with Special Correspondences

In this chapter we show how to construct isogenies and endomorphisms of hyperelliptic curves by means of correspondences. Our methods rely on Deuring's main theorem. The idea all approaches have in common is to find non-constant prime polynomials $P(x) \in L_1[x]$ such that $D_2(x)$ is a square modulo $P(x)$. Here $P(x)$ must be a polynomial in x of degree $\leq g_2$. As we know from the last chapter it then represents a reduced (prime) divisor in the coarser divisor class group and defines a homomorphism from the Jacobian of the curve given by $u^2 = D_1(t)$ to the Jacobian of the curve given by $y^2 = D_2(x)$.
As we are only interested in elliptic and hyperelliptic curves, D_1 and D_2 have to be squarefree.

1. Correspondences based on factors of $D_2(x) - D_1(t)$

The first method we want to describe is to look for factors of $D_2(x) - D_1(t)$. Suppose $L_1 = k(t,u)$, $u^2 = D_1(t)$, $L_2 = k(x,y)$, $y^2 = D_2(x)$ are hyperelliptic function fields and $\Lambda = L_1(x,y)$ is their double field. If $D_1(t) - D_2(x)$ has a factor $P(x) \in k[t,x]$ where $\deg_x(P) \leq g_2$, then $D_2(x)$ is a square in $L_1[x]$ modulo $P(x)$ since $(\pm\sqrt{D(t)})^2 \equiv D_2(x) \bmod P(x)$. So the reduced coarser ideal class of the coarser ideal class group of the double field looks like this:

$$\mathfrak{P}_x = [P(x), \pm\sqrt{D(t)} + \sqrt{D(x)}].$$

A lot of work has already been done on the factorisation of bivariate polynomials of the form $D_2(x) - D_1(t)$.
We first have a look at the case where $D_1 = D_2$.
Here we will apply a theorem of Fried [**Fri70**] about irreducibility of certain bivariate polynomials to find non-trivial endomorphisms.
Let $L_1 = k(t,u)$ with $u^2 = D(t)$ and $L_2 = k(x,y)$, $y^2 = D(x)$ be hyperelliptic genus g function fields. We want to find a non-constant prime polynomial $P \in L_1[x]$ with degree $\deg_x(P) \leq g$ such that $D(x)$ is a square mod $P(x)$. The most obvious $P(x)$ that satisfies this condition is $P(x) = x - t$, since $P(x) \mid D(x) - D(t)$ and therefore $(\sqrt{D(t)})^2 \equiv D(x) \bmod P(x)$. The associated endomorphism is nothing else but the identity map as we have already seen in the last chapter. If, however, $\frac{D(x)-D(t)}{x-t}$ splits, then a prime factor of degree less than g may lead to a nontrivial endomorphism.
To study factorisations of the above mentioned bivariate polynomials, we need to define so-called *normalised Chebyshev polynomials.*

Definition. *Let k be a field with* $\mathrm{char}(k) = 0$*, then we define the normalised Chebyshev polynomials $T_i(x) \in k[x]$ by the following recursion*

$$T_0(x) = 2,\ T_1(x) = x,\ T_{n+1}(x) = xT_n(x) - T_{n-1}(x).$$

They are related to the classical Chebyshev polynomials $C_n(x) = cos(narccos(x))$ *by* $T_n(2x) = 2C_n(x)$ *and satisfy:*

$$T_n \circ T_m = T_{nm} = T_{mn} = T_m \circ T_n.$$

They can also be defined iteratively by

$$T_n(x) = \left(\frac{x}{2} + \sqrt{\left(\frac{x}{2}\right)^2 - 1}\right)^n + \left(\frac{x}{2} - \sqrt{\left(\frac{x}{2}\right)^2 - 1}\right)^n.$$

Fried proves the following theorem in [**Fri70**].

Theorem 1.1. *Let* $k = \bar{k}$ *be a field with* $\mathrm{char}(k) = 0$ *or* $\mathrm{char}(k) > \deg(D) \geq 1$, *then* $\frac{D(x)-D(t)}{x-t}$ *is reducible in* k *if and only if one of the following cases holds*

1. $D(x) = E(F(x))$, *where* $E, F \in k[x]$, $\deg(E), \deg(F) > 1$ *or*
2. $D(x) = U_1 \circ x^n \circ U_2$, $U_1, U_2 \in k[x]$, $\deg(U_1) = \deg(U_2) = 1$.
3. $D(x) = U_1 \circ T_n \circ U_2$, $U_1, U_2 \in k[x]$, $\deg(U_1) = \deg(U_2) = 1$.

We will now study the three cases above with respect to algebraic correspondences. In the first case, since $F(x) - F(t) = (x-t)\tilde{F}(x,t)$ for some non-constant bivariate polynomial $\tilde{F} \in k[x,t]$, it is another factor of $D(x) - D(t)$ and we obtain the factorisation

$$\frac{D(x)-D(t)}{x-t} = (F(x) - F(t)) \cdot G(x,t) = (x-t)P(x,t)\tilde{G}(x,t)$$

for some prime polynomial P and $G, \tilde{G} \in k[x,t]$.
Assume $\deg(P) \leq g$, then the associated correspondence is given by the prime ideal

$$\mathfrak{P}_x = [P(x,t), \sqrt{D(t)} + \sqrt{D(x)}].$$

Example. *Let* $L = GF(19)(t,u)$,

$$\begin{aligned} u^2 = D(t) &= t^9 + 18t^8 + 18t^7 + 16t^6 + 7t^5 + t^4 + 9t^3 + 9t^2 + 13t + 3 \\ &= E(F(t)) \end{aligned}$$

where $E(t) = t^3 + 6t^2 + 4t + 2$ *and* $F(t) = t^3 + 6t^2 + 8t$.
In this case we have

$$\begin{aligned} D(x) - D(t) = {} & (x^6 + 12x^5 + 14x^4 + (t^3 + 6t^2 + 8t + 7)x^3 + (6t^3 + 17t^2 + 10t + 5)x^2 + \\ & (8t^3 + 10t^2 + 7t + 10)x + t^6 + 12t^5 + 14t^4 + 7t^3 + 5t^2 + 10t + 4) \times \\ & (x^2 + (t+6)x + t^2 + 6t + 8)(x - t). \end{aligned}$$

The function field $L = \mathbb{F}_{19}(t, \sqrt{D(t)})$ *has a degree 3 subfield* $\mathbb{F}_{19}(\alpha, \sqrt{E(\alpha)})$ *where* $\alpha = F(t)$.
A correspondence is given by the prime ideal

$$\mathfrak{P}_x = [x^2 + (t+6)x + t^2 + 6t + 8, \sqrt{D(t)} + \sqrt{D(x)}].$$

Its differential matrix is given by

$$M_{\mathfrak{P}} = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

In the second case, D is called a cyclic polynomial. Let $S_1(x) = ax + b$, $S_2(x) = cx + d$, then

$$D(x) - D(t) = c(ax+b)^n - c(at+b)^n = c(S_1(x)^n - S_1(t)^n) = c\prod_{i=0}^{n-1}(S_1(x) - \xi_n^i S_1(t))$$

where ξ_n is an n-th root of unity.
The factors of this bivariate polynomial lead to the following endomorphisms

$$\mathfrak{P}_x = [x - \xi_n^i t, \sqrt{D(t)} + \sqrt{D(x)}].$$

They are in fact even automorphisms and can also be easily read off the defining equation of L.

