CARL VON OSSIETZKY universität OLDENBURG

IfM INSTITUT FÜR MATHEMATIK

Explicit Construction of Rational Torsion Divisors on Jacobians of Curves

Von der Fakultät für Mathematik und Naturwissenschaften der Carl von Ossietzky Universität Oldenburg zur Erlangung des Grades und Titels eines

Doktors der Naturwissenschaften (Dr. rer. nat.)

angenommene Dissertation von

Herrn Max Kronberg

geboren am 09. Januar 1986 in Neumünster.

Gutachter:	**Prof. Dr. Andreas Stein**
Zweitgutachter:	**Prof. Dr. Jaap Top**
Tag der Disputation:	**06. November 2015**

Abstract

In this thesis we describe explicit ways to construct algebraic curves over number fields such that their jacobians admit a certain rational torsion structure. Using these constructions, we give new examples of many different torsion orders over the rational numbers and over some number fields of small degree.

While so far only examples of hyperelliptic curves with a torsion point of large order on the jacobian are known, we develop methods that can be applied to a larger class of algebraic curves. With these methods we are able to give series of algebraic curves with a torsion point of an order which is linear and quadratic in the genus.

Furthermore, we examine possible orders N of torsion points in a certain family of hyperelliptic curves with real multiplication in the jacobian for some small N.

Zusammenfassung

In dieser Dissertation beschreiben wir explizite Methoden zur Konstruktion algebraischer Kurven über Zahlkörpern, so dass deren Jacobischen eine vorgegebene rationale Torsionsuntergruppe besitzen. Mit diesen Methoden berechnen wir neue Beispiele von Kurven mit einem rationalen Punkt gegebener Ordnung, sowohl über den rationalen Zahlen als auch über Zahlkörpern kleinen Grades.

Während bisher nur Beispiele von hyperelliptischen Kurven mit einem Torsionspunkt großer Ordnung auf der Jacobischen bekannt waren, entwickel wir Methoden, welche sich in einer größeren Klasse algebraischer Kurven anwenden lassen. Mit diesen Methoden konstruieren wir Serien algebraischer Kurven mit Torsionspunkten, deren Ordnung linear und quadratisch im Geschlecht der Kurven sind.

Desweiteren untersuchen wir auftretende Ordnungen von Torsionspunkten in einer Familie von hyperelliptischen Kurven mit reeller Multiplikation.

Contents

Introduction

The goal of this thesis is to construct explicit examples of algebraic curves admitting a rational point of prescribed order N on their jacobians. In the case of elliptic curves over the rational numbers for all orders N, such that an elliptic curve with a $\mathbb{Q}$-rational point of order N exists, a parametrized family is known. Furthermore, all possibly occurring N are known [Maz77]. In contrast, for hyperelliptic curves and curves in general of genus greater than one, not much about the torsion subgroup is known.

By a well-known theorem of Mordell and Weil, the group of rational points of an abelian variety A over a number field K is finitely generated. Thus there exists a finite group $A_{tors}(K)$, called the *K-rational torsion subgroup*, and an integer $r \geq 0$, called the *rank* of $A(K)$, such that $A(K) \cong A_{tors}(K) \times \mathbb{Z}^r$. While in some cases a lot is known about the torsion subgroup, about the rank even in the case of elliptic curves little is known. Even in the case where the dimension of A is one, there exist lots of famous conjectures concerning the rank. For an explicitly given elliptic curve it is not always possible to determine the rank of this curve.

In this thesis we consider the torsion part of the rational points on an abelian variety. There are lots of interesting open problems concerning the rational torsion subgroup of an abelian variety.

Problem. *Let $A_{/K}$ be an abelian variety defined over a field K. Is it possible to determine $A_{tors}(K)$?*

Obviously for a finite field K the answer to this question is equivalent to the existence of a point-counting algorithm. For some classes of abelian varieties, for example jacobians of hyperelliptic curves of small genus, there are fast algorithms like the SEA Algorithm [Sch95]. In general, for $K = \mathbb{Q}$ there are no known algorithms. For general abelian varieties, we can use the fact that for an odd prime of good reduction there exists an injection of the torsion subgroup into the group of $\mathbb{F}_p$-rational points on the reduced jacobian variety over $\mathbb{F}_p$. But this does not always yield sharp bounds on the order of the torsion subgroup.

Problem. *Given positive integers N and g, is it possible to find an abelian variety $A_{/K}$ of dimension g such that*

$$N | \# A_{tors}(K)?$$

This problem is central in this thesis. First, we consider the case of jacobians of hyperelliptic and elliptic curves. There are already a lot of positive answers given. For elliptic curves defined over $\mathbb{Q}$ the set of possible integers N that occur as torsion orders is determined by Mazur and for every possible N a one-parameter family with a torsion point of order N is constructed by Ogg.

For higher dimensional abelian varieties over $\mathbb{Q}$ not much is known. We start with the two-dimensional case, that is, jacobians of hyperelliptic curves of genus two. For all primes up to $N = 29$ there is at least one hyperelliptic curve of genus two known which has a rational divisor of order N. The example curve for $N = 29$ was found by Leprévost and is so far the largest prime number such that there exists an example. The technique of Leprévost uses certain relations among divisors on a family of hyperelliptic curves. This technique is described in detail in Section 3.4. We use this technique and variants of it to obtain the following results.

Result. *We construct a new example of a hyperelliptic curve of genus two with*

1. *a rational point of order* 39 *over* $\mathbb{Q}$*,*
2. *a rational* 31*-torsion point over a degree three number field,*
3. *a rational* 37*-torsion point over a degree two number field.*

These curves are non-isomorphic to the known examples.

Furthermore, we are able to find hyperelliptic curves of genus two with a rational point of order $N = 29$ and $N = 40$ with a newly developed variation of the technique by Flynn and Leprévost. These examples lie in the same isomorphism classes as the known examples.

By a straightforward approach, which is based on finding elements in the function field of a hyperelliptic curve defined over $\mathbb{Q}$ such that their norm is a N^{th} power, we construct a one-dimensional family of curves with a rational five-torsion point on the jacobian and an example of a curve with a rational seven-torsion point.

In order to approach the stated problem, we make use of Hensel's Lemma to get the following results.

Result. *Given a prime p, we construct a polynomials $F_1, F_2 \in \mathbb{Q}[X]$ with the following property. Let $i \in \{1, 2\}$. If F_i is separable, then the jacobian of the curve $C_i : Y^2 = F_i(X)$ has a $\mathbb{Q}$-rational point of order p.*

While already Leprévost used Hensel's Lemma to construct a single example, the construction of a series of curves with prime torsion is new. Additionally, for $N = 17$

we get an example of a hyperelliptic curve of genus two defined over a number field of degree seven.

In the case of elliptic curves we illustrate the lifting technique by constructing a one-dimensional family of elliptic curves with a $\mathbb{Q}$-rational seven-torsion point.

We see in this thesis that the task of constructing jacobian varieties with a torsion point of certain order is closely related to solutions of norm equations in the function field of the associated curve. If we consider PELL's equation as a norm equation, such solutions can by found in some cases by the Continued Fraction Algorithm or the VORONOI Algorithm. The known results for hyperelliptic curves with a torsion divisor of order quadratic in the genus, for example by FLYNN, LEPRÉVOST and VAN DER POORTEN, all rely in some sense on the periodicity of a certain continued fraction expansion. For non-hyperelliptic curves defined over $\mathbb{Q}$ such an approach is new. We relate the correctness and periodicity of the VORONOI Algorithm to the finiteness of the order of a special divisor and obtain the following result.

Result (Section 3.8 and Section 3.10)**.** *There exists a family of superelliptic curves defined over $\mathbb{Q}$ with a rational torsion point of order linear in the genus on their jacobians.*

There are at least two families of non-hyperelliptic and non-superelliptic curves defined over $\mathbb{Q}$ with a rational torsion point of order quadratic in the genus on their jacobian.

For composite N HOWE found for $N = 70$ a hyperelliptic curve of genus two defined over $\mathbb{Q}$ such that the jacobian has a $\mathbb{Q}$-rational point of order N. This is the largest order that is known to exist for a $\mathbb{Q}$-rational point on the jacobian of a hyperelliptic curve of genus two over $\mathbb{Q}$. He uses the product of two elliptic curves, one with a seven-torsion point and the other with a ten-torsion point.

Having partial answers for this problem, the natural question to ask is for how large N we should try to search for examples. This motivates the next problem.

Problem. *Let $A_{/K}$ be an abelian variety of dimension g and $P \in A_{tors}(K)$. Does there exist a number $N_0(K, g)$ such that*

$$\operatorname{ord}(P) \leq N_0(K, g)?$$

This problem is a prominent problem in the study of the torsion subgroup of abelian varieties. It is conjectured that such a bound $N_0(K, g)$ exists. There is a uniform version of this conjecture in which the field of definition is not fixed but only the degree of the field extension over the prime field. Again, for elliptic curves the uniform version of this problem is already a theorem by MEREL and OESTERLÉ. For higher dimensional abelian varieties this remains an open problem. But a solution to the previous problem gives at least a lower bound on the number $N_0(K, g)$. For example for $g = 2$ and $K = \mathbb{Q}$,

we know $N_0(\mathbb{Q}, 2) \geq 70$ by a recent result by Howe. For higher dimension g over the rational numbers, it is known that this constant has to be at least $2g^2 + 2g + 1$.

Not only the construction of curves and the search for bounds for possible torsion orders is an interesting task in this area. Also the research on the behavior of the torsion subgroup in families of varieties is of great interest.

Problem. *Given a family of abelian varieties over a field K. Is it possible to determine the fibers with a certain torsion subgroup?*

In this thesis we consider a special one-dimensional family of hyperelliptic curves of genus two. The curves in these family all admit real multiplication in their jacobian. We are able to obtain the following result.

Result. *Let $\lambda \in \mathbb{Q}$, such that $C_\lambda : Y^2 = X^5 - 5X^3 + 5X + \lambda$ is a hyperelliptic curve. Then the following holds.*

1. *If λ is a square,*

$$\mathrm{Jac}(C_\lambda)[2](\mathbb{Q}) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & \text{if } \lambda \in \{0, 1\} \\ \{0\} & \text{else} \end{cases}.$$

2. *There exist only finitely many $\lambda \in \mathbb{Q}$ such that $\mathrm{Jac}(C_\lambda)[3](\mathbb{Q})$ is non-trivial.*

3. $\mathrm{Jac}(C_\lambda)[5](\mathbb{Q}) \cap \{P - P_\infty | P \in C_\lambda(\mathbb{Q})\} = \{0\}$.

It seems hard to find a possibility to determine the torsion structure in a family of abelian varieties in general. Even the determination of the fibers with a three- or five-torsion point involves finding rational solutions in large systems of algebraic equations. The task of finding rational points on varieties is a famous problem and only for very special cases there are algorithms to perform this task. It seems as if other approaches to this problem than the one presented here are needed to deal with this problem.

All these problems remain open but the results of this thesis give tools to make progress and give partial answers in some of these questions.

Outline of the thesis: The thesis is structured in the following way. In the first section we start with generalities about algebraic varieties and schemes. Here we introduce our notation and state some well-known facts about the objects of interest. This section includes the the important results we use in later sections to obtain our results.

In the second section we give the definition and general properties of a moduli space. Furthermore, we describe the construction of analytic spaces parametrizing abelian

varieties of given dimension. Later we try to find examples of abelian varieties with a large torsion subgroup in subspaces of these moduli spaces.

After these two sections of general statements about the objects of interest, the third and fourth section are the central parts of the thesis. The third section deals with the explicit construction of hyperelliptic curves such that there is a point of given order on the jacobian. We introduce different methods to achieve this goal. Central in all the methods is the connection between norm equations in the coordinate ring of the curve and the order of a point of the jacobian.

We present methods going back to Cassels, Flynn, Leprévost and van der Poorten. With these methods and combinations of them we are able to construct unknown examples of hyperelliptic curves with a point of large order on the jacobian. Furthermore, we present an application of Hensel's Lemma to construct series of hyperelliptic curves with a torsion point of prime order. Series of this type were unknown until now.

Using analogies between function fields and number fields we are able to solve norm equations in function fields of degree three by proving the correctness of the Voronoi algorithm in such function fields of characteristic zero.

After considering hyperelliptic curves, we switch to a more general class of curves, namely superelliptic curves. In this class of curves we construct a family with varying genus with a torsion divisor of order linear in the genus. Furthermore, we show that in this case the Hensel lifting approach also works. Following the lines of unit computations in algebraic number fields, we formulate the Voronoi algorithm for cubic function fields of characteristic zero and give a criterion for the periodicity of this algorithm. This relates the computation of units in cubic function fields to non-trivial divisors of finite order. Using the algorithm, we find a family of curves with a function field of degree three with a torsion divisor quadratic in the genus of the curve.

In the fourth section we consider the one-dimensional family of hyperelliptic curves of genus two with real multiplication by $\sqrt{5}$ constructed by Tautz, Top and Verberkmoes. For this family we show that there exist none, finitely many respectively infinitely many members with a $\mathbb{Q}$-rational point of order five, three and two respectively. For order two we consider a subfamily in which we are able to determine all members admitting a $\mathbb{Q}$-rational point of order two on the jacobian.

1. Algebraic Varieties and Schemes

In this chapter we collect some basic properties about algebraic varieties and schemes which we are going to use in the course of this thesis. Most of the definitions and theorems we state without a proof since they can be found in almost every standard book about algebraic geometry, as for example in [Mil11], [Har77], [EH00] or [Mum99]. Algebraic varieties are the central object in this thesis. In section three we construct algebraic varieties with a group structure and point of finite order on them.

Whenever we consider a field in this thesis we assume K to be a perfect field. We start by considering algebraic varieties in general. Afterwards we consider algebraic varieties of dimension one. These are algebraic curves and play a prominent role in section three for the construction of abelian varieties with certain properties. For the definition of moduli spaces we need the notion of schemes first introduced by GROTHENDIECK in [Gro60]. After these generalities we consider abelian varieties and in particular jacobian varieties of algebraic curves.

1.1. General Properties of Algebraic Varieties

Let K be a field and $K[X_1, \ldots, X_n]$ be the polynomial ring in n variables over K. We write $\mathbb{A}^n(K) := K^n$ for the *affine n-space* over K. Given a set of polynomials $S := \{f_1, \ldots, f_m\} \subset K[X_1, \ldots, X_n]$ we can assign a subset $\mathcal{V}(S) \subset K^n$ given by

$$\mathcal{V}(S) := \{x = (x_1, \ldots, x_n) \in K^n \mid f(x) = 0 \text{ for all } f \in S\}.$$

Such a set is called *affine algebraic set*.

Obviously, an element in $\mathcal{V}(S)$ is not only a simultaneous root of all polynomials in the set S but even for all polynomials in the ideal generated by S. So it is enough to look at $\mathcal{V}(I)$ for ideals I in $K[X_1, \ldots, X_n]$.

For a subset $V \subset K^n$ we set

$$\mathcal{I}(V) := \{f \in K[X_1, \ldots, X_n] \mid f(x) = 0 \text{ for all } x \in V\}.$$

Definition 1.1. *Let K be an algebraically closed field and $V \subset \mathbb{A}^n(K)$ an algebraic set. Then we call V* irreducible *or* affine variety *if $\mathcal{I}(V)$ is a prime ideal in $K[X_1, \ldots, X_n]$.*

Definition 1.2. *Let V be an algebraic set over an algebraically closed field K. The ring $\mathcal{O}(V) := {}^{K[X_1,\ldots,X_n]}\!/_{\mathcal{I}(V)}$ is called* coordinate ring *of V.*

The coordinate ring $\mathcal{O}(V)$ of an affine variety V is an integral domain since $\mathcal{I}(V)$ is a prime ideal. So we can make sense of the field of fractions of $\mathcal{O}(V)$. We call this field the *function field* associated to V. We denote this field by $K(V)$.

Definition 1.3. *The* dimension *of an affine variety is defined as the transcendence degree of $K(V)$ over K.*

Example 1.1. *Let $G \in K[X,Y]$ be an irreducible polynomial. Then we call $C := \mathcal{V}(G)$ affine plane curve and the function field of the curve $K(C)$ is given by the field $K(x,y)$ with the relation $G(x,y) = 0$, where x and y are the images of X and Y under the reduction map. So a curve is an affine variety of dimension one.*

For a curve C, we know that the transcendence degree of $K(C)$ over K is one. That means that there exists a transcendental element $x \in K(C)$ such that

$$[K(C) : K(x)] < \infty.$$

In the coordinate ring $\mathcal{O}(V)$ of an affine variety the maximal ideals play an important role. We first assume that K is algebraically closed. Then the maximal ideals of $K[X_1,\ldots,X_n]$ are exactly the ideals of the form $(X_1 - a_1,\ldots,X_n - a_n)$ for some $a_i \in K$. This gives us an one-to-one correspondence between the points $(a_1,\ldots,a_n) \in K^n$ and the maximal ideals in the coordinate ring $K[X_1,\ldots,X_n]$ of $\mathbb{A}^n(K)$. This concept carries over to arbitrary affine varieties V. So we have an one-to-one correspondence between points on V, i.e. $P := (a_1,\ldots,a_n) \in K^n$ such that $f(P) = 0$ for all $f \in \mathcal{I}(V)$, and the maximal ideals of $\mathcal{O}(V)$. We denote the maximal ideal of $\mathcal{O}(V)$ corresponding to the point $P \in V$ by M_P.

Definition 1.4. *Two affine varieties V and W are called* birationally equivalent *if their function fields are isomorphic as fields. If V and W are birationally equivalent varieties, we write $V \cong W$.*

Definition 1.5. *We say that an affine variety V is* defined over a field K*, if there exists an ideal $I \subset K[X_1,\ldots,X_n]$ such that $\mathcal{V}(I) \cong V$. We write $V_{/K}$ for a variety defined over the field K.*

Notation 1.1. *Let L be an algebraic field extension of the field K. Then we denote the set of L-rational points on an affine variety V defined over K by*

$$V(L) := \{P \in V \mid P \in \mathbb{A}^n(L)\} = \{P \in V \mid P^\sigma = P \text{ for all } \sigma \in \mathrm{Gal}(\overline{K}/L)\}.$$

We now introduce the notion of *projective varieties.* Projective varieties are the analog object to affine varieties in the projective space over a field K.

Definition 1.6. *Let K be a field. Then we call the set*

$$\mathbb{P}^n(K) := \{L \subset K^{n+1} \mid L \text{ is an one-dimensional subspace of } K^{n+1}\}$$

the projective n-space *over K.*

If $0 \neq (x_0, \ldots, x_1) =: x$ is an element of K^{n+1}, x defines an one-dimensional vector space by taking the line passing through 0 and $(x_1, \ldots, x_n)$. Two elements $x, x' \in K^{n+1} \setminus \{0\}$ define the same line if and only if there exists $\lambda \in K^*$ such that $x = \lambda x'$. For the element of $\mathbb{P}^n$ given by a point $(x_1, \ldots, x_n) \in K^{n+1}$ we write $[x_0 : \ldots : x_n]$.

Definition 1.7. *A polynomial $G \in K[X_0, \ldots X_n]$ is called* homogeneous *of degree d if for all $\lambda \in K$ and $(x_0, \ldots, x_n) \in K^{n+1}$*

$$G(\lambda x_0, \ldots, \lambda x_n) = \lambda^d G(x_0, \ldots, x_n).$$

For a homogeneous polynomial $G \in K[X_0, \ldots, X_n]$ we can ask whether G vanishes at a point $P \in \mathbb{P}^n$, since if f vanishes at one representative of x it has to vanish at all of them by definition. For an ideal in $K[X_0, \ldots, X_n]$ we say it is homogeneous if it is generated by homogeneous polynomials. So we are able to define projective algebraic sets for homogeneous ideals in $K[X_0, \ldots, X_n]$ and to every subset of $\mathbb{P}^n$ we can assign a homogeneous ideal. So again we are able to talk about irreducibility, coordinate ring and birational equivalence. For the function field we have to take a bit more care. Here we only allow fractions of elements of the coordinate ring which come from polynomials in $K[X_0, \ldots, X_n]$ of the same degree. This ensures that it is possible to evaluate a function at a projective point.

Given an affine variety V we consider its *projective closure*; that is the smallest possible projective variety V^* such that $\phi_i(V) \subset V^*$, where ϕ_i sends $(x_1, \ldots, x_n)$ to $(x_1, \ldots, x_i, 1, x_{i+1}, \ldots, x_n)$ for some $1 \leq i \leq n$. The variety V^* is obtained by considering the zero locus of the ideal generated by the *homogenizations* of the elements in $\mathcal{I}(V)$. The points in $V \setminus V^*$ are called *points at infinity* of V.

Definition 1.8. *Let $G \in K[X_1, \ldots, X_n]$ be a polynomial. Then the* homogenization G^* *of G is defined by*

$$G^* := X_0^{\deg(G)} G\left(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}\right) \in K[X_0, \ldots, X_n].$$

In this thesis we often only consider an affine model of the variety but keep in mind that the objects are projective varieties. Since we often work in the function field of a variety, we mention here that an affine variety and its projective closure have the same function field up to isomorphism.

On a variety V we have even more structure than just the set of points fulfilling the polynomial equations an the coordinate ring V. A variety is always a topological space with the so called Zariski topology.

Definition 1.9 (Zariski Topology on Varieties)**.** *The topology which is defined by the system of closed sets given by the algebraic sets in $\mathbb{A}^n$ (resp. $\mathbb{P}^n$) is called* Zariski topology *of $\mathbb{A}^n$ (resp. $\mathbb{P}^n$). This induces a topology on all algebraic sets in $\mathbb{A}^n$ (resp. $\mathbb{P}^n$).*

Definition 1.10. *Let $U \subset V$ be an open subset of a variety V. Then we set*

$$\mathcal{O}(U) := \bigcap_{P \in U} (\mathcal{O}(V))_{M_P},$$

where M_P is the maximal ideal in $\mathcal{O}(V)$ corresponding to $P \in V$.