The third case is the most interesting one. Since we can write T_n as a composition of $T_k \circ T_l$ if $n = k \cdot l$ is not a prime, we only consider T_p for primes p.
First we consider the elliptic case, namely $p = 3$. We obtain

$$C : y^2 = T_3(x) = x^3 - 3x.$$

This curve has j-invariant $j = 1728$ and its endomorphism ring is isomorphic to $\mathbb{Z} + 1 \cdot O_K$ where O_K is the maximal order of $K = \mathbb{Q}(i)$.
Then we obtain

$$T_3(x) - T_3(t) = (x - t)(x^2 + tx + t^2 - 3).$$

Reducing the non constant prime ideal given by $\mathfrak{P}_x = [x^2 + tx + t^2 - 3, \sqrt{D(t)} + \sqrt{D(x)}]$ leads to the multiplication by $[-1]$ endomorphism

$$\mathfrak{Q} = [x - t, -\sqrt{D(t)} + \sqrt{D(x)}],$$

which is not very surprising.
The more interesting cases are $p \geq 5$. Here we have

$$T_p(x) - T_p(t) = (x - t) \prod_{k=1}^{(p-1)/2} (x^2 - \theta_k xt + t^2 + 4 - \theta_k^2)$$

where $\theta_k = \xi_p^k + \xi_p^{-k}$ and ξ_p is a primitive p-th root of unity.
So there exists an endomorphism that is given by the reduced prime ideal of the double field, namely

$$\mathfrak{P}_x = [x^2 - \theta_1 xt + t^2 + 4 - \theta_1^2, \sqrt{D(t)} + \sqrt{D(x)}]$$

Tautz, Top and Verberkmoes [**TTV91**] proved this endomorphism to be a multiplication by $[2cos(\frac{2\pi}{p})]$. They considered $L = k(t, \sqrt{T_p(t) + a})$ to be the fixed subfield of the function field $k(t, \sqrt{t(t^{2n} + ax^n + 1)})$ when applying the involution σ given by

$$\sigma : (t, u) \mapsto \left(\tfrac{1}{t}, \tfrac{u}{t^{n+1}}\right).$$

Remark. *The Chebyshev polynomials T_p defined above are indeed permutation polynomials, i.e. the map $\mathbb{F}_l \to \mathbb{F}_l$ with $x \mapsto T_p(x)$ is bijective for certain primes l. More information on this kind of polynomials can be found in* [**Shp99**].

Now we consider the factorisations of $D_2(x) - D_1(t)$ where $D_1 \neq D_2$ more generally, i.e. we look for correspondences (isogenies) from the Jacobian of the curve defined by D_1 to the Jacobian of the curve defined by D_2.
It is obvious that if

$$D_1(t) = E(F(t)), D_2(x) = E(G(x))$$

for some polynomials E, F, G, then $D_2(x) - D_1(t)$ is divisible by $G(x) - F(t)$.

Example. *Let $E(X) = X^3 + 7X^2 + 4X + 2$, $F(X) = X^2 + X$, $G(X) = X^2 + 3X$. Then*

$$\begin{array}{rcccl} D_1(t) & = & E(F(t)) & = & 2 + t^6 + 3t^5 + 10t^4 + 15t^3 + 11t^2 + 4t, \\ D_2(x) & = & E(G(x)) & = & 2 + x^6 + 9x^5 + 34x^4 + 69x^3 + 67x^2 + 12x \end{array}$$

and $P(x) = G(x) - F(t) = x^2 + 3x - t^2 - t$ *divides* $D_2(x) - D_1(t)$. *The correpondence is given by*

$$\mathfrak{P}_x = [x^2 + 3x - t^2 - t, \sqrt{D_1(t)} + \sqrt{D_2(x)}].$$

Computing its differential matrix and the dual yields

$$\begin{pmatrix} 0 & 0 \\ 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 0 & 0 \\ 3 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 6 & 4 \end{pmatrix}$$

So applying some basis change, we obtain the representation

$$M_{\mathfrak{P}\mathfrak{P}^*} = \begin{pmatrix} 0 & 0 \\ 0 & 4 \end{pmatrix}.$$

Computing the resultant of the prime polynomials $P(x)$ *and* $P(t)$ *as explained in theorem 3.9 yields a defining polynomial for the extension* $L_1 L_3^{\pi\tau}$, *namely*

$$\operatorname{res}(P(x), P(t)) = A(x,t) = (x-t)^2(x+t+1)^2.$$

Observe that by this method we have found an automorphism, since

$$D(x) \equiv D(t) \bmod (x+t+1) \text{ because } D(-(t-1)) = D(t).$$

Davenport, Lewis and Schinzel [**DLA61**] discovered the example

$$D_2(x) = T_4(x) = x^4 - 4x^2 + 2, D_1(t) = -T_4(t) = -(t^4 - 4t^2 + 2),$$

then

$$D_2(x) - D_1(t) = (t^2 - \sqrt{2}tx + x^2 - 2)(t^2 + \sqrt{2}tx + x^2 - 2),$$

so a correspondence is given by

$$\mathfrak{P}_x = [t^2 + \sqrt{2}tx + x^2 - 2, \sqrt{D_1(t)} + \sqrt{D_2(x)}].$$

Reducing this prime divisor with algorithms for real quadratic function fields, that are described for example in [**Ste96**] or [**Sch96**], yields:

$$\tilde{\mathfrak{P}}_x = [x - \tfrac{\sqrt{2}}{2t}\sqrt{D_1(t)}, \tfrac{1}{2}t^2 - \tfrac{1}{t^2} + \sqrt{D_2(x)}].$$

Since $\deg_t(D_1) = \deg_x(D_2) = 4$, the genus of both L_1 and L_2 is 1, so we can transform the defining equations to Weierstrass normal form (see for example [**SBS99**]). We obtain $\widetilde{D}_1(t) = -t^3 + \frac{40}{3}t + \frac{448}{27}$ and $\widetilde{D}_2(x) = x^3 - \frac{40}{3}x + \frac{448}{27}$ as well as

$$D_2(x) - D_1(t) = \tfrac{1}{3}(x+t)(3x^2 - 3tx - 40 + 3t^2).$$

Moreover, the unique reduced prime ideal of the double field is given by

$$\mathfrak{Q}_x = [x + t, \sqrt{D_1(t)} + \sqrt{D_2(x)}],$$

so this isogeny is not very surprising. In fact it even represents an isomorphism of the associated curves. The corresponding curves C_1, C_2 given by $u^2 = D_1(t)$ and $y^2 = D_2(x)$ have j-Invariant $2^6 5^3$ and their endomorphism ring is isomorphic to $\mathbb{Z} + 1 \cdot O_K$ where O_K is the maximal order of $\mathbb{Q}(\sqrt{-7})$.
Ehrenfeucht gave the following criterion for $D_2(x) - D_1(t)$ to be irreducible, which reduces the classes of polynomials to be investigated considerably.

Theorem 1.2. *Suppose* $gcd(\deg_x(D_2(x)), \deg_t(D_1(t))) = 1$, *then* $D_2(x) - D_1(t)$ *is irreducible.*

Up to now we have had the following cases of factorisations of $D_2(x) - D_1(t)$

- $(x-t) \mid (D(x) - D(t))$
- if $P(x,t) \mid D_2(x) - D_1(t)$, then $P(x,t) \mid D_2(E(x)) - D_2(F(t))$ for $E \in \mathbb{C}[x]$ and $F \in \mathbb{C}[t]$
- if $D_1 = T_4$ and $D_2 = -T_4$, then $D_2(x) - D_1(t) = (t^2 - \sqrt{2}tx + x^2 - 2)(t^2 + \sqrt{2}tx + x^2 - 2)$

- if $D_2(x) - D_1(t)$ is reducible, then for $(a, b) \in \mathbb{C} \times \mathbb{C}$ obviously $(aD_2(x) + b) - (aD_1(t) + b)$ is also reducible.

Definition. *We call polynomials $D_1, D_2 \in \mathbb{C}[x]$ linearly combined, if there exist $(a, b) \in \mathbb{C}^* \times \mathbb{C}$, such that $D_2(x) = D_1(ax + b)$.*

In 1998, Couveignes [**CNC99**] managed to solve the problem of reducibility of bivariate polynomials of the form $D_2(x) - D_1(t)$ over $\mathbb{C}[t, x]$ completely. His result is the following

Theorem 1.3. *Let D_1, D_2 be polynomials that are not of the type mentioned above, i.e. they are non constant, indecomposable and not linearly combined, but are nevertheless reducible over $\mathbb{C}[t, x]$, then*

$$\deg(D_1) = \deg(D_2) \in \{7, 11, 13, 15, 21, 31\}$$

Couveignes' proof uses the fact that the simple finite groups are totally classified into the Cyclic groups, the Lie groups, the Alternating groups and the 26 sporadic groups. Moreover he gives explicit formulas for those special kinds of polynomials. We now consider the examples for $\deg(D_1) = 7, 11$, which had already been found by Birch by 'entirely low brow fiddling' over lunch, see [**Cas70**].