The ring $\mathcal{O}(U)$ can be understood as the functions in $K(V)$ that are defined on the whole open subset $U \subset V$.

Definition 1.11. *We say that a variety V is* complete *if for every variety W the projection $V \times W \to W$ maps closed sets to closed sets.*

Definition 1.12. *A variety V over the field K is called* non-singular *at a point $P \in V$ if $\dim_K \left({M_P}/{M_P^2} \right) = \dim(V)$. A variety is called* non-singular *or* smooth *if it is non-singular in every point.*

1.2. Plane Algebraic Curves

1.2.1. Definitions and Basic Properties

Later in this thesis we are interested in algebraic curves. To these curves we can associate higher dimensional varieties which admit a group structure on its points. Therefore, we want to collect some properties of algebraic curves in this section. As already seen, a curve is an one-dimensional algebraic variety. The term *plane* refers to the fact that we are most of the time consider curves in two-dimensional space. So a curve is given by an irreducible polynomial $G \in K[X, Y]$ (resp. homogeneous $G \in K[X_0, X_1, X_2]$). The first step now is to construct a group associated to the curve and later we have the goal to show that this group actually is a variety itself.

Let P be a smooth point on the curve C defined over a field K. Then we assign the localization

$$\mathcal{O}_P(C) := (\mathcal{O}(C))_{M_P}$$

to P. Here M_P is the unique maximal ideal in $\mathcal{O}(C)$ corresponding to P. Since M_P is a maximal ideal, the resulting ring is a local ring with unique maximal ideal M_P. But this means that we have a discrete valuation on the function field $K(C)$ with residue field $\mathcal{O}_P(C)/M_P$, which is an algebraic extension of K. So we have an one-to-one correspondence of valuations on $K(C)$ and points $P \in C$.

Definition 1.13. *Let S be a set. Then we call the free abelian group generated by S the* divisor group *of S,*

$$\mathrm{Div}(S) := \left\{ \sum_{P \in S} a_P P \mid a_P \in \mathbb{Z} \text{ almost all } a_P = 0 \right\}.$$

Definition 1.14. *A divisor $D \in \mathrm{Div}(S)$ is called* effective *if $a_P \geq 0$ for all $P \in S$.*

Such a divisor group $\mathrm{Div}(S)$ can be partially ordered by defining for $D_1, D_2 \in \mathrm{Div}(S)$

$$D_1 \geq D_2 : \Longleftrightarrow \ D_1 - D_2 \text{ is effective.}$$

Definition 1.15. *Let C be a curve defined over the field K and $P \in C$ a point. Then we set*

$$\deg(P) := \left[\mathcal{O}_P(C)/M_P : K \right].$$

This definition could be understood as the minimum of all extension degrees of fields K_P over K such that $P \in C(K_P)$.

So now it is possible to assign a degree to an element of $\sum_{P \in C} a_P P =: D \in \mathrm{Div}(C)$ by setting $\deg(D) := \sum_{P \in C} a_P \deg(P)$. Obviously the divisors of degree zero form a

subgroup of $\mathrm{Div}(C)$ denoted by $\mathrm{Div}_0(C)$.

We are in general interested in those divisors that are defined over the base field. These are exactly those divisors which are invariant under the absolute GALOIS group.

Definition 1.16. *Let C/K be a curve defined over a perfect field K and let $G := \mathrm{Gal}(\overline{K}/K)$ be the absolute* GALOIS *group of K. Then a divisor $D \in \mathrm{Div}(C)$ is called* K-rational *if $D^\sigma = D$ for all $\sigma \in G$.*

For functions in the function field of a curve we make the analogous definition.

Definition 1.17. *Let C/K be a curve defined over the field K and let $G := \mathrm{Gal}(\overline{K}/K)$ be the absolute* GALOIS *group of K. Then a function $f \in \overline{K}(C)$ is called* K-rational *if $f^\sigma = f$ for all $\sigma \in G$. The set of K-rational functions is denoted by $K(C)$.*

Definition 1.18. *Let $D = \sum_{P \in S} a_P P \in \mathrm{Div}(S)$ be a divisor. Then we define the* support *of D by*

$$\mathrm{supp}(D) := \{P \in S | a_P \neq 0\}.$$

For a divisor $D = \sum_{P \in S} a_P P \in \mathrm{Div}(S)$ we sometimes write

$$D = \{\overbrace{P, \ldots, P}^{a_P\text{-times}} | P \in \mathrm{supp}(D)\}.$$

It is possible to assign a *principal divisor* denoted by $\mathrm{div}(f)$ to a non-zero element f of $K(C)$. This divisor has a non-zero coefficient at a point $P \in C$ if and only if P is a pole of f or $f(P) = 0$. If P is a pole of f, a_P is set to the negated order of the pole and if P is a zero of f, a_P is set to the order of the zero. Since for every $f \in K(C)^*$ the number of poles and zeros (counting multiplicity) is equal by [Sti09, Theorem I.4.11], $\mathrm{div}(f) \in \mathrm{Div}_0(C)$. Obviously

$$\mathrm{div}(f) + \mathrm{div}(g) = \mathrm{div}(fg)$$

for all $f, g \in K(C)^*$, so the set of principal divisors is a subgroup of $\mathrm{Div}_0(C)$. This subgroup is denoted by

$$\mathcal{P}(C) := \{\mathrm{div}(f) \mid f \in K(C)^*\}.$$

This observation gives us two important factor groups for a curve C.

Definition 1.19. *Let $C_{/K}$ be a curve defined over K. Then*

$$\mathrm{Pic}(C) := {}^{\mathrm{Div}(C)}\!/_{\mathcal{P}(C)}$$

is called the picard group *of* C *and*

$$\mathrm{Jac}(C) := {}^{\mathrm{Div}_0(C)}\!/_{\mathcal{P}(C)}$$

the jacobian group *of* C.

As we will see later, the jacobian group of a curve is isomorphic to a projective variety which admits a group structure carried over from $\mathrm{Jac}(C)$ by this isomorphism.

Remark. *In general we do not distinguish in the notation between a divisor* D *and the class of the divisor. Both are denoted by* D*. Since most of the time we are interested in the class of the divisors, there is no space for confusion.*

The two definitions of rationality of functions and divisors are closely related as we see in the following proposition.

Proposition 1.1. *Let* C/K *be a curve defined over the perfect field* K *and let* $f \in \overline{K}(C)$ *be a function. Then the following assertions are equivalent.*

1. *There exists a* K*-rational function* $\widetilde{f} \in K(C)$ *such that* $\mathrm{div}(\widetilde{f}) = \mathrm{div}(f)$
2. $\mathrm{div}(f)$ *is a* K*-rational divisor.*

Proof : Let $f \in \overline{K}(C)$ be a K-rational function. Then the set of zeros and the set of poles of f are $\mathrm{Gal}(\overline{K}/K)$-invariant and thus $\mathrm{div}(f)$ is a K-rational divisor.

Let now $\mathrm{div}(f)$ be K-rational. Then $\mathrm{div}(f)$ is $\mathrm{Gal}(\overline{K}/K)$-invariant and thus there exists a function $\widetilde{f}$ such that $\widetilde{f} = \widetilde{f}^{\sigma}$ and $\mathrm{div}(f) = \mathrm{div}(\widetilde{f})$. This proves the statement. □

Given a divisor $D \in \mathrm{Div}(C)$ we can assign a set of functions.

Definition 1.20. *Let* $D \in \mathrm{Div}(C)$ *be a divisor. Then the space*

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

is called Riemann-Roch space *of* D*. This space is in fact a vector space over* K *and we denote its dimension by* $l(D) := \dim_K(\mathcal{L}(D))$.

This dimension is also well defined for divisor classes in $\mathrm{Pic}(C)$, i.e. there exists a canonical isomorphism $\mathcal{L}(D) \cong \mathcal{L}(D')$ as K vector spaces if $D = D' + \mathrm{div}(f)$ for some $f \in K(C)^*$.

We now collect some properties of the Riemann-Roch spaces.

Lemma 1.2. *Let* $D \in \mathrm{Div}(C) \setminus \{0\}$ *be a divisor such that* $-D$ *is effective. Then* $\mathcal{L}(D) = \{0\}$.

Lemma 1.3. *Let $D_1, D_2 \in \mathrm{Div}(C)$ be divisors such that $D_1 \geq D_2$. Then $\mathcal{L}(D_1) \subset \mathcal{L}(D_2)$.*

Theorem 1.4. *Let C/K be an irreducible curve. Then there exists a positive integer $g(C)$, called the* genus of C*, such that for all divisors $D \in \mathrm{Div}(C)$*

$$l(D) \geq \deg(D) - g(C) + 1.$$

Theorem 1.5 (Riemann-Hurwitz Genus Formula)**.** *Let $C/\mathbb{Q}$ be an irreducible plane curve and let $x \in K(C)$ be a transcendental element such that $K(C)/K(x)$ is separable. Then*

$$2g(C) - 2 = \sum_{P \in C} (e(P) - 1) - 2[\mathbb{Q}(C) : \mathbb{Q}(x)],$$

where for a point P the value $e(P)$ is the ramification index of P.

The norm of an element in the function field of an algebraic curve will play an important role throughout this thesis. Solving certain norm equations is equivalent to finding curves defined over a field K with a K-rational point of given order on the jacobian as we see in Section 3.2.

Definition 1.21. *Let K be an algebraically closed field and let C be a smooth plane curve defined over K. Let $x \in K(C)$ be a transcendental element over K such that $K(C)/K(x)$ is separable and set $n := [K(C) : K(x)]$. Then for a function $f \in K(C)$ we define the* norm *by*

$$\mathrm{N}_{K(C)/K(x)}(f) := \prod_{i=0}^{n} \sigma_i(f) \in K(x),$$

where $\sigma_i : K(C) \hookrightarrow \overline{K(x)}$ are the n embeddings of the function fields in the algebraic closure of the rational function field $K(x)$.

Remark. *The norm function is multiplicative.*

1.2.2. Hyperelliptic Curves

Definition 1.22 (Hyperelliptic Curve)**.** *Let C be a non-singular curve of genus $g > 1$ defined over a field K with function field $K(C)$. C is called* hyperelliptic *if there exists $x \in K(C)$ such that $K(C)$ is separable over $K(x)$ and $[K(C) : K(x)] = 2$.*

This means that a hyperelliptic curve C admits a 2-to-1 cover of $\mathbb{P}^1$. The map

$$\iota : C \to C$$

switching the two branches of this cover, is called the *hyperelliptic involution of C* and its ramification points are called Weierstrass-*points*.

Proposition 1.6. *Let $K(C)$ be the function field of a hyperelliptic curve C of genus $g > 1$ defined over a field K of characteristic* $\mathrm{char}(K) \neq 2$. *Then there exist $x, y \in K(C)$ such that $K(C) = K(x, y)$ with $y^2 = F(x)$ for a separable polynomial F of* $\deg(F) = 2g + 1$ *or* $\deg(F) = 2g + 2$.

Proof : See [Sti09, VI.2.3]. □

Using this proposition, we can assume that a hyperelliptic curve C is given by an affine model $C : Y^2 = F(X)$. Assuming we are given a curve $C : Y^2 = F(X)$ and a point $(x(P), y(P)) =: P \in C$, where x and y are the images of X and Y in $K(C)$, then the hyperelliptic involution acts on P by $\iota(P) = (x(P), -y(P))$.

Proposition 1.7. *Let C/K be a hyperelliptic curve of genus g over a field K with* $\mathrm{char}(K) \neq 2$. *Then there exists an affine model $Y^2 = F(X)$ of C defined over K with* $\deg(F) = 2g + 1$ *if and only if C has a K-rational* Weierstrass*-point.*

Proof : Assume the hyperelliptic curve C/K is given by a polynomial F with

$$\deg(F) = 2g + 1.$$

Then the unique point at infinity of the projective closure of C is a K-rational Weierstrass-point.

Assume C/K is given by a polynomial F of degree $2g+2$ such that C has a K-rational Weierstrass-point P. Then this point has coordinates $P = (x(P), 0)$. The affine change of coordinates given by

$$X \mapsto \frac{1}{X - x(P)}, Y \mapsto \frac{Y}{(X - x(P))^{g+1}}$$

gives us an affine model of the desired form. □

In particular, for an algebraically closed field we always have an affine model of a hyperelliptic curve given by a degree $2g + 1$ polynomial.

Let us now take a closer look at the behavior at infinity depending on the degree of the polynomial F. Obviously in both cases we get only the point $(0 : 1 : 0)$ at infinity. In a desingularization two points lie above this point if and only if the degree of F is even. In this case we can construct a non-singular projective model of the curve with two points at infinity. These two points at infinity we denote by P_∞^+ and P_∞^-.

We now consider the case where the genus is equal to two. This gives us a special

divisor D_∞ on our curve C defined by

$$D_\infty := \begin{cases} 2P_\infty & \deg(F) = 5 \\ P_\infty^+ + P_\infty^- & \deg(F) = 6. \end{cases}$$

This divisor D_∞ is always a K-rational divisor even in the case when $\deg(F) = 6$ and the leading coefficient of F is not a square in K and thus the points at infinity are not rational. For the divisor D_∞ and its multiples we often make use of the RIEMANN-ROCH space. The following lemma tells us how this space looks like.

Lemma 1.8. *Let $N \geq 3$ be an integer. Then*

$$\mathcal{L}(ND_\infty) = \langle 1, x, \ldots, x^N, y, xy, \ldots, x^{N-3}y \rangle_K \subset K(C).$$

Remark. *If $N < \deg(F)$, no terms involving y occur since $\deg_\infty(y) = \deg(F)$.*

Proof : First observe that the pole divisor of the function x is given by D_∞ and the pole divisor of y is $\frac{\deg(F)}{2} D_\infty$. By definition, $\mathcal{L}(ND_\infty)$ contains exactly the functions of $K(C)$ that have only poles at infinity with degree bounded by $2N$ since $\deg(D_\infty) = 2$. But polynomials in $x, y \in K(C)$ are the only functions with this property. So counting multiplicities of the pole orders gives us the result. □

This space $\mathcal{L}(ND_\infty)$ is of big importance in the construction of curves admitting a torsion point of order N on the jacobian. For a hyperelliptic curve given by an odd degree polynomial F we can make sense of $\frac{N}{2} D_\infty$ for all N. In this case we get for $N \notin 2\mathbb{Z}$ big enough

$$\mathcal{L}(NP_\infty) = \langle 1, x, \ldots, x^{\frac{N-1}{2}}, y, xy, \ldots, x^{\frac{N-\deg(F)}{2}} y \rangle_K.$$

These considerations for genus two can be generalized to any genus.

Definition 1.23 (The universal hyperelliptic curve of genus g)**.** *Let L be the rational function field in the $2g+3$ indeterminates $f_0, \ldots, f_{2g+2}$ over a field K. The curve C given by*

$$Y^2 = F(X) := \sum_{i=0}^{2g+2} f_i X^i$$

is called the universal hyperelliptic curve *of genus g.*

Note that not every specialization of the universal hyperelliptic curve gives us an hyperelliptic curve over K. Only specializations such that the polynomial F is separable are suitable.

In order to measure whether a specialization of the universal hyperelliptic curve, that is the evaluation of the universal curve at chosen $\widetilde{f_1}, \ldots, \widetilde{f_{2g+2}} \in K$, is indeed a smooth curve we use the discriminant.

Definition 1.24. *Let $C : Y^2 = F(X) = a\prod_{i=1}^{n}(X - \alpha_i)$ be a hyperelliptic curve defined over a field K with* $\mathrm{char}(K) \neq 2$*, $\alpha_i \in \overline{K}$ and $a \in K$. Then we define the* discriminant *of the curve C as*

$$\Delta(C) := 2^{4g}a^{2n-2}\prod_{i<j}(\alpha_i - \alpha_j)^2 \in K.$$

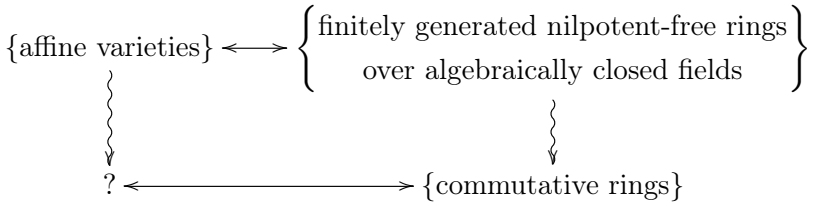
The discriminant is non-zero if and only if the curve C is a smooth curve. If we assume furthermore that C is defined over some local field K with residue characteristic not equal to two and all the coefficients of F are integral in this field, we are able to look at the *reduction* of C modulo the maximal ideal in the ring of integers of K. This reduction is obtained by reducing all the coefficients of F modulo the maximal ideal. Then the reduced curve $\overline{C}$ is a smooth curve of the same genus as C if and only if the discriminant is non-zero modulo the maximal ideal. Often it is possible to get informations about the curve C by looking at its reductions.

Example 1.2. *Let $C/\mathbb{Q}$ be a hyperelliptic curve defined over $\mathbb{Q}$ by an equation $C : Y^2 = F(X)$ with coefficients only lying in $\mathbb{Z}$. Then it is possible to regard C for every prime $p \neq 2$ as a curve over the local field $\mathbb{Q}_p$. The reduction of $C/\mathbb{Q}$ modulo p is then the curve $\overline{C}/\mathbb{F}_p$ given by the same equation as C but every coefficient is reduced modulo p. The resulting curve $\overline{C}/\mathbb{F}_p$ is a hyperelliptic curve if and only if p does not divide $\Delta(C)$.*

Unfortunately, it is not always possible to conclude from local informations about a curve over $\mathbb{Q}_p$ for all p to certain properties of the curve over $\mathbb{Q}$. For example there exist hyperelliptic curves with a $\mathbb{Q}_p$-rational point for every prime p of good reduction and for $\mathbb{Q}_\infty = \mathbb{R}$ but no $\mathbb{Q}$-rational points. But if we find a prime p of good reduction such that a hyperelliptic curve has no p-adic points, we can conclude that there exist no points over $\mathbb{Q}$ since $\mathbb{Q}$ can be regarded as a subfield of $\mathbb{Q}_p$ for all p.

1.3. Schemes

In this chapter we introduce some of the terminology of schemes which we use in later chapters to give the precise notion of moduli spaces. We follow the lines of the book by Eisenbud and Harris [EH00]. Schemes are the natural generalization of algebraic varieties. While in the case of algebraic varieties we consider polynomial rings modulo some radical ideal, the vanishing ideal of the points of the variety, we now want to look at a more general class of rings. If we start with a polynomial ring in finitely many indeterminates over an algebraically closed field and factor out some radical ideal, we obtain a finitely generated nilpotent-free ring. We have seen that these rings correspond one-to-one to affine algebraic varieties. We now want to allow on the side of rings all commutative rings and look for the corresponding geometric objects. That is, our aim is to complete the following diagram.



We will see that affine schemes are the objects that fit into this diagram.

1.3.1. Affine Schemes

Definition 1.25. *Let R be a commutative ring. Then we define the* spectrum *of R as*

$$\mathrm{Spec}(R) := \{I \mid I \text{ prime ideal of } R\}.$$

This set of prime ideals of a given ring R admits a topology which we define in terms of its closed sets.

Definition 1.26. *Let $S \subset R$ be a subset of the commutative ring R then we set*

$$\mathcal{V}(S) := \{I \in \mathrm{Spec}(R) \mid S \subset I\}.$$

This definition is close to the definition of algebraic sets in section 1.1, where we started with a polynomial ring $R = K[X_1, \ldots, X_n]$ over an algebraically closed field K and took a set of polynomials S. For such a set we looked at points in the affine space $\mathbb{A}^n$ that are zeros for all elements in S. But the points of $\mathbb{A}^n$ correspond exactly to the ideals $(X_1 - a_1, \ldots, X_n - a_n)$ which are for an algebraically closed field exactly the

maximal ideals in R. So $\mathbb{A}^n = \mathrm{Spec}(R) \setminus \{(0)\}$ and for an element I being a root of a polynomial in S just means $S \subset I$ as in the definition above.

Definition 1.27 (Zariski Topology)**.** *We define the closed sets in the* Zariski topology *as the sets $\mathcal{V}(S)$ for subsets $S \subset R$ of the ring R.*

Remark. *Obviously the sets of the form $\mathcal{V}(S)$ for $S \subset R$ are closed under arbitrary intersections. Therefore, this gives us indeed a topology on* $\mathrm{Spec}(R)$*.*

So we now have made $\mathrm{Spec}(R)$ into a topological space. The last thing which is missing to make it the corresponding structure to varieties is the existence of a structure sheaf, that is, to assign a ring to all open subsets of $\mathrm{Spec}(R)$. In the case of varieties we had that the coordinate ring was assigned to the whole variety and for each open subset we assigned localizations of the coordinate ring.

So we have constructed with $\mathrm{Spec}(R)$, its topology and its structure sheaf the analogue of affine varieties.

Example 1.3. *Let $\mathcal{O}(V)$ be the coordinate ring of an affine variety V over an algebraically closed field K. Then $\mathcal{V} := \mathrm{Spec}(\mathcal{O}(V))$ consists of an ideal for each of the points in $V(K)$ and one extra element (0), the* generic point *of V. Note that (0) is indeed prime in $\mathcal{O}(V)$ since V is assumed to be an affine variety and this implies that $\mathcal{O}(V)$ is an integral domain. The structure sheaf on $\mathcal{V}$ assigns to the whole variety the ring $\mathcal{O}(V)$ and to each open subset U of $\mathcal{V}$ the intersection of all local rings of the points in U.*

Definition 1.28. *Let X be an affine scheme. Then the* dimension *of X is the supremum of the* Krull *dimensions of of all local rings.*

Definition 1.29. *Let X, Y be affine schemes. A continuous map $\phi : X \to Y$ is called* morphism of schemes *if the pullback of ϕ is a homomorphism of the underlying rings.*

An enlightening example for the way affine schemes generalize the ideas of varieties is to look at an one-dimensional scheme. Let us start with the ring $\mathbb{Z}$. Then $\mathrm{Spec}(\mathbb{Z})$ is the set of primes together with the generic point coming from the zero ideal. Further take a quadratic extension $K = \mathbb{Q}(\alpha)$ of $\mathbb{Q}$ and look at the ring of integers $\mathcal{O}_K$. Obviously we have $\mathbb{Z} \subset \mathcal{O}_K$, therefore, we get a map $\mathrm{Spec}(\mathcal{O}_K) \to \mathrm{Spec}(\mathbb{Z})$ which is $2:1$ except for the ramified and inert primes in $\mathcal{O}_K$.

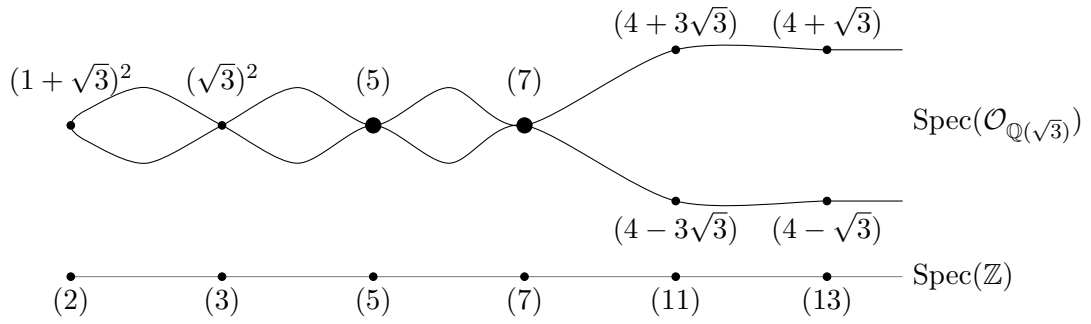


Figure 1.1.: *The scheme* $\mathrm{Spec}\left(\mathcal{O}_{\mathbb{Q}(\sqrt{3})}\right)$ *over* $\mathrm{Spec}(\mathbb{Z})$

1.3.2. Schemes in General

Definition 1.30. *Let X be a topological space. A* sheaf of sets (rings, modules, etc.) *$\mathcal{O}$ on X is a map that assigns to every open subset $U \subset X$ a set (ring, module, etc.) $\mathcal{O}(U)$ together with restriction maps of sets (rings, modules, etc.) for a chain of nested sets $U \subset V \subset W \subset X$*

$$\mathrm{res}_{V,U} : \mathcal{O}(V) \to \mathcal{O}(U)$$

such that $\mathrm{res}_{U,U} = \mathrm{id}$ and $\mathrm{res}_{W,U} = \mathrm{res}_{V,U} \circ \mathrm{res}_{W,V}$. Furthermore, local data on an open covering of an open subset of X should lift uniquely to data on the whole subset. That is, given an open covering U_i of $U \subset X$ and elements $f_i \in \mathcal{O}(U_i)$ fulfilling

$$\mathrm{res}_{U_i,U_i\cap U_j}(f_i) = \mathrm{res}_{U_j,U_i\cap U_j}(f_j),$$

then there exists an unique element $f \in \mathcal{O}(U)$ such that $\mathrm{res}_{U,U_i}(f) = f_i$ for all i.

Remark. *The above mentioned* structure sheaf *of an affine variety is indeed a sheaf of rings.*

Now we have collected enough data to define schemes in general. The idea is to allow any topological space with a sheaf on it, such that it is locally an affine scheme.

Definition 1.31. *Let X be a topological space with a sheaf $\mathcal{O}$ on it. If there is an open covering U_i of X such that U_i with the restriction of $\mathcal{O}$ to U_i is isomorphic to an affine scheme, then X is called a* scheme.

Every open subset of a scheme is again a scheme. For affine schemes the elements I of $\mathrm{Spec}(R)$ are exactly the closed subschemes of $\mathrm{Spec}(R)$ by taking the scheme $\mathrm{Spec}\left({}^{R}\!/_{I}\right)$ and regard it as a subscheme by the inclusion map of schemes coming from the projection $R \twoheadrightarrow {}^{R}\!/_{I}$.

Definition 1.32. *Let X be a scheme. Then we assign to X the* functor of points *given by*

$$\begin{aligned} h_X : \quad (schemes)^\circ &\longrightarrow (sets) \\ S &\longmapsto \mathrm{Mor}(S, X) \end{aligned}$$

on objects and sending a morphism $f : S \to Z$ to the map $h_X(Z) \to h_X(Y)$ which sends $g \in h_X(Z)$ to $g \circ f \in h_X(Y)$.

For a category $\mathcal{C}$ we write $\mathcal{C}^\circ$ for the opposite category*, that is the category consisting of the same objects as $\mathcal{C}$, but all morphisms go in the opposite direction. That is, for all $X, Y \in \mathcal{C}$ we have $\mathrm{Mor}_{\mathcal{C}^\circ}(X, Y) = \mathrm{Mor}_{\mathcal{C}}(Y, X)$.*

Example 1.4. *Let V be an algebraic variety defined over the field K. Then*

$$h_V(\mathrm{Spec}(K)) = \mathrm{Mor}(\mathrm{Spec}(K), V)$$

is just the set of K-valued points of V.

Definition 1.33 (Natural Transformation)**.** *Let $F, G : \mathcal{C} \to \mathcal{C}'$ be two functors. Then a* natural transformation *t from F to G is a collection of morphisms*

$$\{t_X : F(X) \to G(X)\}_{X \in \mathcal{C}}$$

in $\mathcal{C}'$ such that for every morphism $\phi \in \mathrm{Mor}_{\mathcal{C}}(X, Y)$ the diagram

$$\begin{array}{ccc} F(X) & \xrightarrow{t_X} & G(X) \\ {\scriptstyle F(\phi)}\downarrow & & \downarrow{\scriptstyle G(\phi)} \\ F(Y) & \xrightarrow[t_Y]{} & G(Y) \end{array}$$

commutes.

Definition 1.34 (Representablity)**.** *Let $\mathcal{F} : \mathcal{C} \to \mathcal{C}'$ be a functor of categories. Then $\mathcal{F}$ is called* representable *if there exists an object $C \in \mathcal{C}$ such that $\mathcal{F} = h_C := \mathrm{Mor}(\,\cdot\,, C)$.*

By the Yoneda Lemma, the object representing a functor is unique up to unique isomorphism.

1.4. Abelian Varieties and Jacobians

1.4.1. Definitions and Basic Properties

After having collected some basic facts about varieties and schemes in the last sections, we now want to focus to a special class of varieties. The varieties we want to consider have the additional structure of an algebraic group.

Definition 1.35. *An algebraic variety V/K defined over a field K with morphisms*

$$inv : V \to V, m : V \times V \to V$$

and an element $\mathcal{O} \in V(K)$ is called group variety *if these morphisms supply $V(\overline{K})$ with the structure of a group with identity element $\mathcal{O}$.*

Definition 1.36. *Let V be a group variety. If V is complete, V is called* abelian variety*.*

Definition 1.37. *A homomorphism of abelian varieties $\phi : A \to B$ is called* isogeny *if it is surjective and has a finite kernel.*

In this thesis we are in particular interested in certain subgroups of abelian varieties, namely the torsion subgroups. First of all we want to restrict ourselfs to K-rational points, where K is the field of definition of an abelian variety.

Proposition 1.9 (Mordell-Weil,[Wei29])**.** *Let K be a number field and A/K an abelian variety defined over K. Then*

$$A(K) \cong A_{tors}(K) \times \mathbb{Z}^r,$$

where $r \in \mathbb{N}_0$ is called the rank *and $A_{tors}(K)$ is a finite group called the K-*rational torsion subgroup *of A.*

We are mainly interested in the torsion part of the K-rational points and most of the time $K = \mathbb{Q}$ or a number field.

Definition 1.38. *Let A be an abelian variety and $N \in \mathbb{N}$ a positive integer. Then we call*

$$A[N] := \{P \in A | NP = \mathcal{O}\}$$

*the N-*division points *of A. We say $P \in A$ is an N-*torsion point *or a* point of order N *if $P \in A[N]$ and for all $N' < N$, $P \notin A[N']$.*

More generally, if we have an isogeny $\phi : A \to A'$ between abelian varieties A, A', we set $A[\phi] := \ker(\phi)$. Since the multiplication-by-N-map is a morphism with finite kernel and thus an isogeny from A to itself, this notation is consistent with the definition above.

Important examples for abelian varieties are the jacobian varieties of curves.

Theorem 1.10. *Let C be a smooth projective curve of genus g over a field K. Then there exists an abelian variety J of dimension g such that for every separable extension L of K the set of L-rational points on J can be naturally identified with* $\mathrm{Jac}(C)^{\mathrm{Gal}(\overline{K}/L)}$.

In order to prove this theorem, we consider the equivalence classes of degree zero divisors on C. For this purpose we define special divisors which turns out to be very important to describe the group $\mathrm{Jac}(C)$.

Definition 1.39. *Let C be a hyperelliptic curve of genus g defined over the field K and let P_∞ be a K-rational* Weierstrass *point. A divisor D of degree zero is called* semi-reduced divisor *if $D = \sum_{P \in C \setminus P_\infty} a_P P - \left(\sum_{P \in C \setminus P_\infty} a_P\right) P_\infty$ with*

1. *for all P: $a_P \geq 0$,*
2. *$a_P > 0$ implies $a_{\iota(P)} = 0$ for all non-*Weierstrass*-points, and*
3. *$a_P \leq 1$ for all* Weierstrass*-points P.*

If $\sum_{P \in C \setminus P_\infty} a_P \leq g$, we call D a reduced divisor.

Lemma 1.11 ([CFA+05])**.** *Let C/K be a smooth, projective curve of genus g, P_0 a fixed K-rational point on C and $\overline{D}$ a K-rational divisor class in* $\mathrm{Jac}(C)$*. Then there exists an effective divisor A of degree* $\deg(A) = g$ *such that $A - gP_0 \in \overline{D}$.*

Proof : Write $\widetilde{D} \in \overline{D}$ as the difference of its zero divisor $\widetilde{D}_+$ and pole divisor $\widetilde{D}_-$. These are both effective divisors of the same degree. Looking at the divisor $S := -\widetilde{D}_- + kP_0$, we know by the Riemann-Roch-Theorem 1.4 that for k big enough, namely $k > \deg(\widetilde{D}_-) + g$, we have $l(S) > 1$ and so there exists a function $f \in \overline{K}(C)$ such that $S + \mathrm{div}(f)$ is effective. This shows that we can replace $\widetilde{D}$ by a divisor of the form $\widetilde{D} - \deg(\widetilde{D})P_0$ with $\widetilde{D}$ effective. If $\deg(\widetilde{D}) \leq g$ we are done. If $\deg(\widetilde{D})$ is bigger then g, we can again use the Riemann-Roch-Theorem to find a function $f \in \overline{K}(C)$ such that $\widetilde{D} - (\deg(\widetilde{D}) - g)P_0$ is effective. This gives us a divisor of the desired form. □

With this lemma we get that in every divisor class D of a hyperelliptic curve C there exist a unique reduced divisor representing the same divisor class as the divisor D. We use this fact to give $\mathrm{Jac}(C)$ the structure of a projective variety.

Idea of the proof of Theorem 1.10: Let C/K be a hyperelliptic curve of genus g and consider the symmetric g-th power $C^{(g)}$ of C. The elements in $C^{(g)}$ are unordered tupels of points of the curve C. By [Mil08, Ch. III,Prop. 3.2] this is a non-singular algebraic variety of dimension g. Let $\{P_1, \ldots, P_g\}$ be a L-rational point on $C^{(g)}$ for some field

$K \subset L \subset \overline{K}$. This means $\{P_1, \ldots, P_g\}$ is invariant under the action of $G := \mathrm{Gal}(\overline{K}/L)$. But this is only possible if for any $\sigma \in G$ the action of σ on $\{P_1, \ldots, P_g\}$ is just a permutation of the P_i. This fact just means that $\{P_1, \ldots, P_g\}$ corresponds to a L-rational divisor D of C with $\deg(D) = g$. Since in each divisor class of C there exists a unique reduced divisor due to Lemma 1.11, this sets up a bijection between the points of $C^{(g)}$ and $\mathrm{Jac}(C)$. So $\mathrm{Jac}(C)$ is in fact an algebraic variety. □

Definition 1.40. *Let C/K be a hyperelliptic curve and $P \in C(K)$ a K-rational point. Then we define the* Albanese map *with respect to P as*

$$\begin{array}{rccc} \Phi_P : & C & \longrightarrow & \mathrm{Jac}(C) \\ & Q & \longmapsto & Q - P \end{array} .$$

Proposition 1.12. *The* Albanese *map is injective.*

Proof : Let C/K be a hyperelliptic curve of genus $g > 1$ and P a K-rational point on C. Assume there are points $P_1 \neq P_2 \in C$ such that

$$\Phi_P(P_1) = \Phi_P(P_2).$$

Then there exist a function $f \in K(C)$ such that $\mathrm{div}(f) = P_1 - P_2$. But this implies $g(C) = 0$, which can not hold by assumption. □

1.4.2. Different Representations for Points on the Jacobian

We have already seen two important representations of points on the jacobian. The first is the description as elements of the factor group $\mathrm{Jac}(C) = {}^{\mathrm{Div}_0(C)}\!/_{\mathcal{P}(C)}$. The second description is given by unordered g-tuples of points on the curve. The third description is given by the fact, that $\mathrm{Jac}(C)$ is defined by some equations in $\mathbb{P}^n$ for some n (c.f. Section 1.4.3). So the points on $\mathrm{Jac}(C)$ can be given by the coordinates in $\mathbb{P}^n$. With this description it is not easy to do computations on $\mathrm{Jac}(C)$, so most of the time we do not use it.

In this chapter we want to introduce one further representation called the MUMFORD representation. This representation of points on the jacobian of a curve is directly linked to the description with unordered g-tuples of points on the curve.

Definition 1.41 ([Mum84])**.** *Let $C/K : Y^2 = F(X)$ be a hyperelliptic curve of genus g defined over the field K with a K-rational point P_∞. Let $D := \sum_{i=1}^{s} P_i - sP_\infty$ be a reduced divisor on C. Then the* MUMFORD representation *(u, v) of D is given by*

$$u(x) := \prod_{i=1}^{s}(x - x(P_i)) \in K[x] \text{ and}$$
$$v(x(P_i)) = y(P_i) \text{ for } i = 1, \ldots, s,$$

such that $v \in K[x]$, $\deg(v) < \deg(u)$ and $u \mid (v^2 - F)$.

Theorem 1.13. *The* MUMFORD *representation of a point on the jacobian of a genus g hyperelliptic curve is unique.*

The proof can be found in [Mum84].

Lemma 1.14. *Let C/K be an hyperelliptic curve with $C(K) \neq \emptyset$ and D a point on $\mathrm{Jac}(C)$. Then D is a K-rational point if and only if $u, v \in K[x]$.*

The proof can be found in [Mum84].

This representation is used by a lot of computer algebra systems for computations because the algorithm by CANTOR described in the next section uses this representation and can compute the sum of two points on the jacobian very fast.

1.4.3. Embeddings of $\mathrm{Jac}(C)$ in Projective Space

Since the jacobian variety of a curve is a projective variety, there exists an embedding of $\mathrm{Jac}(C)$ in $\mathbb{P}^n$ for some natural number n such that the image is given by the zero locus of a set of homogeneous polynomials. Such an embedding in $\mathbb{P}^{15}$ of the jacobian of the universal hyperelliptic curve was explicitly constructed by Flynn in [Fly93]. He starts with a hyperelliptic curve C given by a polynomial of degree six defined over a field K with $\mathrm{char}(K) \neq 2, 3, 5$. Thus we have two different points at infinity, which we denote as usual with P_∞^+ and P_∞^-. This gives us two possibilities to embed the curve into the jacobian. We denote the images by Θ^+ and Θ^-. By Lefschetz, a basis of $\mathcal{L}(2(\Theta^+ + \Theta^-))$ gives the desired embedding of the jacobian into projective space [Lan82, Thm. 6.1].

Set

$$\begin{aligned}
F_0(x_1,x_2) := \quad & 2f_0 + f_1(x_1+x_2) + 2f_2x_1x_2 + f_3x_1x_2(x_1+x_2) \\
& + 2f_4x_1^2x_2^2 + f_5x_1^2x_2^2(x_1+x_2) + 2f_6x_1^3x_2^3 \\
F_1(x_1,x_2) := \quad & f_0(x_1+x_2) + 2f_1x_1x_2 + f_2x_1x_2(x_1+x_2) + 2f_3x_1^2x_2^2 \\
& + f_4x_1^2x_2^2(x_1+x_2) + 2f_5x_1^3x_2^3 + f_6x_1^3x_2^3(x_1+x_2) \\
G_0(x_1,x_2) := \quad & 4f_0 + f_1(x_1+3x_2) + 2f_2(x_1x_2+x_2^2) + f_3(3x_1x_2^2+x_2^3) \\
& + 4f_4x_1x_2^3 + f_5(x_1^2x_2^3+3x_1x_2^4) + 2f_6(x_1^2x_2^4+x_1x_2^5) \\
G_1(x_1,x_2) := \quad & 2f_0(x_1+x_2) + f_1(3x_1x_2+x_2^2) + 4f_2x_1x_2^2 + f_3(x_1^2x_2^2+3x_1x_2^3) \\
& + 2f_4(x_1^2x_2^3+x_1x_2^4) + f_5(3x_1x_2^4+x_1x_2^5) + 4f_6x_1^2x_2^5.
\end{aligned}$$

Lemma 1.15. *A basis of $\mathcal{L}(2(\Theta^+ + \Theta^-))$ is given by the following 16 functions.*

$$\begin{aligned}
a_{15} &:= 1 & a_{14} &:= x_1 + x_2 \\
a_{13} &:= x_1x_2 & a_{12} &:= x_1^2 + x_2^2 \\
a_{11} &:= x_1x_2(x_1+x_2) & a_{10} &:= (x_1x_2)^2 \\
a_9 &:= \frac{y_1-y_2}{x_1-x_2} & a_8 &:= \frac{x_2y_1-x_1y_2}{x_1-x_2} \\
a_7 &:= \frac{x_2^2y_1-x_1^2y_2}{x_1-x_2} & a_6 &:= \frac{x_2^3y_1-x_1^3y_2}{x_1-x_2} \\
a_5 &:= \frac{F_0(x_1,x_2)-2y_1y_2}{(x_1-x_2)^2} & a_4 &:= \frac{F_1(x_1,x_2)-(x_1+x_2)y_1y_2}{(x_1-x_2)^2} \\
a_3 &:= x_1x_2a_5 & a_2 &:= \frac{G_0(x_1,x_2)y_1-G_0(x_2,x_1)y_2}{(x_1-x_2)^3} \\
a_1 &:= \frac{G_1(x_1,x_2)y_1-G_1(x_2,x_1)y_2}{(x_1-x_2)^3} & a_0 &:= a_5^2,
\end{aligned}$$

where x_1, x_2, y_1, y_2 are the images of the coordinates of the two images of the curve and $f_0, \ldots, f_6$ are the coefficients of the defining polynomial of the curve.

With this basis we want to construct a map $\mathrm{Jac} : C^{(2)} \hookrightarrow \mathbb{P}^{15}$.

Definition 1.42. *Define for an element $D := \{(x_1, y_1), (x_2, y_2)\}$ of $C^{(2)}$*

$$\mathrm{Jac}(D) := (a_0, \ldots, a_{15})$$

and $\mathrm{Jac}(\mathcal{O}) := (1, 0, \ldots, 0)$, where $\mathcal{O}$ denotes all pairs $\{P, \iota(P)\}$ with $P \in C$.

With this definition of the map Jac we get $\mathrm{Jac}(C)$ as a projective variety defined over K given by 72 quadratic forms written out in [Fly93].

Using this embedding, it is possible to write down formulae for the addition of two points of $\mathrm{Jac}(C)$. These formulae are quite complicated and can be found in [Fly93].

1.4.4. The Kummer Variety

In this chapter we discuss a special variety associated with a hyperelliptic curve. We can consider the quotient of $\mathrm{Jac}(C)$ by the multiplication-by-(-1)-map, that is, we identify each point on $\mathrm{Jac}(C)$ with its inverse under the group law of $\mathrm{Jac}(C)$. Obviously, we destroy some of the structure of $\mathrm{Jac}(C)$, but some other parts of the structure, which are used in a lot of applications, are preserved. The remaining parts of the structure we use to examine the three torsion subgroup of a certain family of jacobians of hyperelliptic curves of genus two. In this section we follow [Fly93].

Definition 1.43. *Let A be an abelian variety. Then*

$$\mathcal{K}(A) := {}^{A}\!/_{\pm}$$

is called the Kummer variety *associated to A. We denote the factor map by κ.*

Obviously, we get ramification exactly at the two-torsion points of A since these are the fixed points of the map $P \mapsto -P$.

On the Kummer variety it is no longer possible to define a group law, but one can define a pseudo-addition on it. First we observe that some operations are well defined on the Kummer variety. If we want to add the images of two points $\kappa(P)$ and $\kappa(Q)$ on the Kummer variety, it is possible to take $\kappa(P+Q), \kappa(-P+Q), \kappa(-P-Q)$ or $\kappa(P-Q)$ as the sum of $\kappa(P)$ and $\kappa(Q)$. But if one of the points is a two-torsion point on A, the images $\kappa(\pm P \pm Q)$ are all the same. So the addition of a two-torsion point is well defined on the Kummer variety. And since the *multiplication-by-N-map* commutes with taking the inverse of a point $\pm NP = N(\pm P)$, we obtain a well defined map $\delta_N(P) := \kappa(NP)$ on $\mathcal{K}(A)$. In [Fly93] Flynn gives explicit formulae for doubling a point on the Kummer surface of the jacobian of a hyperelliptic curve of genus two which can be found in Appendix B.