Example. *Let $\xi = -\frac{1}{2} + \frac{1}{2}\sqrt{-7}$ and*

$$\begin{aligned} D_1(t) &= \frac{1}{7}t^7 + (1+\xi)at^5 + (1+\xi)at^4 - (3-2\xi)t^3a^2 - 2(1-2\xi)t^2a^2 - \\ &\quad \frac{1}{28}(5+3\xi)t(28a - 2 - 11\xi)a^2 - (1+\xi)a^3 \end{aligned}$$

a polynomial over $\mathbb{C}$. If we define $D_2(x) = \bar{D}_1(x)$, where $^-$ denotes the complex conjugation, then

$$\begin{aligned} P(x) = \quad & 2x^3 + x^2t - x^2t\sqrt{-7} + 7xa - 3xa\sqrt{-7} - xt^2 \\ - \quad & xt^2\sqrt{-7} - 2a\sqrt{-7} - 2t^3 - 7ta - 3ta\sqrt{-7} \end{aligned}$$

divides $D_2(x) - D_1(t)$. So we obtain the non-trivial correspondence given by

$$\mathfrak{P}_x = [P(x), \sqrt{D_1(t)} + \sqrt{D_2(x)}].$$

The differential matrix of the correspondence is given by

$$\begin{pmatrix} -\frac{1}{2} + \frac{1}{2}\sqrt{-7} & 0 & 0 \\ 0 & -\frac{1}{2} + \frac{1}{2}\sqrt{-7} & 0 \\ -a\sqrt{-7} & 0 & -\frac{1}{2} - \frac{1}{2}\sqrt{-7} \end{pmatrix}$$

and its dual by

$$\begin{pmatrix} -\frac{1}{2} - \frac{1}{2}\sqrt{-7} & 0 & 0 \\ 0 & -\frac{1}{2} - \frac{1}{2}\sqrt{-7} & 0 \\ a\sqrt{-7} & 0 & -\frac{1}{2} + \frac{1}{2}\sqrt{-7} \end{pmatrix}.$$

So the composition is

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

i.e. multiplication by [2].
A computation of the resultant yields

$$\operatorname{res}(P(x), P(t)) = (x - t)^3 Q(x, t)$$

where $Q \in L_1[x]$, $deg_x(Q) = 6$ with $D_1(x) \equiv D_1(t) \bmod Q$. In a coarser sense, $[Q(x, t), \sqrt{D(t)}]$ is equivalent to $[x - t, \sqrt{D(t)}]$, so two of the prime divisors associated to the factors of the resultant must be conjugated and therefore cancel each

other.
If we consider the basic field $k = \mathbb{F}_{29}$*, we obtain* $\xi = 21$ *and* $\bar{\xi} = 7$ *and for* $a = 1$

$$\begin{aligned} D_1(t) &= 25t^7 + 22t^5 + 22t^4 + 10t^3 + 24t^2 + 9t + 7, \\ D_2(x) &= 25x^7 + 8x^5 + 8x^4 + 11x^3 + 26x^2 + 8x + 21, \\ P(x) &= 28x^3 + 3x + 14 + (21x^2 + 10)t + 22xt^2 + t^3. \end{aligned}$$

Example. *For n=11, we obtain*

$$\begin{aligned} D_1(t) = {} & \tfrac{1}{11}t^1 1 - (\tfrac{1}{2} + \tfrac{1}{2}i\sqrt{11})t^9 + 2t^8 + (-\tfrac{21}{2} + \tfrac{3}{2}i\sqrt{11})t^7 - 16(\tfrac{1}{2} + \tfrac{1}{2}i\sqrt{11})t^6 \\ & + (\frac{51}{2} + \frac{21}{2}i\sqrt{11})t^5 + (-105 + 15i\sqrt{11})t^4 - 63(-\frac{1}{2} + \frac{1}{2}i\sqrt{11})t^3 \\ & + (70 + 50i\sqrt{11})t^2 + (-129 + 12i\sqrt{11})t - 9 - 9i\sqrt{11} \end{aligned}$$

as well as

$$\begin{aligned} P(x) = {} & x^5 - (-\tfrac{1}{2} + \tfrac{1}{2}i\sqrt{11})tx^4 + (2i\sqrt{11} - t^2)x^3 + \\ & ((\frac{11}{2} + \frac{1}{2}i\sqrt{11})t + 11 - i\sqrt{11} + t^3)x^2 + \\ & (-(-\frac{1}{2} + \frac{1}{2}i\sqrt{11})t^4 - 6it\sqrt{11}) - (\frac{11}{2} - \frac{1}{2}i\sqrt{11})t^2 - t^4 - 11 + 4i\sqrt{11})x \\ & -t^5 + (11 + 4i\sqrt{11})t + 6i\sqrt{11} - 2(\frac{11}{2} + \frac{1}{2}i\sqrt{11})t^2 + 2i\sqrt{11}t^3. \end{aligned}$$

The composition of the differential matrices is

$$\begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

i.e multiplication by [3].
A computation of the resultant yields

$$\operatorname{res}(P(x), P(t)) = (x - t)^5 Q(x, t)$$

where $D_1(x)$ *does not 'seem' to be a quadratic residue* $\bmod Q$ *(note that it is difficult to decide whether it is or not, since the degree in* t *is not bounded). So two of the prime divisors associated to* $x - t$ *must be conjugated.*

2. The Richelot isogeny

Before we define the Richelot isogeny we want to describe an approach that in fact does not lead to a non-trivial correspondence, but can be seen as a first step towards this isogeny.
Let $D_1(t) = G_1(t)G_2(t)$ and $D_2(x) = F_1(x)F_2(x)$. Suppose $P(x) = G_1(t)F_1(x) - G_2(t)F_2(x)$ is a prime polynomial in $L_1[x]$, then

$$D_1(t)D_2(x) = G_1(t)G_2(t)F_1(x)F_2(x) \equiv (G_2(t)F_2(x))^2 \bmod P(x).$$

As a consequence,

$$D_2(x) \equiv \tfrac{G_2(t)^2 F_2(x)^2}{D_1(t)} = \tfrac{F_2(x)^2}{G_1(t)^2} D_1(t) \bmod P(x).$$

So we obtain the coarser ideal class

$$\mathfrak{P}_x = [G_1(t)F_1(x) - G_2(t)F_2(x), \tfrac{F_2(x)}{G_1(t)}\sqrt{D_1(t)} + \sqrt{D_2(x)}]$$

At a first glance one might think that we have found a non-trivial correspondence. A careful examination shows, however, that this coarser ideal class is nothing else but the trivial one.
To see this, note that

$$P(x)F_2(x) = G_1(t)F_1(x)F_2(x) - G_2(t)F_2(x)^2$$

which can be transformed as a polynomial in $L_1[x]$ to

$$F_1(x)F_2(x) - \tfrac{G_2(t)}{G_1(t)}F_2(x)^2 = D_2(x) - \left(\tfrac{F_2(x)}{G_1(t)}\right)^2 D_1(t).$$

So $\mathfrak{P}_x$ is equivalent to the constant ideal $[F_2(x), \sqrt{D_2(x)}]$ and hence it represents the trivial endomorphism that maps every element of $\mathrm{Jac}(L_1|k)$ to the One in $\mathrm{Jac}(L_2|k)$, namely $\mathfrak{O}_{D_2(x)}$.
Although the above method does not lead to a non-trivial correspondence, it suggests the following construction, which was first found by Richelot, who has been a pupil of Jacobi.
Instead of thinking of polynomials $D_1(t)$ and $D_2(x)$ that factor only into two components, we now assume $D_1(t) = G_0(t)G_1(t)G_2(t)$ and $D_2(x) = F_0(x)F_1(x)F_2(x)$. Here $G_i(t) = g_{i0} + g_{i1}t + g_{i2}t^2$ for $i = 0, \ldots 2$, where $\Delta = \det(g_{ij}) \neq 0$ is a square in the constant field k, and $F_i(x) = f_{i0} + f_{i1}x + f_{i2}x^2$ (if $\det(g_{ij}) = 0$, then C_1 is isomorphic to the product of two elliptic curves, see for example [**CF96**]). Again we define $P(x) = G_1(t)F_1(x) + G_2(t)F_(x)$. Now we obtain

$$D_1(t)D_2(x) = \prod_{i=0}^{2} G_i(t)F_i(x) \equiv -G_0(t)F_0(x)(G_1(t)F_1(x))^2 \bmod P(x)$$

As we want the right hand side to be a square we need to choose the $F_i(x)$ in a way such that $-G_0(t)F_0(x)$ is a square $\bmod P(x)$ in $L_1[x]$. Since $G_0(t)$ and $F_0(x)$ are squarefree, this is not trivial.
Observe now that $\sum_{i=0}^{2} G_i(t)F_i(x) \equiv G_0(t)F_0(x) \bmod P(x)$. So it is sufficient to find $F_i(x)$ such that $\sum_{i=0}^{2} G_i(t)F_i(x)$ is a square in $L_1[x]$.
In 1836/37 Richelot found a solution to this problem. His motivation was to compute elliptic integrals up to a high precision. He remarked that if one defines

$$\begin{aligned} F_0(x) &= G_1'(x)G_2(x) - G_1(x)G_2'(x) \\ F_1(x) &= G_2'(x)G_0(x) - G_2(x)G_1'(x) \\ F_2(x) &= G_0'(x)G_1(x) - G_0(x)G_1'(x), \end{aligned}$$

then

$$\sum_{i=0}^{2} G_i(t)F_i(x) = -\Delta(x-t)^2 \tag{7}$$

is a square in $L_1[x]$ if Δ is a square in k. So we obtain a coarser (non-trivial) ideal class in $\mathrm{Jac}(\Lambda|L_1)$ that is given by

$$\mathfrak{P}_x = [P(x), \sqrt{\Delta}G_0(t)F_0(x)(x-t) + \sqrt{D_2(x)}],$$

where $P(x) = G_1(t)F_1(x) + G_2(t)F_2(x)$. Note that we can reduce the polynomial $\sqrt{\Delta}G_0(t)F_0(x)(x-t)$ in $L_1[x]$ if $\deg_x(P(x)) \leq \deg_x(F_0(x)(x-t))$.

Definition. *We call the curve C_2 given by $y^2 = D_2(x) = F_0(x)F_1(x)F_2(x)$ Richelot dual to $C_1 : u^2 = D_1(t) = G_0(t)G_1(t)G_2(t)$.*

Thus we have shown

Theorem 2.1. *Let $D_1(t) = G_0(t)G_1(t)G_2(t) \in \bar{k}[t]$ be squarefree with $G_i(t) = g_{i0} + g_{i1}t + g_{i2}t^2$ defined over $\bar{k}$, then a correspondence from $L_1 = \bar{k}(t, \sqrt{D_1(t)})$ to $L_2 = \bar{k}(x, \sqrt{D_2(x)})$, where $D_2(x) = F_0(x)F_1(x)F_2(x)$ as defined above, is given by the reduced prime ideal*

$$\mathfrak{P}_x = [G_1(t)F_1(x) + G_2(t)F_2(x), \tfrac{\sqrt{\Delta}G_1(t)F_1(x)(x-t)}{\sqrt{D_1(t)}} + \sqrt{D_2(x)}].$$

Moreover, there is a correspondence from L_2 to L_1 given by the reduced prime divisor

$$\mathfrak{P}_t^* = [P(t), W(t) + \sqrt{D_1(t)}], \text{ where}$$

$$\begin{aligned} P(t) &= G_1(t)F_1(x) + G_2(t)F_2(x) \in L_2[t], \\ W(t) &= \tfrac{\sqrt{\Delta}G_1(t)F_1(x)(x-t)}{\sqrt{D_2(x)}} \in L_2[t]. \end{aligned}$$

3. Generalisation of the Richelot isogeny

When taking a closer look at the construction above, one may ask if there are also any suitable polynomials F_i, $i = 0, \ldots, 2$ when $\deg(G_i) > 2$. The answer is yes, at least for polynomials G_i with some special properties.
We are looking for polynomials $F_i(x)$, $G_i(t)$, $i = 0 \ldots 2$ such that $G_0(t)F_0(x) + G_1(t)F_1(x) + G_2(t)F_2(x)$ is a square in $k[t, x]$. Our main theorem is the following:

Theorem 3.1. *Let $L_1 = k(t, u)$, $u^2 = D_1(t)$, $\mathrm{char}(k) \neq 2$, $a^2 = -1$ in k, be a quadratic function field with $D_1(t) = G_0(t)G_1(t)G_2(t)$, where $\deg(G_i) \leq m = 2k$, $k \geq 1$, $G_i(t) = g_{i0} + g_{i1}t + \cdots + g_{im}t^m$ and $\det((g_{ij})_{i=0..2}^{j=0..2}) \neq 0$. If there exists a bivariate polynomial $R(t, x) = \sum_{i,j=0}^{k} r_{ij}t^i x^j$, such that the linear equation system given by the coefficient matrices*

$$\begin{pmatrix} g_{00} & g_{01} & g_{02} \\ \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots \\ g_{m0} & g_{m1} & g_{m2} \end{pmatrix} \begin{pmatrix} f_{00} & \cdots & \cdots & f_{0m} \\ f_{10} & \cdots & \cdots & f_{1m} \\ f_{20} & \cdots & \cdots & f_{2m} \end{pmatrix} = \begin{pmatrix} s_{00} & \cdots & \cdots & s_{0m} \\ \vdots & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ s_{m0} & \cdots & \cdots & s_{mm} \end{pmatrix}$$

where $S(t, x) = R(t, x)^2$, has a solution matrix $F = (f_{ij})_{i=0..2}^{j=0..m}$, where the square-free part of the coefficient polynomial $D_2(x) = F_0(x)F_1(x)F_2(x)$ is a polynomial of degree ≥ 3 and the bivariate polynomial $P(x) = G_0(t)F_0(x) + G_1(t)F_1(x)$ is absolutely irreducible over $L_1[x]$ and over $L_2[t]$, then we can define a correspondence between $L_1(t, u)$ and $L_2 = k(x, y)$, $y^2 = D_2(x)$ by the coarser prime ideal class

$$\mathfrak{P}_x = [P(x, t), V(x, t) + \sqrt{D_2(x)}], \text{ where}$$

$$\begin{aligned} P(x, t) &= G_1(t)F_1(x) + G_2(t)F_2(x), \\ V(x, t) &= a\tfrac{G_1(t)F_1(x)R(x,t)}{\sqrt{D_1(t)}}. \end{aligned}$$

Moreover, there is a correspondence from L_2 to L_1, given by the coarser ideal class

$$\mathfrak{P}_t^* = [P(t, x), W(t, x) + \sqrt{D_1(t)}], \text{ where}$$

$$\begin{aligned} P(t, x) &= G_1(t)F_1(x) + G_2(t)F_2(x), \\ W(t, x) &= a\tfrac{G_1(t)F_1(x)R(x,t)}{\sqrt{D_2(x)}}. \end{aligned}$$