We consider now a hyperelliptic curve C of genus two. Then we have seen that there exists an embedding of $\mathrm{Jac}(C)$ into $\mathbb{P}^{15}$ as an abelian variety. Since the equations for $\mathrm{Jac}(C) \subset \mathbb{P}^{15}$ are not easy to handle and it is very hard to compute a multiple of a given point on it, it would be nice to use the slightly more simple object $\mathcal{K}(\mathrm{Jac}(C))$ for some computations. The next theorem justifies the term "slightly more simple".

Theorem 1.16. *Let C be a hyperelliptic curve of genus two defined over a field K of characteristic not equal to $2, 3$ or 5. Then there is an embedding*

$$\mathcal{K}(\mathrm{Jac}(C)) \hookrightarrow \mathbb{P}^3.$$

Proof : The proof can be found in [CF96]. □

Now we give a short description of the construction of the KUMMER surface of a genus two hyperelliptic curve following the lines of [Fly93]. The idea is to look at the basis $\mathcal{B} := \{a_0, \ldots, a_{15}\}$ of $\mathcal{L}(2(\Theta^+ + \Theta^-))$ and consider the functions $f \in \mathcal{B}$ such that $f(P) = f(-P)$ for all $P \in \mathrm{Jac}(A)$. We call these functions *even* functions. There are exactly ten even functions in the basis above. Four of these functions give us an embedding into $\mathbb{P}^3$ whose image is our desired KUMMER surface.

Lemma 1.17 ([Fly93, §2])**.** *The following functions give an embedding* $\mathcal{K}(\mathrm{Jac}(C)) \hookrightarrow \mathbb{P}^3$*:*

$$\begin{aligned} a_{15} &= 1, \\ a_{14} &= x_1 + x_2, \\ a_{13} &= x_1 x_2 \text{ and} \\ a_5 &= \frac{F_0(x_1, x_2) - 2y_1 y_2}{(x_1 - x_2)^2}. \end{aligned}$$

With this embedding into $\mathbb{P}^3$ the KUMMER surface in $\mathbb{P}^3$ is given by the following equations.

Proposition 1.18. *The functions* a_{15}, a_{14}, a_{13} *and* a_5 *fulfill the relation*

$$R(a_{15}, a_{14}, a_{13})a_5^2 + S(a_{15}, a_{14}, a_{13})a_5 + T(a_{15}, a_{14}, a_{13}) = 0,$$

where $R, S, T \in \mathbb{Z}[X, Y, Z]$ *are given by*

$$\begin{aligned} R :=& Y^2 - 4XZ \\ S :=& -2(2f_0X^3 + f_1X^2Y + 2f_2X^2Z + f_3XYZ + 2f_4XZ^2 + f_5YZ^2 + 2f_6Z^3) \\ T :=& (f_1^2 - 4f_0f_2)X^4 - 4f_0f_3X^3Y - 2f_1f_3X^3Z - 4f_0f_4X^2Y^2 + (4f_0f_5 - 4f_1f)X^2YZ \\ &+ (2f_1f_5 - 4f_0f_6 - 4f_2f_4 + f_3^2)X^2Z^2 - 4f_0f_5XY^3 + (8f_0f_6 - 4f_1f_5)XY^2Z \\ &+ (4f_1f_6 - 4f_2f_5)XYZ^2 - 2f_3f_5XZ^3 - 4f_0f_6Y^4 - 4f_1f_6Y^3Z - 4f_2f_6Y^2Z^2 \\ &- 4f_3f_6YZ^3 + (f_5^2 - 4f_4f_6)Z^4. \end{aligned}$$

As mentioned above, it is possible for all $N \in \mathbb{Z}$ to give a function δ_N on $\mathcal{K}(\mathrm{Jac}(C))$ such that the following diagram commutes:

$$\begin{array}{ccc} \mathrm{Jac}(C) & \xrightarrow{[N]} & \mathrm{Jac}(C) \\ \downarrow{\scriptstyle \kappa} & & \downarrow{\scriptstyle \kappa} \\ \mathcal{K}(\mathrm{Jac}(C)) & \xrightarrow[\delta_N]{} & \mathcal{K}(\mathrm{Jac}(C)) \end{array}$$

For $N = 2$ it is feasible to give equations for δ_2. These can be found in Appendix B.

If the curve is given by an equation $Y^2 + H(X)Y = F(X)$ with $\deg(H) \leq 3$ and $\deg(H) \leq 6$, a description of the KUMMER surface is given in [Mül10].

We use this description of the KUMMER surface and the map δ_2 to examine a one-dimensional family of hyperelliptic curves and compute conditions on the parameters such that there exist a $\mathbb{Q}$-rational three torsion point on the jacobian. Using the explicit formulae for the duplication on the KUMMER surface, we determine the points on the jacobian of the hyperelliptic curve which are invariant under the multiplication-by-two map.

In the next section we describe an algorithm for point addition on the jacobian of a hyperelliptic curve.

1.4.5. Pointaddition in $\mathrm{Jac}(C)$

In this section we present an algorithm for computing point addition on jacobians of hyperelliptic curves. Since we are mainly interested in the group structure of these jacobian varieties this algorithm is of great importance to study this object.

The algorithm we want to present is due to CANTOR [Can87]. It takes as input two points on the jacobian given in MUMFORD representation and has as output the MUMFORD representation of the sum of the two points. We do not prove the correctness of the algorithm. The proof can be found in [Can87].

Let us first look at the addition on the side of reduced divisors on a genus two hyperelliptic curve C defined over a field K with $\mathrm{char}(K) \neq 2, 3$ given by an equation

$$C : Y^2 = F(X).$$

Let $D_1 := P_1 + Q_1 - D_\infty$ and $D_2 := P_2 + Q_2 - D_\infty$ be the two divisors we want to add. Then we have to take care of two possible cases. In the first case for all $P \in \mathrm{supp}(D_1)$ the hyperelliptic involution $\iota(P)$ of P is not in the support of D_2. Then

$$D_3 := D_1 + D_2 = P_1 + P_2 + Q_1 + Q_2 - 2D_\infty$$

is a semireduced divisor. In the second case we have for P the relation

$$P + \iota(P) - D_\infty = \mathrm{div}(x - x(P)),$$

therefore, we can cancel out P and $\iota(P)$ against each other in $D_1 + D_2$.

The next step is now to find a reduced divisor $\widetilde{D_3} := P_3 + Q_3 - D_\infty$ which is equivalent to D_3. To solve this problem we have to find a function $f \in K(C)$ such that f has zeros exactly at the points P_i and Q_i for $i = 1, 2, 3$. f can be given by $f := y - a(x)$ with $a \in K[X]$ is of degree three. This is true since such an f is uniquely determined by the points P_1, P_2, Q_1 and Q_2 and intersects C in exactly two more points $\iota(P_3), \iota(Q_3)$ by the Theorem of NOETHER. This gives us

$$\mathrm{div}(f) = P_1 + Q_1 + P_2 + Q_2 + \iota(P_3) + \iota(Q_3) - 3D_\infty.$$

Therefore, the hyperelliptic involutions of these two intersection points give us the divisor D_3. This procedure is visualized in Figure 1.2.

Let now D_1 and D_2 be two reduced divisors given in MUMFORD representation by polynomials u_i and v_i, $i = 1, 2$. First we want to compose these divisors to a semireduced divisor representing the divisor class of $D_1 + D_2$. And afterwards we want to reduce this new divisor to the unique reduced divisor in the class.

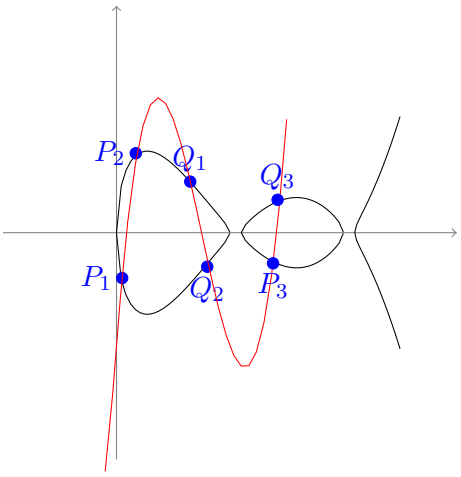


Figure 1.2.: *Geometric description of the point addition in* $\mathrm{Jac}(C)$ *over* $\mathbb{R}$ *for* $C : Y^2 = X(X-1)(X-1.1)(X-2)(X-2.1)$. *We have the relation* $(P_1 + Q_1 - 2P_\infty) + (P_2 + Q_2 - 2P_\infty) = -(P_3 + Q_3 - 2P_\infty)$.

Following the composition step in the case of divisors, we want to have the u-coordinate in Mumford representation to be the product of the u-coordinates of D_1 and D_2 but cancel out the factors coming from points $P \in \mathrm{supp}(D_1)$ such that $\iota(P) \in \mathrm{supp}(D_2)$. Obviously, such a point gives rise to a common factor of u_1 and u_2. Therefore, we have $x - x(P) \mid \gcd(u_1, u_2)$. If there is a point $P \in \mathrm{supp}(D_1) \cap \mathrm{supp}(D2)$, we get $x - x(P) \mid \gcd(u_1, u_2)$. Using the v-coordinate of D_1 and D_2, we get for a point P with $\gcd(u_1, u_2)(x(P)) = 0$ that $\iota(P) \in \mathrm{supp}(D_2)$ if and only if $(v_1 + v_2)(x(P)) = 0$. Therefore, the points we have to cancel out to get a semireduced divisor are exactly the points such that $\gcd(u_1, u_2, v_1 + v_2)(x(P)) = 0$. Therefore, we can set

$$u_3 := \frac{u_1 u_2}{\gcd(u_1, u_2, v_1 + v_2)^2}$$

to get the u-coordinate of a semireduced divisor in the class of $D_1 + D_2$. The square comes from the fact that we want to cancel out the factor coming from P as well as the factor coming from $\iota(P)$.

For the v coordinate of the semireduced divisor we want to construct, we need a polynomial v_3 with degree less then the degree of u_3 and the property $v_3(x(P)) = y(P)$ for all P in the support of the reduced divisor.

So at this point we are able to get a Mumford representation of a semireduced divisor representing the sum of two semireduced divisors. We now want to give an algorithm that takes as input a Mumford representation of a semireduced divisor and returns the representation of the unique reduced divisor in the same class.

Remark. *There are faster reduction algorithms known. See for example [Can87],*

Algorithm 1 Cantors composition algorithm

Input: $D_1 = (u_1, v_1), D_2 = (u_2, v_2)$ reduced divisors
Output: Semireduced Divisor $D_3 \in [D_1 + D_2]$
$d \leftarrow \gcd(u_1, u_2, v_1 + v_2) = s_1 u_1 + s_2 u_2 + s_3(v_1 + v_2)$
$u_3 \leftarrow \frac{u_1 u_2}{d^2}$
$v_3 \leftarrow \frac{s_1 u_1 v_2 + s_2 u_2 v_1 + s_3(v_1 v_2 + F)}{d} \pmod{u_3}$
return $D_3 := (u_3, v_3)$

Algorithm 2 Cantors reduction algorithm

Input: A semireduced divisor $D = (u, v)$
Output: The unique reduced divisor in $[D]$
while $\deg u > g$ **do**
$u \leftarrow \frac{F - v^2}{u}$
$v \leftarrow -v \pmod{u}$
end while
return (u, v)

[Lan05], [CL12] or [DO14].

Remark. *This algorithm can be generalized to hyperelliptic curves given by a polynomial of the form $Y^2 + YH(X) = F(X)$. So it is also applicable in the case where the ground field has characteristic two. Since most of the time in this thesis we are working over a field of characteristic zero and for the sake of simpler equations, we only present this version.*

1.4.6. Simplicity of Jacobians of Genus Two Hyperelliptic Curves

We have to distinguish the set of jacobians of hyperelliptic curves of genus two into two subsets since some arise as the product of two elliptic curves and some are *simple*. It is of interest for us to determine whether a constructed curve has a simple jacobian. While for non-simple jacobians one can exploit the knowledge about torsion points on elliptic curves, for simple jacobians such a tool is not available.

Definition 1.44. *Let A/K be an abelian variety. We say that A is* (absolutely) simple *if it is not ($\overline{K}$-) K-isogenous to the product of abelian varieties of smaller dimension.*

Proposition 1.19 ([Mil08, Prop. 10.1])**.** *Let A be an abelian variety. Then there exist pairwise non-isogenous simple abelian varieties $A_1, \ldots, A_k$ and natural numbers $n_1, \ldots, n_k$ such that there exists an isogeny*

$$\phi : A \to A_1^{n_1} \times \ldots \times A_k^{n_k}.$$

Definition 1.45. *Let $V_{/\mathbb{F}_q}$ be a projective variety over the finite field $\mathbb{F}_q$. Then we define the* Weil zeta function Z_V *of V by*

$$Z_V := \exp\left(\sum_{i=1}^{\infty} \frac{\#V(\mathbb{F}_{q^i})}{i} X^i\right)$$

We now collect some facts about the zeta function of varieties which we use in this chapter.

Proposition 1.20 ([Poo06])**.** *Let $V/\mathbb{F}_q$ be a smooth and projective variety. Then the following holds*

1. $$Z_V = \prod_{i=0}^{2g} P_i^{(-1)^{i+1}},$$

   where $g = \dim(V)$ and $\prod_{j=1}^{b_i}(1 - \alpha_{ij}X) = P_i \in \mathbb{Z}[X]$ for $\alpha_{ij} \in \mathbb{C}$ such that $|\alpha_{ij}| = q^{\frac{i}{2}}$.

2. *If V is abelian and V' is an abelian variety such that V and V' are isogenous, then $Z_V = Z_{V'}$.*

3. *If V is abelian of dimension g and P_V is the characteristic polynomial of the* Frobenius *endomorphism, then $P_1(X) = X^{2g}P_V(X^{-1})$.*

4. *If V is an abelian variety which is isogenous to a product of abelian varieties A and B, we have $P_V = P_A P_B$.*

5. *If* $\dim(V) = 1$, *we have*
$$Z_V = \frac{L_V}{(1-X)(1-qX)},$$
where $L_V = \prod_{i=1}^{g}(1-\alpha_i X)(1-\overline{\alpha_i}X) \in \mathbb{Z}[X]$ *and* g *is the genus of the curve* V. *We call* L_V *the* L-function *of* V.

6. *If* $V = \mathrm{Jac}(C)$, *for a curve* C *and we write* $Z_V = \prod_{i=0}^{2g} P_i^{(-1)^{i+1}}$, *then* $P_1 = L_C$.

7. *Let* $\mathbb{F}_{q^n}$ *be some finite extension of* $\mathbb{F}_q$ *and* $\dim(V) = 1$. *Then*
$$L_{V/\mathbb{F}_{q^n}} = \prod_{i=1}^{g}(1-\alpha_i^n X)(1-\overline{\alpha_i}^n X).$$

We use these properties of the zeta function to determine whether the jacobian $\mathrm{Jac}(C)$ of a hyperelliptic curve $C/\mathbb{Q}$ is absolutely simple . So for a given curve C of genus g we want to compute the polynomial $L_{C/\mathbb{F}_p}$ for some prime p of good reduction of C. This can be done by counting points of the curve C over $\mathbb{F}_{p^i}$ for $i = 1, \ldots, g$.

Let $C/\mathbb{Q}$ be a hyperelliptic curve of genus two and p a prime of good reduction of the curve C and consider the reduced curve $\overline{C}/\mathbb{F}_p$. Then we set
$$\begin{aligned} U &:= p + 1 - \#\overline{C}(\mathbb{F}_p) \\ V &:= \frac{1}{2}(U^2 - (p^2 + 4p + 1 - \#\overline{C}(\mathbb{F}_{p^2}))) \end{aligned}$$
and $P := X^2 - UX + V$. Then P has two roots which we denote by a_p and a'_p. These roots again give us two polynomials $X^2 - a_p X + q$ and $X^2 - a'_p X + q$. For each of these polynomials we fix a root and denote it by α_p and α'_p resp.

Remark. *The quantities* α_p *and* α'_p *are constructed such that they are two of the roots of* $X^4 L_{\overline{C}}\left(\frac{1}{X}\right)$. *Therefore, we can write*
$$L_{\overline{C}} = (1-\alpha_p X)(1-\overline{\alpha_p}X)(1-\alpha'_p X)(1-\overline{\alpha'_p}X) \in \mathbb{Z}[X].$$

Theorem 1.21 ([Lep95])**.** *Let* C *be a genus two curve defined over* $\mathbb{Q}$ *and let* $K := \mathbb{Q}(\alpha_p)$ *and* L *the* Galois *closure of* K, *with* α_p *as above. Assume* $\mathrm{Gal}(L/\mathbb{Q})$ *is isomorphic to the dihedral group* D_4, *then* $\mathrm{Jac}(C)$ *is absolutely simple.*

Proof : Assume there exists a number field M of degree $n := [M : \mathbb{Q}]$ such that $\mathrm{Jac}(C)$ is M-isogenous to a product of elliptic curves E_1 and E_2. Let $\mathcal{O}_M$ denote the ring of integers of M and $\mathfrak{P}$ a prime of $\mathcal{O}_M$ lying over p. Since p is assumed to be a prime of good reduction, we can consider $\overline{\mathrm{Jac}(C)}$ over $\kappa := {}^{\mathcal{O}_M}\!/_{\mathfrak{P}\mathcal{O}_M}$. This reduction of the jacobian has to be isogenous to the product of the reductions of E_1 and E_2. This implies

by Theorem 1 of [Tat66] that the associated Z-functions of the reduced jacobian and the product of the reduced elliptic curves have to be the same. This gives us $L_{\overline{C}} = L_{\overline{E_1}} L_{\overline{E_2}}$ with Proposition 1.20. Since $L_{\overline{E_i}} \in \mathbb{Z}[X]$, we get $A_n := \alpha_p^n + \overline{\alpha_p}^n \in \mathbb{Z}$. Multiplying this equation with α_p^n gives us that α_p^n is a root of the polynomial

$$X^2 - A_n X + p^n,$$

since $\alpha_p \overline{\alpha_p} = p$. So, $[\mathbb{Q}(\alpha_p^n) : \mathbb{Q}] \leq 2$ and $\mathbb{Q}(\alpha_p^n) \subset \mathbb{Q}(\alpha_p) = K$.

So the next step is to look at the possible subfields of K. First observe, that $\mathbb{Q}(A_1)$ is a subfield of degree two of K since A_1 can not be in $\mathbb{Q}$ since otherwise $[K : \mathbb{Q}] \leq 2$. Therefore, $\mathrm{Gal}(L/\mathbb{Q})$ has to be of order two which is a contradiction with the assumption that $\mathrm{Gal}(L/\mathbb{Q}) = D_4$.

Since we have assumed that D_4 is the Galois group of L over $\mathbb{Q}$, we know that there have to exist three subfields L_1, L_2 and L_3 of L such that $[L_i : \mathbb{Q}] = 2$ for $i = 1, 2, 3$. It is easy to see that if two of these subfields are also subfields of K that all three have to be subfields of K. This is not possible since then $K = L$ what is a contradiction to the assumption $[K : \mathbb{Q}] \leq 4$ and $[L : \mathbb{Q}] = 8$. So the only subfield of K of degree two is $\mathbb{Q}(A_1)$.

This yields that $\mathbb{Q}(\alpha_p^n) = \mathbb{Q}$ or $\mathbb{Q}(\alpha_p^n) = \mathbb{Q}(A_1)$. Since $A_1 = \alpha_p + \overline{\alpha_p} \in \mathbb{R}$, we get in either case $\alpha_p^n \in \mathbb{R}$. Since $\alpha_p = \zeta\sqrt{p}$ for some $\zeta \in \mathbb{C}$ of norm one and using that α_p^n is a real number, we get that ζ has to be some root of unity. Therefore, $K \subset \mathbb{Q}(\sqrt{p}, \zeta)$. Since $\mathbb{Q}(\sqrt{p}, \zeta)$ is an abelian Galois extension, K has to be a Galois extension itself. This implies $K = L$ what is impossible by assumption. Therefore, $\mathrm{Jac}(C)$ has to be absolutely simple. □

1.4.7. Rational Points on Curves

Throughout this thesis we are confronted with the task to find $\mathbb{Q}$-rational points on algebraic varieties. Often the only way to find rational points on a variety is a naive search. But if we consider curves for example, there are some classes of curves where we can do better. These methods are presented in this section in a rather short way.

Chabauty Method

Long before Faltings published his proof of the finiteness of the number of $\mathbb{Q}$-rational points on a smooth curve of genus greater then one in [Fal83], Chabauty proved such a result under the assumption that the rank of the jacobian of the curve of interest is strictly smaller then the genus [Cha41]. This result was used by Coleman, who obtained effective bounds for the number of $\mathbb{Q}$-rational points on such a curve [Col85]. We present this result following the paper [MP07] by McCallum and Poonen.