Proof. The only thing we have to show is that $V(x, t)^2 \equiv D_2(x) \bmod P(x, t)$ and $W(x, t)^2 \equiv D_1(t) \bmod P(x, t)$.
Obviously, we have $G_1(t)F_1(x) \equiv -G_0(t)F_0(x) \bmod P(x, t)$. So we have

$$\begin{aligned} D_1(t)D_2(x) &= G_0(t)G_1(t)G_2(t)F_0(x)F_1(x)F_2(x) \\ &\equiv -\ G_0(t)^2F_0(x)^2G_2(t)F_2(x) \\ &\equiv -\ G_0(t)^2F_0(x)^2R(x,t)^2 \qquad \bmod P(x, t) \end{aligned}$$

since $G_2(t)F_2(x) \equiv \sum_{i=0}^{2} G_i(t)F_i(x) = R(x,t)^2 \bmod P(x,t)$.
As a consequence, we can write

$$\begin{aligned} D_2(x) &\equiv -\tfrac{D_1(t)}{G_1(t)^2 G_2(t)^2} F_0(x)^2 R(x,t)^2 \mod P(x,t) \in L_1[x] \\ D_1(t) &\equiv -\tfrac{D_2(x)}{F_1(x)^2 F_2(x)^2} G_0(t)^2 R(x,t)^2 \mod P(x,t) \in L_2[t] \end{aligned}$$

which proves the theorem, considering that $-1 = a$ is a square in k. □

Remark. *Observe that the above theorem only gives a sufficient condition for a curve having this kind of isogeny. For increasing m the probability of the equation system having a solution that leads to a non-trivial correspondence seems to decrease rapidly, since a square polynomial S must exist the coefficient matrix of which consists of rows $4 \ldots m$ that are linearly dependent on the first three rows.*
Up to now we have only been able to find solutions for the case $m = 4$.
A quite obvious solution can be constructed with the help of palindromic polynomials, i.e. polynomials $a_0 + a_1 t + \cdots + a_m t^m$ the coefficient vectors $(a_0, a_1, \ldots, a_m)$ of which have the property $(a_0, a_1, \ldots, a_m) = (a_m, a_{m-1}, \ldots, a_0)$.
Let $R(x,t) = r_{00} + r_{01}x + r_{00}x^2 + r_{10}t + r_{11}tx + r_{10}tx^2 + r_{20}t^2 + r_{21}t^2x + r_{20}t^2x^2$, then we obtain the matrix $S =$

$$\begin{pmatrix} r_{00}^2 & 2r_{00}r_{10} & 2r_{00}r_{20} + r_{10}^2 & 2r_{10}r_{20} & r_{20}^2 \\ 2r_{00}r_{01} & 2r_{00}r_{11} + 2r_{10}r_{01} & 2r_{00}r_{21} + 2r_{10}r_{11} + 2r_{20}r_{01} & 2r_{10}r_{21} + 2r_{20}r_{11} & 2r_{20}r_{21} \\ 2r_{00}^2 + r_{01}^2 & 4r_{00}r_{10} + 2r_{01}r_{11} & 4r_{00}r_{20} + 2r_{10}^2 + 2r_{01}r_{21} + r_{11}^2 & 4r_{10}r_{20} + 2r_{11}r_{21} & 2r_{20}^2 + r_{21}^2 \\ 2r_{00}r_{01} & 2r_{00}r_{11} + 2r_{10}r_{01} & 2r_{00}r_{21} + 2r_{10}r_{11} + 2r_{20}r_{01} & 2r_{10}r_{21} + 2r_{20}r_{11} & 2r_{20}r_{21} \\ r_{00}^2 & 2r_{00}r_{10} & 2r_{00}r_{20} + r_{10}^2 & 2r_{10}r_{20} & r_{20}^2 \end{pmatrix}.$$

As a consequence, we can choose $G_0(t), G_1(t), G_2(t)$ palindromic and there will always be a solution to the linear equation system. It is not difficult to see that those function fields have non-trivial automorphisms besides the hyperelliptic involution. If we subsitute t by $1/t$ in G_i, we obtain $t^4 G_i(1/t) = G_i(t)$ and therefore $t^{12} D_1(1/t) = D_1(t)$. The corresponding endomorphism, which in fact is an automorphism, is given by the reduced prime divisor

$$\mathfrak{P}_x = [x - \tfrac{1}{t}, \tfrac{1}{t^6}\sqrt{D_1(t)}].$$

Example. *Let $G_0(t) = -88 - 100t + 80t^2 - 100t^3 - 88t^4$, $G_1(t) = 31 - 34t - 54t^2 - 34t^3 + 31t^4$ and $G_2(t) = -16 + 51t + 47t^2 + 51t^3 - 16t^4$, $D_1(t) = G_0(t)G_1(t)G_2(t)$. Then we obtain a correspondence of the above type from $L_1 = k(t, \sqrt{D_1(t)})$ to $L_2 = k(x, \sqrt{D_2(x)})$ for*

$$\begin{aligned} D_2(x) = {} & 1/66587713448768 \times \\ & (1574273 + 12197892x^4 - 8377962x + 45614097x^2 - 22758036x^3) \times \\ & (10882996 + 84265424x^4 - 59747656x + 290685252x^2 - 163011088x^3) \times \\ & (-11310140 - 87654000x^4 + 59361832x - 282318796x^2 + 162160656x^3) \end{aligned}$$

Composing its differential matrix with the corresponding dual matrix we obtain after some basis change,

$$M_{\mathfrak{P}\mathfrak{P}^*} = \begin{pmatrix} 8 & 0 & 0 & 0 & 0 \\ 0 & 8 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

So the endomorphism ring of L_1 is not simple. But this can also be seen from the fact that L_1 admits an involutoric automorphism different from the hyperelliptic involution as shown above. This means that L_1 has a genus 2 function subfield. Function field of this type should not be used for cryptographic purposes, since the order of the Jacobian of L_1 can be divided by the order of the Jacobian of the subfield according to a theorem by Madan [**Mad70**].

The above class is not the only class, admitting a generalised Richelot isogeny. With the help of the computer algebra system Maple [**Map**] we were able to find a more general class. Let $G_{(0)},\dots,G_{(4)}$ be the rows of the coefficient matrix $G=(g_{ij})$. If the rows $G_{(3)}$ and $G_{(4)}$ can be written as

$$\begin{aligned} G_{(3)} &= (-\mu_2^3-2\mu_2\mu_1)G_{(0)}+ & \mu_1 G_{(1)}+ & \mu_2 G_{(2)}\\ G_{(4)} &= (\tfrac{1}{2}\mu_1\mu_2^2+\mu_1^2)G_{(0)}+ & (\tfrac{1}{8}\mu_2^3+\tfrac{1}{2}\mu_2\mu_1)G_{(1)}+ & (\tfrac{1}{4}\mu_2^2)G_{(2)} \end{aligned}$$

for some $\mu_1,\mu_2\in k$, then there exists a generalised Richelot isogeny from $L_1=k(t,\sqrt{D_1(t)})$ with

$$\begin{aligned} D_1(t) = {} & (g_{11}+g_{21}t+g_{31}t^2+(-g_{11}\mu_2^3-2g_{11}\mu_2\mu_1+\mu_1 g_{21}+\mu_2 g_{31})t^3+\\ & (1/2g_{11}\mu_1\mu_2^2+g_{11}\mu_1^2+1/8g_{21}\mu_2^3+1/2g_{21}\mu_2\mu_1+1/4\mu_2^2 g_{31})t^4)\times\\ & (g_{12}+g_{22}t+g_{32}t^2+(-g_{12}\mu_2^3-2g_{12}\mu_2\mu_1+\mu_1 g_{22}+\mu_2 g_{32})t^3+\\ & (1/2g_{12}\mu_1\mu_2^2+g_{12}\mu_1^2+1/8g_{22}\mu_2^3+1/2g_{22}\mu_2\mu_1+1/4\mu_2^2 g_{32})t^4)\times\\ & (g_{13}+g_{23}t+g_{33}t^2+(-g_{13}\mu_2^3-2g_{13}\mu_2\mu_1+\mu_1 g_{23}+\mu_2 g_{33})t^3+\\ & (1/2g_{13}\mu_1\mu_2^2+g_{13}\mu_1^2+1/8g_{23}\mu_2^3+1/2g_{23}\mu_2\mu_1+1/4\mu_2^2 g_{33})t^4) \end{aligned}$$

to some $L_2=k(x,\sqrt{D_2(x)})$. Observe that for $\mu_1=1$ and $\mu_2=0$ we obtain the palindromic case of above.

First we will give an example where both L_1 and L_2 have genus 5.