Theorem 1.22 (Chabauty)**.** *Let $C/\mathbb{Q}$ be a curve of genus g such that* $\operatorname{rank}(\operatorname{Jac}(C)(\mathbb{Q})) \leq g-1$*. Then $C(\mathbb{Q})$ is finite.*

We do not give a proof of this theorem but give a sketch of the used ideas. For simplicity we assume that we know a $\mathbb{Q}$-rational point P_0 on the hyperelliptic curve C. Then we have the embedding $\Phi_{P_0} : C \hookrightarrow \operatorname{Jac}(C)$ with the property that $\mathbb{Q}$-rational points on C is mapped to $\mathbb{Q}$-rational points on $\operatorname{Jac}(C)$. By the theorem of Mordell-Weil we have that $\operatorname{Jac}(C)(\mathbb{Q})$ is a finitely generated abelian group. If we were able to compute $\operatorname{Jac}(C)(\mathbb{Q})$, this can be used to find points in $\operatorname{Jac}(C)(\mathbb{Q})$ which lie in $\Phi_{P_0}(C)$. Therefore, we can determine $C(\mathbb{Q})$. Unfortunately, the task of computing $\operatorname{Jac}(C)(\mathbb{Q})$ can not be done efficiently in general. The idea now is to take a prime p of good reduction and consider the jacobian as a variety over $\mathbb{Q}_p$ and look at the p-adic closure $\overline{\operatorname{Jac}(C)(\mathbb{Q})}$ of $\operatorname{Jac}(C)(\mathbb{Q})$ in $\operatorname{Jac}(C)(\mathbb{Q}_p)$. Then it can be shown that the dimension of $\overline{\operatorname{Jac}(C)(\mathbb{Q})}$ is bounded by the rank of $\operatorname{Jac}(C)(\mathbb{Q})$. Chabauty then showed that we have finiteness of $C(\mathbb{Q})$ under the condition that $\dim(\overline{\operatorname{Jac}(C)(\mathbb{Q})}) < g$.

The nice thing about this theorem is that the proof by Chabauty gives an explicit bound for $\#C(\mathbb{Q})$ so that it is possible to completely determine the set of $\mathbb{Q}$-rational points on C.

Theorem 1.23 (Coleman)**.** *Let $C/\mathbb{Q}$ be a hyperelliptic curve of genus two such that* $\operatorname{rank}\operatorname{Jac}(C)(\mathbb{Q}) \leq 1$ *and $p \geq 5$ a prime of good reduction. Then*

$$\#C(\mathbb{Q}) \leq \#\overline{C}(\mathbb{F}_p) + 2.$$

More recently, Stoll used similar techniques in [Sto13] to prove the existence of a uniform bound for the number of K-rational points on a genus g curve with a jacobian of rank at most $g-3$ depending only on $[K:\mathbb{Q}]$ and g.

Compute Rational Torsion of a Given Curve

While it is very hard to check what orders of torsion subgroups can occur in general, it is possible to determine the torsion subgroup of the jacobian of an explicitly given hyperelliptic curve over $\mathbb{Q}$.

Theorem 1.24. *Let $C/\mathbb{Q}$ be a hyperelliptic curve, p an odd prime of good reduction and $J := \mathrm{Jac}(C)$. Then there exists an injective group homomorphism*

$$J_{tors}(\mathbb{Q}) \hookrightarrow \overline{J}(\mathbb{F}_p).$$

Proof : See [CF96, Th. 7.4.1] or [Har77, Ex. IV.4.19]. □

This theorem gives a way to compute a bound for the order of the $\mathbb{Q}$-rational torsion subgroup of the jacobian of a hyperelliptic curve as follows. Let S be a set of odd primes of good reduction for a hyperelliptic curve C and set $a_p := \#\overline{\mathrm{Jac}(C)}(\mathbb{F}_p)$ for all $p \in S$. Then we get

$$\#\,\mathrm{Jac}(C)_{tors}(\mathbb{Q}) \mid \gcd(a_p \mid p \in S).$$

So there is good hope to determine a sharp bound for the number of $\mathbb{Q}$-rational points with finite order.

Example 1.5. *Let C be the hyperelliptic curve given by $C : Y^2 = X^5 + 1$. The point on the jacobian $\mathrm{Jac}(C)$ given by $(x^2 + x, x + 1)$ has order 10. We now look at the curve $\overline{C}$ obtained by reducing the equation of C modulo 3. C has good reduction modulo 3 since $3 \nmid \Delta(C) = 2^8 5^5$. Then counting the number of points gives us $\#\overline{J}(\mathbb{F}_3) = 10$ so we can conclude $\#\,\mathrm{Jac}(C)_{tors}(\mathbb{Q}) = 10$ and the point above is a generator of the complete torsion subgroup.*

This example is very simple since the rational points over $\mathbb{F}_3$ are exactly the images of the torsion points under the reduction map.

Example 1.6. *Consider the curve C given by*

$$Y^2 = -4X^5 + 44715641X^4 + 149041202X^3 + 384504629X^2 + 384207068X - 653328796.$$

This curve has a $\mathbb{Q}$-rational 11-torsion point on its jacobian by Example 3.5. The

discriminant of C is

$$\Delta(C) = 2^{32}3^{25}5^{13}11^{11}19^{11}1296109 \cdot 746457109.$$

Reducing the curve modulo the primes in $S := \{7, 29\}$ gives us

$$a_7 = 2^3 \cdot 11 \text{ and } a_{29} = 3 \cdot 11 \cdot 29.$$

Therefore, we can conclude that all its rational torsion is determined by the 11*-torsion point since* $\gcd(a_7, a_{29}) = 11$. *The set S is the smallest set of primes which gives us the desired result.*

Unfortunately this procedure does not always give us a sharp bound.

For elliptic curves there is a very powerful theorem dealing with the computation of torsion points of elliptic curves.

Theorem 1.25 (Nagell-Lutz)**.** *Let $E/\mathbb{Q}$ be an elliptic curve given by a short* Weierstrass *equation with integral coefficients, Δ the discriminant of E and $P = (x, y) \in E_{tors}(\mathbb{Q})$ a point of finite order. Then $x, y \in \mathbb{Z}$ are integers and $P \in E[2]$ or $y^2 \mid \Delta$.*

For the proof of this theorem see Silverman [Sil09].

Theorem 1.25 makes the search of $\mathbb{Q}$-points of finite order on an elliptic curve to a finite problem since a divisibility criterion of the discriminant is involved.

In [Gra13] Grant proves an analogous result for hyperelliptic curves of genus g.

Theorem 1.26 ([Gra13, Thm. 3])**.** *Let*

$$C : Y^2 = X^{2g+1} + \sum_{i=0}^{2g} a_i X^i$$

be an affine model of a hyperelliptic curve defined over $\mathbb{Z}$. Let

$$\Phi_{P_\infty} : C \to \mathrm{Jac}(C)$$

be the Albanese *map with respect to P_∞. Assume $P = (x, y) \in C(\mathbb{Q})$ is a point such that $\Phi_{P_\infty}(P) \in \mathrm{Jac}(C)_{tors}$ is of finite order. Then we have*

1. *$x, y \in \mathbb{Z}$, and*
2. *$y = 0$ or $y^2 \mid \Delta(C)$,*

where $\Delta(C)$ is the discriminant of C.

While in the case of elliptic curves the result is about all torsion points of the elliptic curves, for hyperelliptic curves we only get a result for points in the image of C under the Albanese map.

Remark. *The set*

$$\Phi_P(C) \cap \mathrm{Jac}(C)_{tors}$$

is finite for all $P \in C(\mathbb{Q})$. This is a special case of the Manin-Mumford *conjecture proven by* Raynaud *in [Ray83].*

As stated in the beginning of this section, most of the time it is only possible to find rational points by a naive search. For such a search we have to bound in some way the area we want to search for solutions of the defining equations. In general this is done by taking heights in to account. A height on a projective space measures in some way the "arithmetic complexity" of a point. An important fact is that a set of points of bounded height is finite.

Definition 1.46 (Logarithmic Height)**.** *Let $A/\mathbb{Q}$ be an abelian variety with neutral element $\mathcal{O}$. Then define the* logarithmic height $h : A \to \mathbb{R}$ *on A by*

$$h(P) = \sum_{\nu \in M_K} n_\nu \log(\max(\mid x_0 \mid_\nu, \ldots, \mid x_n \mid_\nu))$$

where $P = [x_0 : \ldots : x_n] \in A(K) \subset \mathbb{P}^n(K)$, M_K is the set of valuations of K and $n_\nu := [K_\nu : \mathbb{Q}_\nu]$.

Remark. *For a $\mathbb{Q}$-rational point P this height function coincides with a more naive one. Namely if we write $P = [x_0 : \ldots : x_n]$ with $x_0, \ldots, x_n \in \mathbb{Z}$, $\gcd(x_0, \ldots, x_n) = 1$ its logarithmic height is given by*

$$h(P) = \log(\max(|x_0|, \ldots, |x_n|)).$$

Definition 1.47 (Canonical Height)**.** *Let $A/\mathbb{Q}$ be an abelian variety and fix an embedding $A \subset \mathbb{P}^n$. Then define the* canonical height $\hat{h} : A \to \mathbb{R}$ *on A by*

$$\hat{h}(P) = \lim_{N \to \infty} N^{-2} h([N]P).$$

Theorem 1.27. *For all $P \in A(\overline{\mathbb{Q}})$ and $m \in \mathbb{Z}$, the relation $\hat{h}([m]P) = m^2 \hat{h}(P)$ holds.*

With the theorem above we directly obtain the first direction of the following corollary. For the other direction we use that the set of points with bounded canonical height is finite.

Corollary 1.28. *Let A be an abelian variety defined over $\mathbb{Q}$ with canonical height $\hat{h}$. Then $P \in A$ is a point of finite order if and only if $\hat{h}(P) = 0$.*

Proposition 1.29. *Let A/K be an abelian variety over some number field K. Then the set of points with bounded height is finite.*

The existence of the height function on an abelian variety over a number field K gives us the Mordell-Weil Theorem 1.9 via infinite descent.

2. Moduli Spaces and Families of Curves

In this chapter our goal is to give some properties of moduli spaces and constructions of them for some special objects. Since in general the construction of such spaces is very complicated, we restrict ourselves to small genus hyperelliptic curves and small-dimensional abelian varieties.

2.1. Generalities

In this section we introduce some basic definitions and properties of moduli spaces. We loosely follow [HM98]. The purpose of a moduli space is to classify all equivalence classes of certain geometric objects of a special type. For example one can consider the set of all elliptic curves defined over a field K with $\mathrm{char}(K) \neq 2, 3$ up to $\overline{K}$-isomorphisms. Then the first thing to observe is that every elliptic curve E can be given by an affine model of the form $E : Y^2 = F(X)$ with a degree three polynomial F. Obviously such a polynomial F has three different roots over the algebraic closure of the field of definition K of E since E is assumed to be elliptic. Now it is possible to send two of these roots to $x = 1$ resp. $x = 0$ by an automorphism of $\mathbb{P}^2$. So over $\overline{K}$ the elliptic curve we started with is isomorphic to the a curve $E_\lambda : Y^2 = X(X-1)(X-\lambda)$. Therefore, we are only left to check whether two such curves E_λ and $E_{\lambda'}$ are isomorphic. This is the case if and only if $\lambda' \in \left\{\lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{\lambda}{1-\lambda}, \frac{\lambda-1}{\lambda}\right\}$. For an elliptic curve of such a form we can give its j-invariant by $j(E_\lambda) = \frac{2^8(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$. This function is invariant in the set mentioned above. Therefore, it sets up a bijection between the set of isomorphism classes of elliptic curves and $\mathbb{A}^1$.

As seen in the genus one example, we want the space characterizing the objects of interest to be a variety $\mathcal{M}$. Furthermore we wish that this variety resembles the structure of families of the considered objects. That is, if we are given a family of objects $\pi : C \to S$ parametrized by a scheme S, we want that the map $S(k) \to \mathcal{M}(k)$ comes from a morphism $S \to \mathcal{M}$.

Definition 2.1. *Let S and $\mathcal{C}$ be schemes. Then a morphism of schemes $\pi : \mathcal{C} \to S$ is called* family of schemes.

Example 2.1. *Let $C/\mathbb{Q}$ be a plane algebraic curve given by a primitive polynomial with integral coefficients. Then C can be considered as a family of curves $\mathcal{C}$ over* $\mathrm{Spec}(\mathbb{Z})$ *in the following way. Let $\pi : \mathcal{C} \to \mathrm{Spec}(\mathbb{Z})$ be the map such that for every $p \in \mathrm{Spec}(\mathbb{Z})$ the fiber $\pi^{-1}(p)$ above p is the reduction of the curve C modulo the prime p.*

Example 2.2. *We now consider curves over some rational function field as a family of curves; that is, we start with a field K and the rational function field $L := K(x_1, \ldots, x_n)$ in n variables over K. Then a plane curve C over L given by a primitive polynomial with coefficients in $K[x_1, \ldots, x_n]$ is nothing else than a family of curves $\mathcal{C}$ over K. This can be seen by considering the embedding $L \hookrightarrow L(C)$ which induces a rational map $\mathcal{C} \to \mathbb{A}^n$ since the function field of $\mathbb{A}^n$ is just the rational function field in n variables.*

If we are given a family $\mathcal{C}$ of curves, we often write $C \in \mathcal{C}$ for a specialization. That is we consider a family of curves as a set of curves by forgetting the structure of the family. Sometimes we do not differentiate between a family of curves and a curve over a function field.

Definition 2.2. *A scheme $\mathcal{M}$ with a family of schemes $\pi : \mathcal{C} \to \mathcal{M}$ parametrized by $\mathcal{M}$ is called* fine moduli space *if for all families of schemes $f : C \to S$ there exists a unique morphism $h : S \to \mathcal{M}$ such that $C \cong S \times_{\mathcal{M}} \mathcal{C}$.*

Remark. *In the language of categories this means that the* moduli functor

$$\mathcal{F} : (Schemes)^\circ \to (Sets),$$

which sends a scheme S to the set of equivalence classes of schemes over S, is representable by the scheme $\mathcal{M}$. The scheme representing this functor is the moduli space.

In general we would not expect that such a fine moduli space exists. If the objects we are interested in have automorphisms, this construction does not work in general.

We now present two possibilities to deal with the non-representablity of the moduli functor.

1. Weaken the conditions on a moduli space.

2. Demand for extra structure that rules out automorphisms.

Let us consider the first possibility in the list. Instead of wanting moduli functor to be representable we ask for a scheme M and a natural transformation $\Psi_M : \mathcal{F} \to h_M$ such that the following holds:

1. For any algebraically closed field K the map

$$\mathcal{F}(\mathrm{Spec}(K)) \to M(K)$$

is a bijection.

2. For any scheme M' with a natural transformation $\Phi_{M'} : \mathcal{F} \to h_{M'}$ there exists a unique morphism $M \to M'$ such that the functor of points between the two schemes is connected via the morphism between them.

Definition 2.3. *A scheme with the properties above is called* coarse moduli space.

Remark. *If such a coarse moduli space exists, it is unique up to unique isomorphism by the universal property.*

Example 2.3. $\mathbb{A}^1$ *is a coarse moduli space for elliptic curves. It is only coarse because two elliptic curves defined over a field K can have the same j-invariant even if there is no isomorphism defined over K between them.*

Remark. *For smooth genus g curves there exists a coarse moduli space denoted by M_g.*

The second approach we consider is to require extra structure on the objects we are interested in. This extra structure should encode enough information that there is no possibility for automorphisms on the objects. One possibility is to consider as objects instead of isomorphism classes of curves isomorphism classes of pointed curves. That is, considering $(C, P_1, \ldots, P_n)$ as objects, where we identify $(C, P_1, \ldots, P_n)$ and $(C', P'_1, \ldots, P'_n)$ if there exists an isomorphisms between C and C' which sends $\{P_1, \ldots, P_n\}$ to $\{P'_1, \ldots, P'_n\}$.

Example 2.4. *For $N > 3$ the modular curve $\mathrm{X}_1(N)$ is a fine moduli space parametrizing pairs of an elliptic curve with a point of exact order N on it.*

If we have a fine moduli space for our moduli problem, then it is possible to answer a lot of interesting questions. For example if K is some number field, the K-rational points of $\mathrm{X}_1(N)$ correspond exactly to the K-isomorphism classes of elliptic curves with a K-rational point of order N on it.

2.2. Constructing Moduli Spaces over $\mathbb{C}$

In this chapter we construct moduli spaces of abelian varieties. Then our goal is to determine the subvariety whose points correspond to the abelian varieties with real multiplication. First we recall a known connection between lattices in $\mathbb{C}^g$ and abelian varieties of dimension g.

2.2.1. Siegel Moduli Space

We consider abelian varieties of dimension g defined over the complex numbers. The goal is to describe the complex points of the moduli space of the isomorphism classes of such objects. Therefore, we briefly recall the construction in the dimension one case.

An elliptic curve defined over the complex numbers can be uniquely determined by a complex torus. This torus is given by $E = \mathbb{C}/\Lambda_z$, where $\Lambda_z := \mathbb{Z} + z\mathbb{Z}$ and

$$z \in \mathbb{H} := \{z \in \mathbb{C} \mid \Im(z) > 0\}.$$

Two such tori are isomorphic if and only if the corresponding lattices are homothetic. We have an action of $\mathrm{SL}(2,\mathbb{Z})$ on the upper half plane $\mathbb{H}$ which is given by Möbius transformation. Then it is easy to see that Λ_z and Λ_w are homothetic if and only if z is a Möbius transformation of w. So we get a bijection between the $\mathbb{C}$-isomorphism classes of elliptic curves and the set $\mathrm{SL}(2,\mathbb{Z})\backslash\mathbb{H}$. For the set $\mathrm{SL}(2,\mathbb{Z})\backslash\mathbb{H}$ it can be shown that it is a non-compact Riemann surface of genus zero and after compactifying, it can be identified with $\mathbb{P}^1$ via the j-function.

We want to mimic this construction for abelian varieties of higher dimension. But here it is getting more complicated since not every g-dimensional torus is an abelian variety. We follow loosely the lines of [BL04] and omit most of the proofs.

Theorem 2.1. *Let A be an abelian variety of dimension g defined over $\mathbb{C}$. Then there exists a lattice $\Lambda_A \subset \mathbb{C}^g$ of $\mathbb{R}$-rank $2g$ such that*

$$A \cong \mathbb{C}^g/\Lambda_A.$$

Unfortunately, not every torus is an abelian variety. To determine when this is the case we now give the definition of a Riemann *form*.

Definition 2.4. *Let V be a $\mathbb{C}$-vector space. Let $\Lambda \subset V$ be a lattice. Then a skewsymmetric $\mathbb{R}$-bilinear form $E : V \times V \to \mathbb{R}$ is called* Riemann form *with respect to Λ if the following conditions hold:*

1. *$E(iv, iw) = E(v, w)$ for all $v, w \in V$.*

2. *$H_E(v,w) := E(iv,w) + iE(v,w)$ is positive definite.*

3. *If $v, w \in \Lambda$, then $E(v,w) \in \mathbb{Z}$.*

Lemma 2.2. *Let V be a vector space over $\mathbb{C}$ of dimension $\dim_{\mathbb{C}} V = g$, let $\Lambda \subset V$ be a lattice. Then $A_\Lambda := {}^{V}\!/_{\Lambda}$ is an abelian variety over $\mathbb{C}$ of dimension $\dim A_\Lambda = g$ if there exists a* Riemann *form E with respect to Λ. E is called* polarization *of A_Λ.*

There is a connection between a polarization on A_Λ and an isogeny between A_Λ and its dual. In order to discuss this connection we first give the definition of the dual of an abelian variety. The *dual vector space* $V^\vee$ of V is given by

$$\begin{aligned} V^\vee :=& \quad \operatorname{Hom}_{\overline{\mathbb{C}}}(V, \mathbb{C}) \\ =& \quad \left\{ f : V \to \mathbb{C} \,\middle|\, \begin{matrix} f(\lambda v) = \overline{\lambda} f(v) \\ f(v+w) = f(v) + f(w) \end{matrix} \text{ for all } v, w \in V, \lambda \in \mathbb{C} \right\}. \end{aligned}$$

Let Λ be a lattice in V with a Riemann form, then the set

$$\Lambda^\vee := \{ f \in V^\vee \mid \Im(f(\Lambda)) \subset \mathbb{Z} \}$$

forms a lattice in $V^\vee$ which also admits a Riemann form. So the torus

$$A_\Lambda^\vee := {}^{V^\vee}\!/_{\Lambda^\vee}$$

is again an abelian variety of dimension g, since $\dim_{\mathbb{C}} V^\vee = g$. Then the map

$$\begin{aligned} \lambda_E : \quad A_\Lambda &\longrightarrow A_\Lambda^\vee \\ v &\longmapsto H_E(v, \cdot) \end{aligned}$$

associated to the Riemann form E is an isogeny from the abelian variety to its dual, i.e. it is surjective and has a finite kernel. So we can associate a degree to a polarization by taking the degree of the associated isogeny.

Definition 2.5. *Let $\phi : A \to A'$ be an isogeny of abelian varieties defined over the field K. Then we define*

$$\deg(\phi) := [\phi^* K(A) : K(A')]$$

as the degree *of the isogeny.*

The first observation is that a polarization of degree one implies that A_Λ is isomorphic to its dual $A_\Lambda^\vee$. For elliptic curves, i.e. abelian varieties of dimension one, this always is true. If $\deg \lambda_E = 1$, we call E *principal polarization.* While a polarization E on A gives rise to an isogeny of A to its dual $A^\vee$, the converse is not always true.

Proposition 2.3. *Let λ_E be an isogeny induced by the polarization E on $A/\mathbb{C}$. Then the isogeny $-\lambda_E$ is never induced by a polarization on A.*

Proof : Assume $-\lambda_E$ is induced by some polarization $\widetilde{E}$ on A. Then

$$-\lambda_E(v) = -H_E(v,\cdot) = H_{\widetilde{E}}(v,\cdot) = \lambda_{\widetilde{E}}(v)$$

for all $v \in A$. But since H_E and $H_{\widetilde{E}}$ are both positive definite by assumption, this is not possible. Therefore, the assertion holds. □

The next step is to characterize polarizations. Therefore, we choose a basis of our lattice Λ such that the RIEMANN form E is given by a matrix A_E of the form

$$A_E = \begin{pmatrix} 0 & -D \\ -D & 0 \end{pmatrix},$$

where $D = \operatorname{diag}(d_1, d_2)$ is a diagonal matrix with $d_1 \mid d_2$. It is possible to choose such a basis by the elementary divisor theorem. We say the polarization E is of type (d_1, d_2).

Proposition 2.4. *Let A be an abelian variety over $\mathbb{C}$ and let E be a polarization on A. Then* $\det A_E = 1 \iff \deg \lambda_E = 1$.

Thus, in order to characterize the complex abelian varieties we have to take care that only lattices are considered that admit a polarization. This leads us to the following definition.

Definition 2.6. *The* SIEGEL upper half plane $\mathbb{H}_g$ *is given by*

$$\mathbb{H}_g := \left\{ M \in \mathbb{C}^{g\times g} \mid M = M^t, \Im(M) \text{ is positive definite} \right\}.$$

Lemma 2.5. *Let $\Lambda \subset \mathbb{C}^g$ be a lattice given by $\Lambda = \mathbb{Z}^g + M\mathbb{Z}^g$ for some matrix $M \in \mathbb{H}_g$, then Λ admits a polarization.*

We directly see that $\mathbb{H}_1$ is just the usual upper half plane $\mathbb{H}$.

Now it is left to determine when two elements in $\mathbb{H}_g$ define isomorphic abelian varieties. For $g = 1$ this was given by the action of $\mathrm{SL}(2,\mathbb{Z})$ on $\mathbb{H}$.

Definition 2.7. *The subgroup*

$$\mathrm{Sp}\,(2g,\mathbb{R}) := \left\{ M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}(2g,\mathbb{R}) \,\middle|\, \begin{array}{rcl} \alpha\beta^t & = & \beta\alpha^t \\ \gamma\delta^t & = & \delta\gamma^t \\ \alpha\delta^t + \beta\gamma^t & = & I_g \end{array} \right\}$$

of $\mathrm{GL}(2g,\mathbb{R})$ *is called the* symplectic group *of dimension g.*

There is an action of $\mathrm{Sp}\,(2g,\mathbb{R})$ on the Siegel upper half plane $\mathbb{H}_g$ given by

$$M \mapsto (\alpha M + \beta)(\gamma M + \delta)^{-1}.$$

For $g = 1$ we have the well-known action of the $\mathrm{SL}(2,\mathbb{R})$ on the upper half plane $\mathbb{H}$.

Lemma 2.6. *Let $M, M' \in \mathbb{H}_g$ be such that A_M and $A_{M'}$ are two isomorphic abelian varieties. Then there exists a matrix $S \in \mathrm{Sp}\,(2g,\mathbb{Z})$ such that $M = S \cdot M'$.*

So we have constructed an analytic space $\mathrm{Sp}\,(2g,\mathbb{Z})\backslash\mathbb{H}_g$ such that the complex points of this space correspond to the $\mathbb{C}$-isomorphism classes of principal polarized abelian varieties of dimension g.

Remark. *This construction can be easily generalized to different polarizations.*

Theorem 2.7 ([BL04])**.** *The space $\mathcal{A}_g := \mathrm{Sp}\,(2g,\mathbb{Z})\backslash\mathbb{H}_g$ is $\frac{g(g+1)}{2}$-dimensional.*

Since we are not only interested in parametrizing abelian varieties of given dimension and polarization, but in parametrizing such varieties with certain subgroups of fixed order, we have to look for some level structure on $\mathcal{A}_g$. For the elliptic curves we had three important level structures namely the full level-N-structure, the $\Gamma_0(N)$- and the $\Gamma_1(N)$-structure. Using the fact that there is a morphism $\mathrm{X}_1(N) \to \mathrm{X}_0(N)$, Mazur is able to determine some $N_0 \in \mathbb{N}$ such that for all $N > N_0$ the modular curve $\mathrm{X}_0(N)$ has no rational points [Maz77].

Now we want to consider only isomorphisms of abelian varieties which respect a certain level structure, namely for example fix the whole N-torsion subgroup of A.

Assume A_M is the abelian variety given by the symplectic matrix $M \in \mathbb{H}_g$ then a basis for the N-torsion subgroup is given by

$$\left\{\frac{1}{N}e_1,\ldots,\frac{1}{N}e_g,\frac{1}{N}v_1,\ldots,\frac{1}{N}v_g\right\},$$

where e_i is the i-th vector of the standard basis of $\mathbb{C}^g$ and v_i denotes the i-th line of the matrix M. Then two abelian varieties $A_M, A_{M'}$ together with a basis for the N-torsion subgroups are isomorphic if and only if there exists a matrix

$$\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} = S \in \mathrm{Sp}\,(2g,\mathbb{Z})$$

such that $M = SM'$ and

$$(\gamma M + \delta)\left\{\frac{1}{N}e_1,\ldots,\frac{1}{N}e_g,\frac{1}{N}v_1,\ldots,\frac{1}{N}v_g\right\} = \left\{\frac{1}{N}e_1,\ldots,\frac{1}{N}e_g,\frac{1}{N}v'_1,\ldots,\frac{1}{N}v'_g\right\}.$$

This is true if and only if $S \equiv I_{2g} \pmod N$. This is an easy calculation. This leads us to the following definition of the *principal congruence subgroup.*

Definition 2.8. *The subgroup*

$$\Gamma_g(N) := \{S \in \mathrm{Sp}\,(2g, \mathbb{Z}) \mid S \equiv I_{2g} \pmod N\}$$

is called the principal congruence subgroup of level N and degree g.

With this subgroup we are able to define the Siegel modular variety of degree g and level N. This space is a parameter space for isomorphism classes of abelian varieties of dimension g with fixed complete N-torsion subgroup. This follows from the considerations above.

Definition 2.9. *For $N \in \mathbb{N}$ we define the* Siegel modular variety of degree g and full level N *by*

$$\mathcal{A}_g(N) := \Gamma_g(N) \backslash \mathbb{H}_g\,.$$

Remark. *The space defined above is indeed a quasi-projective algebraic variety [BB66].*

Remark. $[\mathrm{Sp}\,(2g, \mathbb{Z}) : \Gamma_g(N)]$ *is finite since $\Gamma_g(N)$ is the kernel of the reduction homomorphism*

$$\mathrm{Sp}\,(2g, \mathbb{Z}) \to \mathrm{Sp}\left(2g, \mathbb{Z}/N\mathbb{Z}\right).$$

Therefore, we get a holomorphic map of finite degree of the spaces $\mathcal{A}_g(N) \to \mathcal{A}_g$.

Example 2.5 ([HW01])**.** *The* Burkhardt *quartic given by the polynomial*

$$X^4 - X\left(V^3 + W^3 + Y^3 + Z^3\right) + 3VWYZ$$

in $\mathbb{P}^4$ is isomorphic to a compactification of $\mathcal{A}_2(3)$.

Definition 2.10. *A subgroup $\Gamma \subset \mathrm{Sp}\,(2g, \mathbb{Z})$ is called* congruence subgroup of level N and degree g *if $\Gamma_g(N) \subset \Gamma$.*

Analogously we can consider pairs given by an abelian variety A_Λ and a product of g cyclic subgroups of exact order N. Such a subgroup can be given by its g generators. One possibility is to pick the images of $\frac{1}{N}e_i \in \mathbb{C}^g$, for $i = 1, \ldots, g$ under the reduction modulo Λ. Then the condition for two abelian varieties $A_M, A_{M'}$ of dimension g to have an isomorphism sending one subgroup of order N^g to the other subgroup of the same order becomes the following

$$\exists \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = S \in \mathrm{Sp}\,(2g, \mathbb{Z}) :$$

$$(\gamma M' + \delta)\left(\frac{1}{N}e_i + \Lambda_M\right) \in \langle \frac{1}{N}e_i + \Lambda_{M'} \rangle, i = 1, \dots g.$$

This yields that the i-th column of γ reduced modulo N has to be the zero column for $i = 1, \dots, g$. Therefore, we must have $\gamma \equiv 0 \pmod{N}$.

Lemma 2.8. *For $N \in \mathbb{N}$ the group*

$$\Gamma_{g,0}(N) := \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{Sp}\,(2g, \mathbb{Z}) \middle| \; \gamma \equiv 0 \pmod{N} \right\}$$

is a congruence subgroup of $\mathrm{Sp}\,(2g, \mathbb{Z})$.

By the discussion above the quotient space

$$\mathcal{A}_{g,0}(N) := \Gamma_{g,0}(N) \backslash \mathbb{H}_g$$

parametrizes isomorphism classes of abelian varieties together with g cyclic subgroups of order N. We can again see that for $g = 1$ this coincides with the well-known

$$\mathrm{X}_0(N) = \Gamma_0(N) \backslash \mathbb{H}.$$

We want to introduce one more congruence subgroup which corresponds to isomorphism classes of abelian varieties of dimension g together with g points of exact order N. So let us assume now that we have two abelian varieties $A_M, A_{M'}$ together with the g points of order N given by the images of $\frac{1}{N}e_i$ for $i = 1, \dots, g$. Assume there exists an isomorphism $\phi : A_M \to A_{M'}$ of these varieties such that for each $i \in \{1, \dots, g\}$

$$\phi\left(\frac{1}{N}e_i + \Lambda_M\right) = \frac{1}{N}e_i + \Lambda_{M'}.$$

Since this isomorphism ϕ again comes from a matrix $S \in \mathrm{Sp}\,(2g, \mathbb{Z})$, this gives us conditions on the occurring block matrices in S. The i-th relation from above gives us that the reduction of the i-th row in S modulo N has to be $e_i \in \mathbb{Z}/N\mathbb{Z}$. That is, for

$$S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

we get $\alpha \equiv I_g \pmod{N}$ and $\gamma \equiv 0 \pmod{N}$. Since $S \in \mathrm{Sp}\,(2g, \mathbb{Z})$, we know $\alpha\delta^t + \beta\gamma^t = I_g$ has to hold. Therefore,

$$\delta \equiv I_g \pmod{N}.$$

Lemma 2.9. *For $N \in \mathbb{N}$ the group*

$$\Gamma_{g,1}(N) := \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{Sp}\,(2g, \mathbb{Z}) \middle| \; \gamma \equiv 0 \pmod{N}, \alpha \equiv \delta \equiv I_g \pmod{N} \right\}$$

is a congruence subgroup of $\mathrm{Sp}\,(2g, \mathbb{Z})$.

To find equations which describe the spaces $\Gamma \backslash \mathbb{H}_g$ for some of the above mentioned subgroups Γ, one needs to understand the holomorphic functions on these factor spaces. These functions are called Siegel *modular forms*. In general this is a hard problem to construct equations for these spaces.

We do not get into more detail about Siegel moduli spaces. We want to have a closer look for a subspace of isomorphism classes of abelian varieties with a certain endomorphism ring. For this we sum up some information about endomorphism rings of abelian varieties in the following section.

2.2.2. Endomorphismrings of Abelian Varieties

In this section we want to give a description of the endomorphism ring of an abelian variety. After introducing the possible types of endomorphism rings, we restrict to the case of abelian surfaces over number fields and explain which types of endomorphism rings actually can occur. For the endomorphism ring of an abelian variety A over a field K we write

$$\mathrm{End}(A) := \{\phi : A \to A \mid \phi \text{ is an isogeny}\}$$

and for the endomorphism algebra

$$\mathrm{End}^0(A) := \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

It is easy to see that for non-isogenous abelian varieties A, B we have

$$\mathrm{End}^0(A \times B) = \mathrm{End}^0(A) \times \mathrm{End}^0(B)$$

and

$$\mathrm{End}^0(A^n) = \mathrm{End}^0(A)^{n \times n}.$$

So by Proposition 1.19 it is enough to restrict ourselves to simple abelian varieties.

Proposition 2.10 ([Shi98, Ch. II, Prop. 5])**.** *Let K be any field and A/K be a simple abelian variety of dimension g over K. Write K_0 for the center of* $\mathrm{End}^0(A)$*. Then one of the following holds.*

1. *K_0 is a totally real number field, or*
2. *K_0 is an totally imaginary quadratic extension of a totally real number field.*

Now we want to consider abelian surfaces defined over a number field and write down the possible endomorphism rings.

Proposition 2.11 ([Oor88])**.** *Let K be a number field and A/K a simple abelian variety of dimension two over K. Then one of the following holds.*

1. $\mathrm{End}(A) \cong \mathbb{Z}$.
2. $\mathrm{End}(A) \cong \mathcal{O}$*, where $\mathcal{O}$ is an order in a totally real number field of degree two. We say A* has real multiplication (RM) by $\mathcal{O}$.
3. $\mathrm{End}(A) \cong \mathcal{O}$*, where $\mathcal{O}$ is an order in a imaginary quadratic extension L of a totally real number field K with $[L : K] = 2 = [K : \mathbb{Q}]$. We say A* has complex multiplication (CM) by $\mathcal{O}$.

4. $\mathrm{End}(A) \cong \mathcal{O}$*, where* $\mathcal{O}$ *is an order in an indefinite rational quaternion algebra.*

Chosen a random abelian surface A over a number field K one expects that $\mathrm{End}(A) \cong \mathbb{Z}$. Speaking in terms of moduli spaces, that means that the subspace consisting of abelian surfaces with RM (resp. CM) is only two-dimensional (resp. zero-dimensional), as stated in [Run99].

2.2.3. Hilbert Surfaces

It is clear that the abelian varieties with RM form a subset of the moduli space of all abelian varieties. Now, we describe it as a subvariety by constructing a complex manifold which parametrizes these varieties and give an embedding of the constructed manifold into $\mathcal{A}_g$. The main references are [Gor02] and [vdG88]. As in the sections before we omit most of the proofs.

Let L be a totally real field with $[L:\mathbb{Q}] = g$ and let $\sigma_i : L \hookrightarrow \mathbb{R}$ for $i = 1, \ldots, g$ denote the g embeddings of L in $\mathbb{R}$. Let $\mathcal{O}_L$ be the ring of integers of the field L. Then we can embed $\mathrm{SL}(2, \mathcal{O}_L)$ in $\mathrm{SL}(2,\mathbb{R})^g$ by the map

$$\begin{array}{rccc} (\sigma_1, \ldots, \sigma_g): & \mathrm{SL}(2,\mathcal{O}_L) & \longrightarrow & \mathrm{SL}(2,\mathbb{R})^g \\ & M & \longmapsto & (\sigma_1(M), \ldots, \sigma_g(M)) \end{array}$$

So it is possible to define an action of the $\mathrm{SL}(2,\mathcal{O}_L)$ on the g-fold upper half plane $\mathbb{H}^g$ by fractional linear transformations of $\sigma_i(\mathrm{SL}(2,\mathcal{O}_L))$ on the i-th copy of $\mathbb{H}$.

With $g = 1$ and $K = \mathbb{Q}$ we again obtain the well-known action of the $\mathrm{SL}(2,\mathbb{Z})$ on the upper half plane $\mathbb{H}$.

We now have a closer look at abelian surfaces with maximal RM. By maximal RM we mean, given an abelian variety A we have that $\mathrm{End}(A)$ is the maximal order in $\mathrm{End}^0(A)$. The methods we use in this section generalize straight-forwardly to higher dimension and arbitrary order $\mathrm{End}(A)$ in $\mathrm{End}^0(A)$.

Let now $A_{/\mathbb{C}} := {}^{\mathbb{C}^2}\!/_{\Lambda}$ be an abelian surface with maximal RM by the real quadratic number field L. There is an action of L on $\mathbb{H}^2$ given by

$$\alpha \cdot (x_1, x_2) = (\alpha x_1, \sigma(\alpha) x_2),$$

where $\alpha \in L$ and σ is the non-trivial automorphism of L.

Proposition 2.12. *The defining lattice of A up to isomorphism is of the form*

$$\Lambda = \Lambda_z := \mathcal{O}_L \cdot (1,1) + \mathcal{O}_L \cdot z,$$

where $z = (z_1, z_2) \in \mathbb{H}^2$.

For the proof see [Gor02].

This is the first step to describe a moduli space for abelian surfaces with maximal RM by a given real quadratic number field. Now we show the following.

Proposition 2.13. *Let $z \in \mathbb{H}^2$ define the lattice $\Lambda_z = \mathcal{O}_L \cdot (1,1) + \mathcal{O}_L \cdot z$. Then $A_z := {}^{\mathbb{C}^2}\!/_{\Lambda_z}$ is an abelian variety with maximal RM by L.*

Proof : By [Gor02, Lemma 2.8 and Lemma 2.9] there exists a RIEMANN form on A_z over $\mathbb{C}$. Therefore, A_z is an abelian variety over $\mathbb{C}$. Obviously we have by construction for all $\alpha \in \mathcal{O}_L$ that $\alpha\Lambda_z \subset \Lambda_z$, thus α is an endomorphism of A_z. This gives us an embedding

$$\mathcal{O}_L \hookrightarrow \mathrm{End}(A_z).$$

□

This gives us that $\mathbb{H}^2$ is a parameter space for abelian surfaces with maximal RM by a given number field. The remaining question is, when two elements of $\mathbb{H}^2$ give the same isomorphism class of of abelian surfaces.

Proposition 2.14 ([Gor02, Th. 2.17])**.** *Two abelian surfaces A_z and $A_{z'}$ defined over $\mathbb{C}$ with RM are isomorphic if and only if there exists $A \in \mathrm{SL}(2, \mathcal{O}_L)$ such that $z = A \cdot z'$.*

Putting all together, we get the bijection

$$\mathrm{SL}(2, \mathcal{O}_L) \backslash \mathbb{H}^2 \leftrightarrow \{\text{isomorphism classes of abelian surfaces with RM by } \mathcal{O}_L\}.$$

Our next goal is to embed these constructed spaces in the SIEGEL modular space. So we need an embedding of $\mathbb{H}^2$ into $\mathbb{H}_2$ which respects the group actions. The image

$$\mathrm{SL}(2, \mathcal{O}_L) \backslash \mathbb{H}^2 \hookrightarrow \mathrm{Sp}\,(4, \mathbb{Z}) \backslash \mathbb{H}_2$$

is called the HUMBERT *surface of discriminant d*. Let $(1, \alpha)$ be a integral basis for $\mathcal{O}_L$ and set

$$R := \begin{pmatrix} 1 & \alpha \\ 1 & \sigma(\alpha) \end{pmatrix}.$$

Then the embedding $\mathbb{H}^2 \hookrightarrow \mathbb{H}_2$ given by

$$(z_1, z_2) \mapsto R^T \begin{pmatrix} z_1 & 0 \\ 0 & z_2 \end{pmatrix} R$$

is equivariant relative to the embedding $\mathrm{SL}(2, \mathcal{O}_L) \hookrightarrow \mathrm{Sp}\,(4, \mathbb{Z})$ given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} R^T & 0 \\ 0 & R^{-1} \end{pmatrix} \begin{pmatrix} a & 0 & b & 0 \\ 0 & \sigma(a) & 0 & \sigma(b) \\ c & 0 & d & 0 \\ 0 & \sigma(c) & 0 & \sigma(d) \end{pmatrix} \begin{pmatrix} \left(R^{-1}\right)^T & 0 \\ 0 & R \end{pmatrix}.$$

Since this embedding is equivariant, we get an embedding

$$\mathrm{SL}(2,\mathcal{O}_L)\backslash\mathbb{H}^2 \hookrightarrow \mathrm{Sp}\,(4,\mathbb{Z})\backslash\mathbb{H}_2\,.$$

For more details of modular embeddings see [Ham66].

Now we want to consider isomorphism classes of pairs (A,H), where A is an abelian surface with RM by $\mathcal{O}_L$ and H is a subgroup of fixed order N. Assume (A,H) is isomorphic to (A',H'), that is, $A\cong A'$ as abelian surfaces and the isomorphism sends H to H'. Let now A be given as A_z and A' as A_w with $z,w\in\mathbb{H}^2$. Then there exists a matrix

$$M := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathcal{O}_L)$$

such that $z = M\cdot w$. This is equivalent to

$$\Lambda_w \cdot \begin{pmatrix} cz_1+d & 0 \\ 0 & \sigma(c)z_2+\sigma(d) \end{pmatrix} = \Lambda_z.$$

Let denote the image of the subgroup generated by $\left(\frac{1}{N},\frac{1}{N}\right)+\Lambda_z$ over $\mathcal{O}_L$ in A_z by H. This subgroup is of order N. By assumption we have

$$\langle\left(\frac{1}{N},\frac{1}{N}\right)+\Lambda_w\rangle_{\mathcal{O}_L}\cdot\begin{pmatrix} cz_1+d & 0 \\ 0 & \sigma(c)z_2+\sigma(d) \end{pmatrix} = \langle\left(\frac{1}{N},\frac{1}{N}\right)+\Lambda_z\rangle_{\mathcal{O}_L}.$$

This is true if and only if $\langle\left(\frac{cz_1+d}{N},\frac{\sigma(c)z_2+\sigma(d)}{N}\right)+\Lambda_z\rangle_{\mathcal{O}_L} = \langle\left(\frac{1}{N},\frac{1}{N}\right)+\Lambda_z\rangle_{\mathcal{O}_L}$. Since both subgroups are of order N, it suffices to check under what conditions the generator of one subgroup is in the other one. This holds exactly under the condition that $\left(\frac{cz_1+d}{N},\frac{\sigma(c)z_2+\sigma(d)}{N}\right)\equiv\left(\frac{1}{N},\frac{1}{N}\right) \pmod{\Lambda_z}$. So c has to be divisible by N in $\mathcal{O}_L$.

Definition 2.11. $\Gamma_{2,0}(N,\mathcal{O}_L) := \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in\mathrm{SL}(2,\mathcal{O}_L)\middle| c\equiv 0 \pmod{N}\right\}$

Lemma 2.15. *$\Gamma_{2,0}(N,\mathcal{O}_L)$ is a subgroup of finite index in $\mathrm{SL}(2,\mathcal{O}_L)$.*

The space $\Gamma_{2,0}(N,\mathcal{O}_L)\backslash\mathbb{H}^2$ parametrizes isomorphism classes of pairs (A,H) as defined above.