Example. *Let* $L_1=\mathbb{C}(t,\sqrt{D_1(t)})$ *and* $L_2=\mathbb{C}(x,\sqrt{D_2(x)})$ *with*

$$D_1(t)=G_0(t)G_1(t)G_2(t),\ D_2(x)=F_0(x)F_1(x)F_2(x)$$

with the linear equation system given by the coefficient matrices

$$\begin{pmatrix} 1 & 7 & 9\\ -\frac{17}{3} & -41 & -55\\ \frac{28}{3} & 63 & 83\\ 1 & 1 & 3\\ 1 & 2 & 0 \end{pmatrix}\begin{pmatrix} 72 & 114 & 175 & \frac{201}{2} & \frac{265}{4}\\ -18 & -15 & -21 & -\frac{5}{4} & -\frac{69}{8}\\ 6 & -1 & -\frac{8}{3} & -\frac{39}{4} & -\frac{13}{24} \end{pmatrix}=\begin{pmatrix} 0 & 0 & 4 & 4 & 1\\ 0 & 24 & 16 & 18 & 8\\ 36 & 36 & 89 & 50 & 30\\ 72 & 96 & 146 & 70 & 56\\ 36 & 84 & 133 & 98 & 49 \end{pmatrix},$$

where

$$S(x,t)=R(x,t)^2=(6t+6t^2+2x+tx+7t^2x+x^2+4tx^2+7t^2x^2)^2.$$

Here we have chosen $\mu_1=1$ *and* $\mu_2=2$.
Composing the matrix of differentials with the corresponding dual matrix we obtain after some basis change again

$$M_{\mathfrak{P}\mathfrak{P}^*}=\begin{pmatrix} 8 & 0 & 0 & 0 & 0\\ 0 & 8 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Moreover, a resultant computation yields

$$\operatorname{res}(P(x),P(t))=(x-t)^4(3xt-x-1-t)^4H(x,t)^4.$$

Since $D_1(\frac{t+1}{3t-1})=2^{12}\frac{D_1(t)}{(3t-1)^{12}}$, *the prime ideal*

$$\mathfrak{P}_x=[x-\tfrac{t+1}{3t-1},2^6\tfrac{\sqrt{D_1(t)}}{(3t-1)^6}]$$

defines an automorphism on the function field $L_1=\mathbb{C}(t,\sqrt{D_1(t)})$.

In the next example, we obtain an isogeny from a genus 5 to a genus 2 function field.

Example. *Let* $L_1 = \mathbb{C}(t, \sqrt{D_1(t)})$ *and* $L_2 = \mathbb{C}(x, \sqrt{D_2(x)})$ *where*

$$D_1(t) = G_0(t)G_1(t)G_2(t),\ D_2(x) = F_0(x)F_1(x)F_2(x)$$

with the linear equation system given by the coefficient matrices

$$\begin{pmatrix} 4 & 9 & 4 \\ 6 & 6 & 2 \\ 9 & 6 & 1 \\ -\frac{32}{3} & -50 & -\frac{76}{3} \\ \frac{97}{9} & 5 & \frac{1}{9} \end{pmatrix} \begin{pmatrix} 0 & 0 & -\frac{19}{2} & -6 & -\frac{7}{6} \\ 0 & 0 & \frac{115}{3} & \frac{82}{3} & \frac{49}{9} \\ 0 & 0 & -\frac{149}{2} & -54 & -\frac{65}{6} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 9 & 6 & 1 \\ 0 & 0 & 24 & 20 & 4 \\ 0 & 0 & 70 & 56 & \frac{34}{3} \\ 0 & 0 & 72 & \frac{196}{3} & \frac{44}{3} \\ 0 & 0 & 81 & 66 & \frac{121}{9} \end{pmatrix},$$

where

$$S(x,t) = R(x,t)^2 = (3x + 4tx + 9t^2x + x^2 + 2tx^2 + \frac{11}{3}t^2x^2)^2.$$

Here the prime polynomial $P(x)$ *is of degree* 2 *in* x *and of degree* 4 *in* t.
Composing the matrix of differentials with the corresponding dual matrix we obtain after some basis change

$$M_{\mathfrak{P}\mathfrak{P}^*} = \begin{pmatrix} 4 & 0 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Similarly, applying first $\mathfrak{P}^*$ *and then* $\mathfrak{P}$ *we have*

$$M_{\mathfrak{P}^*\mathfrak{P}} = \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix},$$

i.e. a multiplication by $[4]$ *in the endomorphism ring of* $\mathrm{Jac}(L_2|\mathbb{C})$.
A resultant computation yields

$$\mathrm{res}(P(x), P(t)) = (x-t)^2(5xt - 3x - 3 - 3t)^2 H(x,t)$$

Since $D_1(\frac{3t+3}{5t-3}) = 191102976\frac{D_1(t)}{(5t-3)^{12}}$, *the prime divisor*

$$\mathfrak{P}_x = [x - \tfrac{t+1}{3t-1}, 13824\tfrac{\sqrt{D_1(t)}}{(5t-3)^6} + \sqrt{D(x)}]$$

defines an automorphism on $L_1|\mathbb{C}$.

In our last example, both function fields have genus 3. This can be achieved by setting some of the coefficients of the G_i to zero.

Example. *Let* L_1 *and* L_2 *be given by the coefficient matrices*

$$\begin{pmatrix} 1 & 7 & 9 \\ -\frac{383}{66} & \frac{919}{66} & \frac{33}{2} \\ -\frac{13933}{1584} & \frac{12629}{1584} & \frac{121}{16} \\ 3 & 1 & 0 \\ 5 & 0 & 0 \end{pmatrix} \begin{pmatrix} \frac{36}{5} & -2 & \frac{1357}{180} & -\frac{37}{36} & \frac{1369}{720} \\ \frac{252}{5} & 8 & \frac{3643}{60} & \frac{31}{12} & \frac{1517}{80} \\ -40 & -6 & -\frac{3857}{81} & -\frac{235}{162} & -\frac{4811}{324} \end{pmatrix} =$$

$$\begin{pmatrix} 0 & 0 & 4 & 4 & 1 \\ 0 & 24 & 16 & 18 & 8 \\ 36 & 36 & \frac{173}{3} & \frac{56}{3} & \frac{133}{6} \\ 72 & 2 & \frac{250}{3} & -\frac{1}{2} & \frac{74}{3} \\ 36 & -10 & \frac{1357}{36} & -\frac{185}{36} & \frac{1369}{144} \end{pmatrix},$$

where

$$S(x,t) = R(x,t)^2 = (6t + 6t^2 + 2x + tx - \tfrac{5}{6}t^2x + x^2 + 4tx^2 + \tfrac{37}{12}t^2x^2)^2.$$

Here we have the case that $G_2(t)$ *and also* $F_0(x)$ *are square polynomials, namely*

$$G_2(t) = (\tfrac{1}{4}(11t+12))^2 \text{ and } F_0(x) = (\tfrac{37x^2-10x+72}{12\sqrt{5}})^2.$$

Moreover, $G_0(t)F_0(x) + G_1(t)F_1(x)$ *can be divided by* $37x^2 - 10x + 72$, *so* $P(x)$ *is of degree* 2 *in* x *and of degree* 4 *in* t.
Composing the matrix of differentials with the corresponding dual matrix we obtain after some basis change,

$$M_{\mathfrak{P}\mathfrak{P}^*} = \begin{pmatrix} 8 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

The resultant is given by

$$\operatorname{res}(P(x), P(t)) = (x-t)^2((11t+12)x + 12t + 12)^2 H(x,t)^2.$$

Since $D_1(-\frac{12t+12}{11t+12}) = 2^8 3^4 \frac{D_1(t)}{(11t+12)^8}$, *the prime ideal*

$$\mathfrak{P}_x = [x - \tfrac{12t+12}{11t+12}, 2^4 3^2 \tfrac{\sqrt{D_1(t)}}{(11t+12)^4}]$$

defines an automorphism on the function field $L_1 = \mathbb{C}(t, \sqrt{D_1(t)})$.

4. Construction of $\sqrt{2}$-endomorphisms via Cholesky decomposition

In this section we show how to construct hyperelliptic function fields the Jacobian of which has a $\sqrt{2}$-endomorphism. To achieve this we assume the polynomials F_i of the last sections to be equal to the G_i. Therefore the Richelot isogenous curve is isomorphic to the original and we obtain the $\sqrt{2}$-endomorphism.