Now, we do not only fix a subgroup generated by an element of order N. Now we want to fix the generator itself, that is, to consider pairs (A,P), where P is a point of fixed order N. This leads to the question under which conditions two abelian surfaces are isomorphic over $\mathbb{C}$ such that the isomorphism sends a fixed point of order N to a fixed point of order N on the other surface. Let P be the image of $\left(\frac{1}{N},\frac{1}{N}\right)+\Lambda_z$ in A_z

and let P' be the image of $\left(\frac{1}{N}, \frac{1}{N}\right) + \Lambda_w$ in A_w with

$$\Lambda_w \cdot \begin{pmatrix} cz_1 + d & 0 \\ 0 & \sigma(c)z_2 + \sigma(d) \end{pmatrix} = \Lambda_z.$$

Then

$$P' \cdot \begin{pmatrix} cz_1 + d & 0 \\ 0 & \sigma(c)z_2 + \sigma(d) \end{pmatrix} = P$$
$$\iff c \equiv 0 \pmod{N} \text{ and } d \equiv 1 \pmod{N}$$

in $\mathcal{O}_L$.

Definition 2.12. $\Gamma_{2,1}(N, \mathcal{O}_L) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathcal{O}_L) \middle| \begin{matrix} c \equiv 0 \pmod{N}, \\ d \equiv 1 \pmod{N} \end{matrix} \right\}$

Lemma 2.16. *$\Gamma_{2,1}(N, \mathcal{O}_L)$ is a subgroup of finite index in $\mathrm{SL}(2, \mathcal{O}_L)$.*

2.2.4. Families of Hyperelliptic Curves with Real Multiplication

In section 4 we consider $\mathbb{Q}$-rational torsion points of low order on the jacobians of a family of hyperelliptic curves with real multiplication by $\sqrt{5}$. In this section we present how this family is constructed. Before giving the one-parameter family we actually use later, we give the construction of a two-parameter family due to MESTRE [Mes91].

The idea is to start with a family of elliptic curves with a five-torsion point P on it. Such a family is given by

$$E_\lambda : Y^2 + (1-\lambda)XY - \lambda Y = X^3 - \lambda X^2 \text{ (see Theorem 3.2).}$$

On this family the point $P = (0,0)$ has order five for all specializations. The finite subgroup $\langle P \rangle$ gives us an isogeny

$$\phi : E_\lambda \to {}^{E_\lambda}\!/_{\langle P \rangle} =: E'_\lambda$$

of degree five. Since both E_λ and E'_λ are elliptic curves, we have a projection to $\mathbb{P}^1$ using the x-coordinate.

$$\begin{array}{ccc} E_\lambda & \xrightarrow{\phi} & E' \\ {\scriptstyle x_{E_\lambda}}\downarrow & & \downarrow{\scriptstyle x_{E'_\lambda}} \\ \mathbb{P}^1 & \xrightarrow[u]{} & \mathbb{P}^1 \end{array}$$

The curve $C : Y^2 = u(X) - \mu$ is hyperelliptic of genus two with RM by $\mathcal{O}_L$. By MESTRE this yields a two-parameter-family given by

$$C_{\lambda,\mu} : Y^2 = (1-X)^3 + \lambda X((1-X)^3 + \lambda X^2 - X^3(1-X)) - \mu X^2(X-1)^2.$$

In [Has00] HASHIMOTO constructed a three-parameter-family of hyperelliptic curves with RM by $\mathcal{O}_L$ in a very different way. He started with a family of polynomials with GALOIS group A_5. This family of polynomials he used to construct the three-parameter-family of hyperelliptic curves with RM by $\mathcal{O}_L$.

In [TTV91], TAUTZ, TOP and VERBERKMOES constructed a one-parameter-family of hyperelliptic curves with real multiplication by $\mathbb{Q}(\sqrt{5})$ by replacing the curve $X_1(5)$ in MESTRES construction by the multiplicative group $\mathbb{G}_m$, which is the cusp at infinity of $X_1(5)$.

Theorem 2.17. *For all $\lambda \in \mathbb{Q}$ such that*

$$C_\lambda : Y^2 = X^5 - 5X^3 + 5X + \lambda$$

defines a hyperelliptic curve, $\mathrm{Jac}(C_\lambda)$ *admits RM by* $\mathbb{Q}(\alpha)$*, where* $\alpha := \zeta_5 + \zeta_5^{-1}$.

Remark. *In the paper they give a more general result. Namely if $p > 3$ is a prime, they construct a family of hyperelliptic curves defined over $\mathbb{Q}$ of genus $\frac{p-1}{2}$ with RM by $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$. But we are only interested in the case where the resulting family is a family of genus two curves.*

2.3. Igusa Invariants

In order to navigate in a variety it is very useful to have the variety described in terms of some coordinates. Since two varieties are isomorphic if and only if they define the same point in the moduli space, the introduction of computable coordinates in this space is an important tool to determine whether two given hyperelliptic curves are birationally equivalent.

As we have seen before, the space of isomorphism classes of elliptic curves can be described via the j-function. IGUSA found in his famous paper [Igu60] invariants which classify all hyperelliptic curves of genus two up to birational equivalence. They are used to determine dimensions of families of genus two hyperelliptic curves and to find isomorphisms between them.

Definition 2.13 (IGUSA Invariants)**.** *Let $C : Y^2 = X^6 + \sum_{i=1}^{5} f_i X^i =: F(X)$ be a hyperelliptic curve and denote the six pairwise different roots of F by α_i, $i = 1, \ldots, 6$. Write $(ij) := \alpha_i - \alpha_j$, $i \neq j \in \{1, \ldots, 6\}$ and set*

$$\begin{aligned}
J_2(C) :=& 2^{-3} \sum_{15 \text{ terms}} (12)^2(34)^2(56)^2 \\
J_4(C) :=& 2^{-5}3^{-1} \left(4J_2^2 - \sum_{10 \text{ terms}} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2 \right) \\
J_6(C) :=& 2^{-6}3^{-2} \big(8J_2^3 - 160 J_2 J_4 \\
& - \sum_{60 \text{ terms}} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2(14)^2(25)^2(36)^2 \right) \\
J_{10}(C) :=& 2^{-20} \Delta(C),
\end{aligned}$$

where the sums in J_{2i}, $i = 1, 2, 3$, range over all possible permutations in the summands. These invariants are called IGUSA invariants *of C.*

The following proposition makes clear why we call $(J_2(C), J_4(C), J_6(C), J_{10}(C))$ invariants.

Proposition 2.18. *Two hyperelliptic curves C/K and C'/K of genus two are isomorphic if and only if there exists $r \in \overline{K} \setminus \{0\}$ such that*

$$J_{2i}(C) = r^{2i} J_{2i}(C'),$$

for $i = 1, 2, 3, 5$.

The proof can be found in [Igu60, p. 632]. Most of the time we use the absolute IGUSA

invariants to determine whether two given hyperelliptic curves are isomorphic. For this task we introduce the *absolute* IGUSA *invariants*.

Definition 2.14. *Let C be a hyperelliptic curve of genus two such that $J_2(C) \neq 0$. Then we set*

$$\alpha(C) := \frac{J_4(C)}{J_2(C)^2}$$
$$\beta(C) := \frac{J_6(C)}{J_2(C)^3}$$
$$\gamma(C) := \frac{J_{10}(C)}{J_2(C)^5}$$

as the absolute IGUSA invariants *of C.*

With this definition and Proposition 2.18 we directly get the following corollary.

Corollary 2.19. *Two hyperelliptic curves C/K and C'/K, such that $J_2(C) \neq 0 \neq J_2(C')$, are isomorphic if and only if their absolute* IGUSA *invariants are equal.*

Remark. IGUSA *showed in his paper that with this absolute invariants it is possible to describe the* arithmetic modular variety *of hyperelliptic curves of genus two.*

If we now look at a parametrized family of hyperelliptic curves $\mathcal{C}$ of genus two over the field $\mathbb{Q}$ regarded as a hyperelliptic curve C over the function field $\mathbb{Q}(s)$, where s is the vector of the parameters in the family, we get that there are infinitely many non-isomorphic hyperelliptic curves in the family $\mathcal{C}$ if and only if one of $\alpha(C), \beta(C), \gamma(C)$ is non-constant.

3. Rational Torsion Points on Jacobians of Curves

This chapter is one of the central ones in this thesis. Here we present different approaches to the explicit construction of certain torsion structures on jacobians of algebraic curves. We give a partial answer to the following problem.

Problem. *Given a positive integers N, g and a field K, is it possible to find an abelian variety $A_{/K}$ of dimension g such that*

$$N | \#A_{tors}(K)?$$

More precisely, for given positive integers N, g and a field K, we construct abelian varieties of dimension g defined over K with a K-ratoinal point of exact order N. We are mainly interested in the case where $K = \mathbb{Q}$. In order to achieve a solution to the stated problem, it is of importance to be able to perform computations in the abelian variety.

The used methods are a mix of already known methods due to Flynn and Leprévost, classical constructions motivated by number fields and new approaches. We are able to present new examples of hyperelliptic curves defined over $\mathbb{Q}$ and some number fields of small degree admitting a torsion point of prescribed order on their jacobian.

For the elliptic curves the question for rational torsion points is answered for several fields. The most prominent result is the theorem of Mazur which classifies all possible $\mathbb{Q}$-rational torsion subgroups of elliptic curves.

Theorem 3.1 ([Maz77])**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Then $E_{tors}(\mathbb{Q})$ is isomorphic to one of the following groups.*

$$E_{tors}(\mathbb{Q}) \cong \begin{cases} \mathbb{Z}/n\mathbb{Z} & 1 \leq n \leq 10 \text{ or } n = 12 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} & 1 \leq n \leq 4. \end{cases}$$

Furthermore, for all occurring groups in the theorem there exists an infinite family of non-isomorphic elliptic curves admitting this group as a torsion subgroup. Historically,

first a parametrization of the curves with a given torsion subgroup was found and afterwards it was shown that no other subgroups can occur.

Theorem 3.2 ([Kub76])**.** *Each of the groups in Theorem 3.1 occur for infinitely many different j-invariants.*

For jacobians of hyperelliptic curves we do not expect to succeed with the methods from the elliptic curves defined over a number field since we essentially exploit that the regarded moduli spaces are of dimension one. This gives us the tool of using jacobians of the modular curves, see [Maz77]. For hyperelliptic curves of genus g we have a moduli space of dimension $2g-1$ since every hyperelliptic curve C defined over K with $\mathrm{char}(K) \neq 2$ is $\overline{K}$-isomorphic to a curve of the form $Y^2 = X(X-1)\widetilde{F}$, where $\widetilde{F}$ is a monic polynomial of degree $\deg(\widetilde{F}) = 2g-1$. This is known as the Rosenhain form of the hyperelliptic curve C. For abelian varieties of dimension g it seems to be even harder since $\dim(\mathcal{A}_g) = \frac{g(g+1)}{2}$. So at the moment it is unknown how to obtain an analogous result for hyperelliptic curves to Theorem 3.1.

The goal of this section is to present different methods for the construction of families and examples of curves defined over a number field K with a certain K-rational torsion point on the jacobian. At first we present methods for hyperelliptic curves. The central object in all methods is some norm equation (see Definition 1.21) in the coordinate ring of a curve defined over a rational function field over $\mathbb{Q}$. A solution to such an equation then yields a curve with the desired properties. We start solving norm equations by comparing coefficients in these equations. Even for small torsion orders, this approach leads to very complicated systems of polynomial equations in the parameter.

Later, we use more sophisticated approaches for the construction of torsion divisors. The first method to solve norm equation of the form

$$a^2 - Fb^2 = u^N$$

for polynomials $a, b, u, F \in K[X]$ and some give positive integer N is to use a lifting idea which is based on Hensel's Lemma. We first construct a solution

$$R^2 \equiv u \pmod{b}$$

which we can lift to a solution modulo b^2. This approach was already used by Leprévost in [Lep91a] to construct hyperelliptic curves of genus two with a 13-torsion divisor. We extend this approach to find for a given prime p a hyperelliptic curve C whose genus depends on the prime with a torsion point of order p.

Furthermore, we are able to construct a new example of a hyperelliptic curve of genus two defined over a number field of degree seven with a 17-torsion divisor. Results of this

form were not known prior to this thesis.

The second method for solving norm equations is to investigate a special norm equation which is related to the units in the coordinate ring of the curve. These equations are known as Pell's Equations and can be solved by continued fraction expansion algorithms. The analysis of continued fraction expansions in series of number fields and function fields has a long tradition. A very systematic treatment of these expansions can be found in the thesis of Patterson [Pat07] and van der Poorten [vdP04b] and [vdP04a].

Following an approach of Flynn [Fly90], we do not try to solve the above mentioned norm equation directly but impose multiple different norm equations which can be combined to the desired form. In [Lep93] Leprévost constructs the so far known record for a point of prime order on the jacobian of a genus two hyperelliptic curve. We state a combination of the methods described by Flynn and Leprévost and construct new examples of hyperelliptic curves with a large torsion point on the jacobian. Our examples are not only defined over the rational numbers, but also over small degree number fields. Examples over number fields were not known until now.

Besides the study of hyperelliptic curves, we also consider series of superelliptic curves with a torsion point of given order on the jacobian. For superelliptic curves some of the methods we use for hyperelliptic curves still work. For example we can use Hensel's Lemma to find a solution for a norm equation of the form $a^k - Fb^k = X^p$. In higher degree function fields it becomes more difficult to find explicit solutions to certain norm equations. For certain number fields there exists an algorithm due to Voronoi which computes the fundamental units of the ring of integers under some constraints on the splitting behavior of the infinite place. In the last part of this section we are able to show that exactly the same algorithm works for function fields of characteristic zero. In the positive characteristic case the correctness of this algorithm is shown in different settings. See for example [SS00] or the thesis of Tang [Tan11]. Using this algorithm we find two series of degree three function fields with a large unit and hence, series of curves with a torsion point of large order on the jacobian.

3.1. Using Explicit Formulae

In this section we briefly want to mention the most explicit way to determine torsion points on the jacobian. For this purpose we use the explicit formulas for computation in the jacobian mentioned in Section 1.4.5. Since the degree of the formulas is large with respect to N, this attempt to describe the rational torsion points becomes hard even for small torsion orders. We start with the generic hyperelliptic curve of genus two, or some other family of hyperelliptic curves, with a generic point on its jacobian. The representation of the point depends on the formula we want to use. For example

for the CANTOR algorithm we represent a point on the jacobian by the MUMFORD representation and for the explicit formulas for the jacobian in $\mathbb{P}^{15}$ we represent a point by a 2-tuple of points on the curve with affine coordinates.

Using CANTOR's algorithm, FLYNN's formulae for the embedded curve in $\mathbb{P}^{15}$ and the division polynomials due to CANTOR for computing a multiple of a generic point on a family of hyperelliptic curves give way too large algebraic expressions in the parameters, so we do not present them here. We only give an example which uses the duplication formula due to FLYNN on the KUMMER surface of the jacobian of a hyperelliptic curve of genus two. But even here, we are neither able to give an example for a three-torsion point nor prove the non-existence of a example in this particular family.

Example 3.1. *Let*

$$C_\lambda : Y^2 = \lambda X^6 + 5X^5 - 5X^3 + X$$

be the family of hyperelliptic curves with RM constructed by TOP, TAUTZ *and* VERBERKMOES *and let* $\{P, Q\}$ *represent a* $\mathbb{Q}(\lambda)$*-rational divisor* D *on* C_λ*. Furthermore, assume* $D \in \mathrm{Jac}(C_\lambda)[3]$*. This implies* $2D = -D$ *on the jacobian, but taking the image in the* KUMMER *surface yields*

$$\delta_2(\kappa(D)) = \kappa(D).$$

Applying the formulae for δ_2 *given in Appendix B, this relation gives us three equations in the parameter* λ *and the four coordinate parameters of* P *and* Q*. Since* $S \in C$*, we have*

$$y(S)^2 = \lambda x(S)^6 + 5x(S)^5 - 5x(S)^3 + x(S)$$

for $S \in \{P, Q\}$*. Thus, we get five equations in the five indeterminates* $\lambda, x(P), y(P), x(Q)$ *and* $y(Q)$*. These equations define a zero-dimensional algebraic set. Unfortunately, the description of this algebraic set is so complicated that we could not actually find such a point.*

As we can see in this example it seems to be hard to construct torsion points of large order by this method. Therefore, it is much more convenient not to use the addition formulae on the jacobians directly, but conditions on objects immediately related to a point on the jacobian, for example certain relations in the function field of the curve or certain relations of divisors of the underlying hyperelliptic curve.

3.2. Solving Norm Equations

In this section we relate the norm of elements in the function field of a curve with torsion divisors on the jacobian of the curve defined over $\mathbb{Q}$. This connection of these two objects plays a central role in all constructions of torsion points of large order on jacobians of curves. After proving this connection, we make direct use of it to explicitly describe a one-dimensional family of hyperelliptic curves of genus two with a five-torsion divisor and an example of a hyperelliptic curve of genus two with a seven-torsion divisor.

Since points in the jacobian of a curve can be described as divisors of degree zero modulo principal divisors, we get a direct connection between elements in the function field of the curve and divisors which are equivalent to zero in the jacobian. We are especially interested in functions $f \in K(C)$, where C is a curve over the field K, such that $\mathrm{div}(f) = ND$ for some degree zero divisor D and some integer N. The existence of such a function f is equivalent with the existence of a torsion point of order dividing N. This observation we make explicit in the following two lemmas.

Lemma 3.3. *Assume $C/\mathbb{Q} : Y^2 = F(X)$ is a hyperelliptic curve of genus two with a $\mathbb{Q}$-rational* Weierstrass *point. Assume further that there is a point $D \in \mathrm{Jac}(C)[N](\mathbb{Q})$ for a given natural number N. Then there exists a function $f \in \mathbb{Q}(C)$ such that*

$$\mathrm{N}_{\overline{\mathbb{Q}}(C)/\overline{\mathbb{Q}}(x)}(f) = \varepsilon u(x)^N$$

for some polynomial $u \in \mathbb{Q}[X] \setminus \mathbb{Q}$ with $\deg(u) \leq 2$ and $\varepsilon \in \mathbb{Q}^*$.

Proof : Let $C/\mathbb{Q} : Y^2 = F(X)$ be a hyperelliptic curve of genus two with $\deg(F) = 5$. Now we know that every point $D \in \mathrm{Jac}(C)(\mathbb{Q})$ can be represented by two points

$$Q_1 \neq Q_2 \in C(\mathbb{Q}) \cup \{P_\infty\} \text{ or } Q_1, Q_2 = Q_1^\sigma \in C(K)$$

for some quadratic extension $\mathbb{Q} \subset K$, where σ is the non-trivial automorphism of K over $\mathbb{Q}$. So write $D = Q_1 + Q_2 - 2P_\infty$. The assumption that D is of order dividing N translates to the fact that

$$\mathcal{O} = ND = NQ_1 + NQ_2 - 2NP_\infty.$$

We have to look at two different cases.

1. case $P_\infty \notin \{Q_1, Q_2\}$:
   Thus there exists a function $f \in \mathbb{Q}(C)$ which has a pole of order $2N$ at P_∞ and nowhere else and a zero of order N at the two points Q_1 and Q_2. So we can deduce

that $f \in \mathcal{L}(2NP_\infty)$ and f can be written in the form

$$f = a(x) + b(x)y$$

with polynomials $a, b \in \mathbb{Q}[X]$ by Lemma 1.8. Since Q_1 and Q_2 are assumed to be N-fold zeros of f, we get

$$f(Q_i) = a(x(Q_i)) + y(Q_i)b(x(Q_i)) = 0$$

for $i = 1, 2$. This implies that

$$a(x(Q_i))^2 - b(x(Q_i))^2 F(x(Q_i)) = 0.$$

Therefore, we get that $(X - x(Q_i))^N$ divides $a^2 - b^2F$ for $i = 1, 2$. By comparing degrees, we obtain

$$a(x)^2 - b(x)^2 F(x) = \mathrm{N}_{\overline{\mathbb{Q}}(C)/\overline{\mathbb{Q}}(x)}(f) = \varepsilon(x - x(Q_1))^N (x - x(Q_2))^N$$

and the lemma is proven since $(X - x(Q_1))(X - x(Q_2)) \in \mathbb{Q}[X]$ by assumption.

2. case $P_\infty \in \{Q_1, Q_2\}$:
We can assume without loss of generality that $Q_2 = P_\infty$, so we get $D = Q_1 - P_\infty$ and $Q_1 \in C(\mathbb{Q})$. Hence there exists a function $f \in \mathcal{L}(NP_\infty)$ with a N-fold zero at Q_1 and no zeros elsewhere. With the same arguments as above we get

$$a^2 - b^2 F = \mathrm{N}_{\overline{\mathbb{Q}}(C)/\overline{\mathbb{Q}}(x)}(f) = \varepsilon(x - x(Q_1))^N$$

for some $\varepsilon \in \mathbb{Q}^*$. □

Remark. *The polynomial u in Lemma 3.3 gives the first coordinate of the* Mumford *representation of the point $D \in \mathrm{Jac}(C)$. Obviously the assertion in the lemma can also be formulated for curves of arbitrary genus and for curves without a $\mathbb{Q}$-rational* Weierstrass *point. The proofs are completely analogous to the given one, but we would have to consider a lot more cases. Since this gives no further insights, we restricted ourselves to the most simple case.*

The next lemma states that the converse of Lemma 3.3 is also true.