Theorem 4.1. *Let* $L = k(t,u)$, $u^2 = D(t)$ *be a genus* 2 *hyperelliptic function field, where* $D(t)$ *can be written as* $D(t) = G_0(t)G_1(t)G_2(t)$ *and* $G_i(t) = g_{i0} + g_{i1}t + g_{i2}t^2$, $g_{ij} \in k$. *Moreover, the coefficient matrix* $G = g_{ij} = C \circ S$, *where* C *is given by*

$$\begin{pmatrix} r_{00} & 0 & 0 \\ 2r_{10} & \sqrt{-2r_{10}^2 + 2r_{00}r_{11}} & 0 \\ \frac{r_{10}^2}{r_{00}} & \frac{-2r_{10}^3 + 2r_{00}r_{10}r_{11}}{r_{00}\sqrt{-2r_{10}^2+2r_{00}r_{11}}} & \frac{-r_{10}^2 + r_{00}r_{11}}{r_{00}} \end{pmatrix}$$

with $r_{00} \in k^*$, $r_{00}r_{11} \neq r_{10}^2$ *and* $S \in O_k(3)$ *is an orthogonal matrix. Then the Richelot isogeny defines a* $\sqrt{2}$*-endomorphism on* $\operatorname{Jac}(L)$.

Proof. Via some computation we obtain

$$CC^T = \begin{pmatrix} r_{00}^2 & 2r_{00}r_{10} & r_{10}^2 \\ 2r_{00}r_{10} & 2r_{10}^2 + 2r_{00}r_{11} & 2r_{10}r_{11} \\ r_{10}^2 & 2r_{10}r_{11} & r_{11}^2 \end{pmatrix}$$

which is nothing else but the coefficient matrix of the square of a bivariate symmetric polynomial $R(x,t) = r_{00} + r_{10}(t+x) + r_{11}xt$ (CC^T is nothing else but the Cholesky decomposition of the right hand side matrix). If we define, as usual,

$$\begin{aligned} P(x,t) &= G_0(t)G_0(x) + G_1(t)G_1(x) \\ V(x,t) &= a\tfrac{G_1(t)G_1(x)}{\sqrt{D(t)}}R(x,t), \end{aligned}$$

$V^2(x) \equiv D(x) \bmod P(x)$ in $L[x]$. Since $\deg(P) \leq 2$, $\mathfrak{P}_x = [P(x), V(x) + \sqrt{D(x)}]$ defines a reduced prime ideal and we obtain an endomorphism ε on the Jacobian of L. The composition $\varepsilon \circ \varepsilon$ defines a multiplication by [2] on the Jacobian. This can either be seen by composition of correspondences as done in chapter 2 or by computing the composition of the differential matrices of the Richelot isogeny and its dual. □

Remark. *Note that the coefficient matrix C itself never defines a hyperelliptic curve, since the corresponding*

$$D(t) = G_0(t)G_1(t)G_2(t) = c \cdot (r_{10}t + r_{00})^3 t^3$$

for some constant $c \in k^*$. Reducing the squares, we are left with some polynomial of degree 2, which, as we have seen in chapter 1, defines a function field that is isomorphic to the rational function field.

We now consider examples, where D defines a hyperelliptic function field.

Example. *We put $r_{00} = 3, r_{10} = 1, r_{11} = 2$. Then we obtain $R(x,t) = 3+t+x+2tx$ and*

$$CC^T = \begin{pmatrix} 3 & 0 & 0 \\ 2 & \sqrt{10} & 0 \\ \frac{1}{3} & \frac{1}{3}\sqrt{10} & \frac{5}{3} \end{pmatrix} \circ \begin{pmatrix} 3 & 2 & \frac{1}{3} \\ 0 & \sqrt{10} & \frac{1}{3}\sqrt{10} \\ 0 & 0 & \frac{5}{3} \end{pmatrix} = \begin{pmatrix} 9 & 6 & 1 \\ 6 & 14 & 4 \\ 1 & 4 & 4 \end{pmatrix}.$$

For $S \in O(3)$ we choose

$$S = \begin{pmatrix} \frac{1}{2}\sqrt{2} & 0 & \frac{1}{2}\sqrt{2} \\ 0 & 1 & 0 \\ -\frac{1}{2}\sqrt{2} & 0 & \frac{1}{2}\sqrt{2} \end{pmatrix}$$

As a consequence,

$$C \circ S = \begin{pmatrix} \frac{3}{2}\sqrt{2} & 0 & \frac{3}{2}\sqrt{2} \\ \sqrt{2} & \sqrt{10} & \sqrt{2} \\ -\frac{2}{3}\sqrt{2} & \frac{1}{3}\sqrt{10} & \sqrt{2} \end{pmatrix}.$$

So we have

$$D(t) = G_0(t)G_1(t)G_2(t) = \tfrac{1}{72}\sqrt{10}(-4t+3+3\sqrt{5})(4t-3+3\sqrt{5})(3+t)t(3+2t+2t^2).$$

Conclusion

In this thesis we have shown that the theory of algebraic correspondences introduced by Deuring in the 1930s can be applied to construct non-trivial homomorphisms between the Jacobi groups of hyperelliptic function fields.
Concretely, we have deduced algorithms to add and multiply correspondences which perform in a reasonable time if the degrees of the associated divisors of the double field are small. Moreover, we have shown how to compute the differential matrices associated to prime divisors of the double field for arbitrary genus. These matrices give a representation for the homomorphisms or endomorphisms in the additive group (ring) of matrices which is even faithful if the ground field has characteristic zero. As first examples for non-trivial correspondences we have investigated multiplication by m endomorphisms. Afterwards we have used factorisations of certain bivariate polynomials to construct prime divisors of the double field that are not equivalent to 0 in a coarser sense. Applying the theory of Deuring, these divisors yield homomorphisms between the Jacobi groups of special classes of hyperelliptic function fields. Finally, we have generalised the Richelot isogeny to higher genus and by this way derived a class of hyperelliptic function fields given in terms of their defining polynomials which admit non-trivial homomorphisms. These include homomorphisms between the Jacobi groups of hyperelliptic curves of different as well as of equal genus. In addition, the last section of chapter 4 provides an explicit method to construct genus 2 function fields the endomorphism ring of which contains a $\sqrt{2}$ multiplication with the help of the Cholesky decomposition of a certain matrix.
For further research, it would be interesting to find non-trivial correspondences by factoring bivariate polynomials of the form $A(t)^2 D_1(t) - B(t)^2 D_2(x)$. A factor of degree less than or equal to $\frac{1}{2}g_2$ would give rise to a split prime divisor not equivalent to the trivial class, since then $A(t)\sqrt{D_1(t)}/B(t) \equiv D_2(x) \bmod P(x)$. However, such an approach without any further restrictions to the defining polynomials $D_1(t)$ and $D_2(x)$ seems to be computationally infeasible already for elliptic function fields. What should be tried is to find similar constructions to the Richelot isogeny and its generalisation or the Cholesky decomposition presented in chapter 4.

Index

Bibliography

[ADH94] L. Adleman, J. DeMarrais, and M. Huang. A subexponential algorithm for discrete logarithms over the rational subgroup of the jacobians of large genus hyperelliptic curves over finite fields. *Algorithmic Number Theory, LNCS 877*, pages 28–40, 1994.

[Art21] Emil Artin. *Quadratische Körper im Gebiete der höheren Kongruenzen.* PhD thesis, Universität Leipzig, 1921.

[BCLW02] N. Boston, T. Clancy, Y. Liow, and J. Webster. Genus 2 hyperelliptic curve coprocessor. *Lecture Notes in Computer Science 2523*, pages 400–414, 2002.

[Ben99] Peter Bending. *Curves of Genus 2 with sqrt 2 Multiplication.* PhD thesis, University of Oxford, 1999. http://front.math.ucdavis.edu/ANT/0213/.

[BS66] S.L. Borewics and I.R. Safarevic. *Zahlentheorie.* Birkhäuser Verlag Basel/Stuttgart, 1966.

[Can94] David Cantor. On the analogue of the division polynomials for hyperelliptic curves. *Crelle J. 447*, pages 91–145, 1994.

[Cas70] J.W.S. Cassels. Factorization of polynomials in several variables. *Proc. 15th Scandinavian Congress, Oslo 1968, LNM 118, Springer Verlag*, pages 1–17, 1970.

[CF96] J.W.S. Cassels and V. Flynn. *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2.* London Mathematical Society Lecture Notes, 230, Cambridge University Press, 1996.

[CMT00] J. Chao, N. Matsuda, and S. Tsujii. Construction of hyperelliptic curves with cm and its application to cryptosystems. *Asiacrypt 2000*, pages 259–273, 2000.

[CNC99] P. Cassou-Nogues and J.M. Couveignes. Factorisations explicites de g(y)-h(z). *Acta Arith. 87 (1999), no. 4*, pages 291–317, 1999.

[Deu37] Max Deuring. Arithmetische Theorie der Korrespondenzen algebraischer Funktionenkörper, Teil I. *Crelle J. 177*, pages 161–191, 1937. Teil II, Crelle J. 183, pages 25-36, 1940.

[Deu73] Max Deuring. *Lectures on the Theory of Algebraic Functions of One Variable.* Lecture Notes in Mathematics, Springer Verlag, 1973.

[DLA61] H. Davenport, D.J. Lewis, and A.Schinzel. Equations of the form f(x)=g(y). *Quart. J. Math. Oxford (2), 12*, pages 304–312, 1961.

[Eic63] Martin Eichler. *Einführung in die Theorie der algebraischen Zahlen und Funktionen.* Basel, Birkhäuser Verlag, 1963.

[FR94] G. Frey and H. Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Mathematics of Computation*, 62:865–874, 1994.

[Fri70] Fried. On a conjecture of schur. *Michigan Math. J. 17*, pages 41–55, 1970.

[FT91] A. Fröhlich and M.J. Taylor. *Algebraic number theory.* Cambridge studies in advanced mathematics 27, 1991.

[Gau00] P. Gaudry. An algorithm for solving the discrete log problem on hyperelliptic curves. *Advances in Cryptology, Eurocrypt'2000, Springer-Verlag, LNCS 1807*, pages 19–34, 2000.

[GLS01] C. Günter, T. Lange, and A. Stein. Speeding up the arithmetic on hyperelliptic koblitz curves of genus 2. *Selected Areas in Cryptography, SAC 2001, Lecture Notes in Computer Science 2012, (Springer)*, pages 106–117, 2001.

[Gor97] B. Brent Gordon. A survey of the hodge conjecture for abelian varieties, 1997. http://arxiv.org/pdf/alg-geom/9709030.

[Har77] Robin Hartshorne. *Algebraic geometry.* Graduate Texts in Mathematics 52, Springer-Verlag, 1977.

[Has34] Helmut Hasse. Über die kongruenzzetafunktionen. *Sitzungsber. Preuß. Akad. Wiss. Berlin, Phys.-Math.*, 1934.

[HS00] M. Hindry and J.H. Silverman. *Diophantine Geometry, An Introduction.* Graduate Texts in Mathematics 201, Springer-Verlag, 2000.

[Iwa93] K. Iwasawa. *Algebraic Functions.* Translations of Mathematical Monographs, AMS 118, 1993.

[Ked01] Kiran S. Kedlaya. Counting points on hyperelliptic curves using monsky-washnitzer cohomology. *Journal of the Ramanujan Mathematical Society 16*, pages 323–338, 2001.

[Kob89] Neil Koblitz. Hyperelliptic cryptosystems. *J. Cryptology 1*, pages 139–150, 1989.

[Koc97] Helmut Koch. *Zahlentheorie, Algebraische Zahlen und Funktionen.* Vieweg Verlag, 1997.

[Lan64] Serge Lang. *Algebraic numbers.* Addison-Wesley Publishing Company, Inc., 1964.

[Lan87] Serge Lang. *Elliptic Functions, 2nd edition.* Graduate Texts in Mathematics, 112. New York, Springer-Verlag, 1987.

[Lan94] Serge Lang. *Algebraic number theory, 2nd edition.* Graduate Texts in Mathematics. 110. New York, Springer-Verlag, 1994.

[Mad70] M.L. Madan. On class numbers in fields of algebraic functions. *Archiv der Mathematik 21*, pages 167–171, 1970.

[Map] Maple. Version 8.01, Nov 2, 2002, Copyright (c) 1981-2002 Waterloo Maple Inc. All Rights Reserved.

[MCT02] K. Matsuo, J. Chao, and S. Tsujii. An improved baby step giant step algorithm for point counting of hyperelliptic curves over finite fields. *ANTS 2002*, pages 461–474, 2002.

[Mum70] D. Mumford. *Abelian Varieties.* Tata Institute of Fundamental Research Studies in Mathematics. 5. London: Oxford University Press. VIII, 1970.

[Poh78] Martin E. Pohlig, Stephen C.; Hellman. An improved algorithm for computing logarithms over gf(p) and its cryptographic significance. *IEEE Trans. Inf. Theory 24*, pages 106–110, 1978.

[PR99] Sachar Paulus and Hans-Georg Rück. Real and imaginary quadratic representations of hyperelliptic function fields. *Mathematics of Computation*, 68(227):1233–1241, 1999.

[PWGP03] J. Pelzl, T. Wollinger, J. Guajardo, and C. Paar. Hyperelliptic curves cryptosystems: closing the performance gap to elliptic curves. *Cryptology ePrint archive, http://eprint.iacr.org/*, 2003.

[PWP03] J. Pelzl, T. Wollinger, and C. Paar. Low cost security: Explicit formulae for genus 4 hyperelliptic curves. *Selected Areas in Cryptography, SAC 2003, Lecture Notes in Computer Science 2012, (Springer)*, 2003.

[Rüc99] H. Rück. On the discrete logarithm in the divisor class group of curves. *Mathematics of Computation*, 68:805–806, 1999.

[Roq51] Peter Roquette. *Arithmetischer Beweis der Riemannschen Vermutung in Kongruenzfunktionenkörpern beliebigen Geschlechts.* PhD thesis, Universität Hamburg, 1951.

[Ros02] Michael Rosen. *Number Theory in Function Fields.* Graduate Texts in Mathematics. 210. New York, Springer-Verlag, 2002.

[SBS99] N. Smart, I. Blake, and G. Seroussi. *Elliptic Curves in Cryptography.* London Mathematical Society Lecture Notes, 265, Cambridge University Press, 1999.

[Sch95] Rene Schoof. Counting points on elliptic curves over finite fields. *Les 18ièmes Journées Arithmétiques, Bordeaux 1993, J. Théorie de Nombres Bordeaux 7*, pages 219–254, 1995.

[Sch96] Renate Scheidler. Cryptography in real quadratic congruence function fields. *Proceedings of Pragocrypt 1996, CTU Publishing House, Prague (Czech Republic)*, pages 109–128, 1996.

[Shp99] Igor Shparlinski. *Finite Fields: Theory and Computation.* Dordrecht, Boston, London, Kluwer Academic Publishers, 1999.

[Ste96] Andreas Stein. *Algorithmen in reell-quadratischen Kongruenzfunktionenkörpern.* PhD thesis, Universität Saarbrücken, 1996.

[Ste99] Andreas Stein. Infrastructure in real quadratic function fields. Technical report, Department of Combinatorics and Optimization, University of Waterloo, Ontario, 1999.

[Ste01] Andreas Stein. Sharp upper bounds for arithmetics in hyperelliptic function fields. *Journal of the Ramanujan Mathematical Society 16, No. 2*, pages 1–86, 2001.

[Sti93] H. Stichtenoth. *Algebraic function fields and codes.* Springer Verlag, 1993.

[Tes01] E. Teske. Square-root algorithms for the discrete logarithm problem. *Public Key Cryptography and Computational Number Theory*, pages 283–301, 2001.

[TTV91] W. Tautz, J. Top, and A. Verberkmoes. Explicit hyperelliptic curves with real multiplication and permutation polynomials. *Can. J. Math. Vol. 43*, pages 1055–1064, 1991.

[vdW93] B.L. van der Waerden. *Algebra II, sechste Auflage.* Springer Verlag, 1993.

[Wei71] André Weil. *Courbes Algébriques et Variétés Abeliennes.* Hermann, Paris, 1971.

[Wen03] A. Weng. Constructing hyperelliptic curves of genus 2 suitable for cryptography. *Math. Comp. 72*, pages 435–458, 2003.

Curriculum Vitae

1984-1993	Besuch des Johannesgymnasiums Lahnstein
1994-2000	Student an der Universität Kaiserslautern Diplom in Mathematik mit Nebenfach Informatik im März 2000
2000-2003	Doktorand am Fraunhofer-Institut für Techno- und Wirtschaftsmathematik (ITWM) in Kaiserslautern, finanziert über ein Stipendium der BGS Systemplanung AG