Lemma 3.4. *Let $C/\mathbb{Q}$ be a hyperelliptic curve of genus two with a $\mathbb{Q}$-rational* Weierstrass *point and $D \in \mathrm{Jac}(C)(\mathbb{Q})$ having first coordinate in* Mumford *representation equal to the polynomial u with $1 \leq \deg(u) \leq 2$. If there exists a function $f \in \mathcal{L}(\deg(u)NP_\infty)$ such that $\mathrm{N}_{\overline{\mathbb{Q}}(C)/\overline{\mathbb{Q}}(x)}(f) = \varepsilon u^N$ for some $\varepsilon \in \mathbb{Q}^*$, then $\mathrm{ord}(D) | N$.*

Proof : Assume $C/\mathbb{Q}$ is a hyperelliptic curve of genus two and there exists a function $f \in \mathcal{L}(\deg(u)NP_\infty)$ such that

$$\mathrm{N}_{\overline{\mathbb{Q}}(C)/\overline{\mathbb{Q}}(x)}(f) = \varepsilon u^N.$$

Then the principal divisor of f is

$$\mathrm{div}(f) = NQ_1 + NQ_2 - 2NP_\infty$$

for some points $Q_1, Q_2 \in C$ such that $u(x(Q_i)) = 0$. Therefore,

$$N(Q_1 + Q_2 - 2P_\infty)$$

has to be the identity in the jacobian. Hence, the divisor $(Q_1 + Q_2 - 2P_\infty)$ has to be of order dividing N. □

Remark. *Again, this can easily be generalized to curves with arbitrary genus.*

We use these two lemmas to produce families of hyperelliptic curves admitting a point of certain order on their jacobians. The strategy is to take a parametrized family $\mathcal{C}$ of hyperelliptic curves and assume the existence of a function $f \in \mathbb{Q}(C)$ with a norm equal to

$$\mathrm{N}_{\overline{\mathbb{Q}}(C)/\overline{\mathbb{Q}}(x)}(f) = \varepsilon u^N$$

for $C \in \mathcal{C}$. Then, by comparing coefficients, we get equations in the parameters of the family $\mathcal{C}$, the parameters of the function f and the u-coordinate of the potential point of order N. If we further start with a prime N, we can be sure that on every constructed curve there is a point of exact order N on the jacobian.

We compute an example of this construction for five-torsion. We start with the universal hyperelliptic curve of genus two. Since the equations we are dealing with are rather complicated, we restrict the functions $f \in \mathcal{L}(10P_\infty)$ to be in the subvectorspace spanned by $\{1, x, x^2, x^3, x^4, x^5, y\}$.

Set

$$\begin{aligned}
f_5 &:= -\frac{3}{128}\lambda^5 + \frac{5}{16}\lambda^3\mu - \frac{15}{8}\lambda\mu^2 + 2\eta,\\
f_4 &:= -\frac{25}{512}\lambda^6 + \frac{85}{128}\lambda^4\mu - \frac{135}{32}\lambda^2\mu^2 + 5\lambda\eta - \frac{5}{8}\mu^3,\\
f_3 &:= -\frac{25}{1024}\lambda^7 + \frac{75}{256}\lambda^5\mu - \frac{115}{64}\lambda^3\mu^2 + \frac{15}{4}\lambda^2\eta - \frac{95}{16}\lambda\mu^3 + 5\mu\eta,\\
f_2 &:= \frac{25}{16384}\lambda^8 - \frac{75}{1024}\lambda^6\mu + \frac{375}{512}\lambda^4\mu^2 + \frac{5}{8}\lambda^3\eta - \frac{415}{64}\lambda^2\mu^3 + \frac{15}{2}\lambda\mu\eta - \frac{95}{64}\mu^4,
\end{aligned}$$

$$f_1 := -\frac{5}{64}\lambda^4\eta + \frac{15}{8}\lambda^2\mu\eta - 5\lambda\mu^4 + \frac{15}{4}\mu^2\eta,$$
$$f_0 := \eta^2 - \mu^5.$$

Proposition 3.5. *The family*

$$C_{\lambda,\mu,\eta} : y^2 = f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0,$$

generically admits a $\mathbb{Q}$-rational point of order 5 on its jacobian.

The u-coordinate of this point in MUMFORD*-representation is given by the polynomial*

$$u := x^2 + \lambda x + \mu.$$

Proof : Let

$$C : Y^2 = f_5X^5 + f_4X^4 + f_3X^3 + f_2X^2 + f_1X + f_0 =: F(X)$$

be the universal hyperelliptic curve of genus two with one rational WEIERSTRASS-Point at infinity. Assume $x^2 + \lambda x + \mu$ to be the first coordinate of a $\mathbb{Q}$-rational point

$$D := P_1 + P_2 - 2P_\infty \in \mathrm{Jac}(C)[5](\mathbb{Q})$$

of order five on the jacobian $\mathrm{Jac}(C)$ in MUMFORD-representation. Since we have assumed $D \in \mathrm{Jac}(C)[5]$, we have $l(5D) \geq 1$. This means that there exists a function $f \in \mathbb{Q}(C)$ of norm $\varepsilon(x^2 + \lambda x + \mu)^5$ by Lemma 3.3. So there is a solution to the equation

$$a^2 - Fb^2 = \varepsilon(X^2 + \lambda X + \mu)^5,$$

where a and b are polynomials in X. By assuming $b = 1$, we can simplify the equation to

$$a^2 - F = (X^2 + \lambda X + \mu)^5,$$

where a has to be monic of degree five. Setting

$$a := \eta + a_1X + a_2X^2 + a_3X^3 + a_4X^4 + X^5$$

and by comparing coefficients of both sides of the equation, we get the equations for $f_0, \ldots, f_5$. □

The family $C_{\lambda,\mu,\eta}$ in Proposition 3.5 is one-dimensional as we can see with the following considerations. First we consider the subfamily given by $\lambda := 1$ and $\mu := 0$ and show that

this family is one-dimensional. This is done by computing the absolute IGUSA invariants of this family. These are given by

$$\begin{aligned}
\alpha(C_{1,0,\eta}) &= \frac{\frac{17}{2^4 3^3 5}\eta^4 - \frac{17}{2^{10}3^3 5}\eta^3 + \frac{1399}{2^{21}3^3 5}\eta^2 - \frac{35}{2^{28}3^2}\eta + \frac{175}{2^{38}3^4}}{(\eta^2 - \frac{3}{2^7}\eta + \frac{25}{2^{14}3^2})^2} \\
\beta(C_{1,0,\eta}) &= \frac{h}{(\eta^2 - \frac{3}{2^7}\eta + \frac{25}{2^{14}3^2})^3} \\
\gamma(C_{1,0,\eta}) &= \frac{\eta^5(\eta - \frac{3}{2^7})^5(\eta - \frac{3}{2^8})^2(\eta^2 - \frac{3}{2^7}\eta + \frac{1}{2^{16}})}{(\eta^2 - \frac{3}{2^7}\eta + \frac{25}{2^{14}3^2})^5},
\end{aligned}$$

where h is a polynomial of degree eight in η.

Since these invariants are non-constant rational functions in the parameter η, we get that there are infinitely many pairwise non-isomorphic curves in this family. So the family $C_{1,0,\eta}$ has to be one-dimensional. Therefore, the dimension of $C_{\lambda,\mu,\eta}$ has to be at least one.

The next step is to show that for every choice of $\lambda, \mu, \eta \in \mathbb{Q}$ there exists a $\eta' \in \overline{\mathbb{Q}}$ such that $C_{\lambda,\mu,\eta} \cong C_{1,0,\eta'}$. To show this we look at the differences of the absolute IGUSA invariants of $C_{\lambda,\mu,\eta}$ and $C_{1,0,\eta'}$ and compute the greatest common divisor d of their nominators. This is given by $d = d_2\eta'^2 + d_1\eta' + d_0$, where

$$\begin{aligned}
d_2 :=& \lambda^{10} - 20\lambda^8\mu + 160\lambda^6\mu^2 - 640\lambda^4\mu^3 + 1280\lambda^2\mu^4 - 1024\mu^5, \\
d_1 :=& 24\mu^5 - 30\lambda^2\mu^4 + 15\lambda^4\mu^3 - \frac{15}{4}\lambda^6\mu^2 + \frac{15}{32}\lambda^8\mu - \frac{3}{128}\lambda^{10}, \\
d_0 :=& \frac{15}{8}\lambda\mu^2\eta - \frac{9}{64}\mu^5 - \eta^2 - \frac{45}{64}\lambda^2\mu^4 - \frac{5}{16}\lambda^3\mu\eta + \frac{3}{128}\lambda^5\eta - \frac{25}{1024}\lambda^6\mu^2 \\
&+ \frac{105}{512}\lambda^4\mu^3 + \frac{15}{16384}\lambda^8\mu.
\end{aligned}$$

So for any given $\lambda, \mu, \eta \in \mathbb{Q}$ we can find $\eta' \in \overline{\mathbb{Q}}$ such that $d = 0$. Therefore, $C_{\lambda,\mu,\eta} \cong C_{1,0,\eta'}$ over $\overline{\mathbb{Q}}$. We now check under what conditions this isomorphism is defined over the rational numbers. This is done by computing the roots of the polynomial d and check when these are defined over $\mathbb{Q}(\lambda, \mu, \eta)$. Since d is a polynomial of degree two, we can easily determine its roots. These roots are rational if and only if

$$\frac{d_1^2}{4d_2^2} - \frac{d_0}{d_2} = \frac{3^2(\lambda^5 - \frac{40}{3}\lambda^3\mu + 80\lambda\mu^2 - \frac{256}{3}\eta)^2}{256^2(\lambda^2 - 4\mu)^5}$$

is a square in $\mathbb{Q}$. This is true if and only if $\lambda^2 - 4\mu$ is a square in $\mathbb{Q}$. This answers the question of the field of definition of the isomorphism described above.

We also have tried to construct a family of curves defined over $\mathbb{Q}$ admitting a seven-torsion point on their jacobians. But the restriction to functions in $\langle 1, y, x, \ldots, x^7\rangle_{\mathbb{Q}}$

just leads to the empty family. Allowing functions in the whole space $\mathcal{L}(14P_\infty)$ gives equations which define a four-dimensional parameter space. Since these equations are rather large, we do not state them here. The following example is the fiber above a rational point in the mentioned parameter space.

Example 3.2. *Let* $C : Y^2 = F(X)$ *with*

$$F = X^5 - \frac{39}{4}X^4 + 65X^3 - 146X^2 + 198X - 127.$$

Then there exists a non-trivial point D *in* $\mathrm{Jac}(C)[7](\mathbb{Q})$.

The attempt to construct in this direct approach a family of curves with a seven-torsion point on their jacobians shows that in order to construct large torsion orders one has to be able to find $\mathbb{Q}$-rational points in affine varieties which are given by complicated polynomials in the parameters.

3.3. Hensel Lifting

In the preceding section we have seen that the approach of directly solving the norm equation leads to complicated equations even for a small prime like seven.

As in the preceding section we are looking for a possibility to construct a solution of a norm equation in the coordinate ring of a curve. Let us first make some assumptions on the curve C. Let $C : Y^2 = F(X)$ be a hyperelliptic curve of genus two defined over $\mathbb{Q}$ and assume the support of the divisor at infinity D_∞ is contained in one Galois orbit (i.e. $\deg(F)$ is odd or the leading coefficient is not a square).

We make this assumption to be able to handle the pole orders at the points at infinity of the constructed function. Assume further $D := P + Q - D_\infty$ is a p-torsion divisor on C for some prime $p \neq 2$. Then we get with Lemma 3.4 of the preceding section that there exists a function

$$a(x) + yb(x) =: f \in \mathcal{O}(C)$$

such that

$$a^2 - Fb^2 = \varepsilon u^p,$$

for some $\varepsilon \in K^*$ and some polynomial $u \in K[X]$ of degree two. Then

$$F = \frac{a^2 - \varepsilon u^p}{b^2},$$

where all the terms are polynomials in X. Therefore, we require $a^2 \equiv \varepsilon u^p \pmod{b^2}$.

For simplification we introduce the following notation.

Notation 3.1. *Let K be a field and $a, b \in K[X]$. Then we write $a \mod b \in K[X]$ for the unique polynomial $h \in K[X]$ with $\deg h \leq b$ and $h \equiv a \pmod{b}$.*

In order to find a solution to this congruence we make use of the following lemmas.

Lemma 3.6 (Hensel's Lemma, [Hen18])**.** *Let K be a field with $\mathrm{char}(K) \neq 2$ and $b, R \in K[X]$ with $\gcd(b, R) = 1$. Assume that there exists a polynomial $g \in K[X][Y]$ with $g = Y^2 + u$ for some $u \in K[X]$ with $g(R) \equiv 0 \pmod{b}$. Then there exists a polynomial $\widetilde{R} \in K[X]$ such that*

$$\begin{aligned} \widetilde{R} &\equiv R \pmod{b} \\ g(\widetilde{R}) &\equiv 0 \pmod{b^2}. \end{aligned}$$

This polynomial $\widetilde{R}$ is unique up to multiples of b^2.

Proof : Assume that there are $b, R \in K[X]$ and $g \in K[X][Y]$ such that $\gcd(b, R) = 1$ and $g(R) \equiv 0 \pmod{b}$. Set $\lambda_1 := \frac{g(R)}{b}$. Then λ_1 is in $K[X]$ since $g(R) \equiv 0 \pmod{b}$ is

assumed. Further set $\lambda_2 := -\frac{\lambda_1}{2R} \mod b$. Since $\gcd(R, b) = 1$ and $\mathrm{char}(K) \neq 2$ hold by assumption, $2R$ is invertible modulo b. Therefore, λ_2 is an element of $K[X]$ with $\deg(\lambda_2) < \deg(b)$. Now set $\widetilde{R} := R + \lambda_2 b$. Obviously, $\widetilde{R} \equiv R \pmod b$. Further we calculate

$$\begin{aligned} g(\widetilde{R}) = g(R + \lambda_2 b) &= R^2 + 2R\lambda_2 b + \lambda_2^2 b^2 + u \\ &\equiv R^2 + 2R\lambda_2 b + u &&\equiv R^2 - \frac{2R\lambda_1 b}{2R} + u \\ &\equiv g(R) - \lambda_1 b &&\equiv 0 \pmod{b^2}. \end{aligned}$$

So it is only left to show that this solution $\widetilde{R}$ is unique. If $\widetilde{R_2}$ is another solution, we directly get that $\widetilde{R_2}$ and R can only differ by a multiple of b. So $\widetilde{R_2} = R + \mu b$ for some polynomial $\mu \in R$. Since we assumed that $\widetilde{R_2}$ is a solution, we have

$$\begin{aligned} 0 \equiv g(\widetilde{R_2}) &= g(R + \mu b) \\ = R^2 + 2R\mu b + \mu^2 b^2 + u &\equiv R^2 + u + 2R\mu b = g(R) + 2R\mu b. \end{aligned}$$

This is equivalent to $\mu \equiv \lambda_2 \pmod b$ by the way λ_2 was constructed. Therefore, we have $\widetilde{R} \equiv \widetilde{R_2} \pmod{b^2}$. This completes the proof of this special version of Hensel's Lemma. □

We now use this version of Hensel's Lemma to give a criterion for when it is possible to find a solution to the norm equation.

Lemma 3.7. *Let N be a positive integer, K a field with $\mathrm{char}(K) \neq 2$ and $b, u \in K[X]$ polynomials such that $\gcd(b, u) = 1$ and u is a square modulo b. Then for all $\varepsilon \in K^*$ there exist polynomials $a, F \in K[X]$ such that the following equation holds true:*

$$a^2 - b^2 F = \varepsilon^2 u^N.$$

Proof : Assume $u \equiv R^2 \pmod b$ for some $R \in K[X]$. Since $\gcd(u, b) = 1$, we directly get $\gcd(R, b) = 1$. Therefore, by the Lemma of Hensel 3.6 there exists a polynomial $\widetilde{R} \in K[X]$ such that $u \equiv \widetilde{R}^2 \pmod{b^2}$. Setting $a := \varepsilon \widetilde{R}^N \mod b^2$, we get

$$a^2 \equiv \varepsilon^2 u^N \pmod{b^2}.$$

Therefore, there exists a polynomial $F \in K[X]$ such that

$$a^2 - b^2 F = \varepsilon^2 u^N.$$ □

By using Lemma 3.7, we construct an example of a family of hyperelliptic curves

defined over $\mathbb{Q}$ with a $\mathbb{Q}$-rational seven-torsion point on its jacobian. First we fix the polynomial b in such a way that there exist squares of degree two in the algebra

$$\mathbb{Q}(\alpha) := {}^{\mathbb{Q}[X]}\!/_{(b)}$$

that do not come from squares in $\mathbb{Q}[X]$. For example fix an odd prime p. Then the polynomials

$$b_\lambda := X^{p-3} + 2\lambda X^{\frac{p-1}{2}} + 2 \text{ and } u := \lambda^2 X^2 - 2$$

have no common factors and in ${}^{\mathbb{Q}[X]}\!/_{(b_\lambda)}$ we have

$$(X^{\frac{p-3}{2}} + \lambda X)^2 = X^{p-3} + 2\lambda X^{\frac{p-1}{2}} + \lambda^2 X^2 = b - 2 + \lambda^2 X^2 \equiv (\lambda^2 X^2 - 2) \pmod{b_\lambda}.$$

So we have found polynomials $b_\lambda, u \in \mathbb{Q}[X]$ such that the conditions of Lemma 3.7 are fulfilled, therefore, there exist polynomials $a, F \in \mathbb{Q}[X]$ fulfilling $a^2 - Fb_\lambda^2 = \varepsilon u^p$, where $\varepsilon \in \mathbb{Q}^*$. We now check the degrees of the polynomials we constructed. We have $\deg(b_\lambda) = 4$, so we get $\deg(a) \leq 7$. This is enough to compute the degree of the constructed polynomial F:

$$\begin{aligned}\deg(F) &= \deg\left(\frac{a^2 - u^p}{b_\lambda^2}\right) = \max(2\deg(a), p\deg(u)) - 2\deg(b_\lambda) \\ &= \max(2\deg(a), 2p) - 2p + 6\end{aligned}$$

The second equality holds since the degrees of a^2 and u^p are different by construction. This gives us that the degree of the polynomial F is six if and only if the degree of a is less or equal to p. Since one summand of a is $\lambda_2 b$, the degree of a is less or equal to p if and only if the degree of λ_2 is less or equal to three. So only for $p = 7$ we can be sure to get a polynomial F of the right degree.

It would be a nice result to have a criterion when it is possible to find a λ_2 of the right degree for larger primes.

Let us now go through the construction for the special case $p = 7$. In order to compute a explicit example we start with the polynomial $b_\lambda := X^4 + 2\lambda X^3 + 2$. Then the relation

$$(X^2 + \lambda X)^2 \equiv \lambda^2 X^2 - 2 \pmod{b_\lambda}$$

holds. We set $u := \lambda^2 X^2 - 2$ and compute $\lambda_1 = 1$. If we further set

$$c := \frac{1}{\lambda^8 - 4\lambda^4 + 4}, \qquad a_7 := \left(\frac{1}{8}\lambda^7 - \frac{1}{2}\lambda^3\right), \qquad a_6 := \left(\frac{1}{2}\lambda^8 - 2\lambda^4 + \frac{1}{2}\right),$$

$$a_5 := \left(\frac{1}{2}\lambda^9 - 2\lambda^5 + \frac{3}{2}\lambda\right), \quad a_4 := \frac{1}{2}\lambda^2, \quad a_3 := \left(\frac{1}{2}\lambda^7 - \frac{5}{2}\lambda^3\right),$$
$$a_2 := \left(\lambda^8 - \frac{7}{2}\lambda^4 + 2\right), \quad a_1 := \left(-\frac{1}{2}\lambda^5 + 2\lambda\right), \quad a_0 := \frac{1}{2}\lambda^6 - 2\lambda^2,$$

this gives us $\lambda_2 = c\sum_{i=0}^{7} a_i X^i$.

Hence, the congruence

$$\left((X^2 + \lambda X) + \lambda_2(X^4 + 2\lambda X^3 + 2)\right)^2 \equiv \lambda^2 X^2 - 2 \pmod{(X^4 + 2\lambda X^3 + 2)^2}$$

holds by construction.

Taking the 7^{th} power of the square root of the left hand side modulo b_λ^2, we obtain the polynomial

$$\begin{aligned} a_\lambda =& (-\lambda^7 - 2\lambda^3)X^7 + (-9\lambda^4 - 2)X^6 + (-5\lambda^5 - 6\lambda)X^5 + (-4\lambda^6 + 4\lambda^2)X^4 \\ &+ (2\lambda^4 - 12)X^2 + (-2\lambda^5 - 12\lambda)X - 8\lambda^2. \end{aligned}$$

Now we are able to compute the defining polynomial

$$F_\lambda = \frac{a_\lambda^2 - u^7}{b_\lambda^2}.$$

This gives us

$$\begin{aligned} F_\lambda :=& (4\lambda^{10} + 4\lambda^6)X^6 + (2\lambda^{11} + 24\lambda^7 + 8\lambda^3)X^5 + (\lambda^8 + 28\lambda^4 + 4)X^4 \\ &- (-2\lambda^9 - 32\lambda^5 + 8\lambda)X^3 - (\lambda^{10} + 4\lambda^6 - 28\lambda^2)X^2 + (8\lambda^7 + 48\lambda^3)X + 16\lambda^4 + 32. \end{aligned}$$

The polynomial F_λ defines a hyperelliptic curve of genus two for any $\lambda \in \mathbb{Q} \setminus \{0\}$ since the discriminant of the curve above is

$$\Delta(C) = 2^{19}\lambda^{14}(\lambda^4 - 2)^{17}(27\lambda^{12} + 2428\lambda^8 - 3844\lambda^4 - 512).$$

This discriminant is non-zero, therefore, $C/\mathbb{Q}(\lambda)$ is hyperelliptic. Let now λ be a rational number. Then the discriminant of the specialization of C to λ is zero if and only if $\lambda = 0$ since all other factors of $\Delta(C_\lambda)$ are irreducible over $\mathbb{Q}$.

Lemma 3.8. *Let $\lambda \in \mathbb{Q}$ be a rational number. Then $\lambda^4 + 1$ is a square in $\mathbb{Q}$ if and only if $\lambda = 0$.*

Proof : A solution (y, λ) to $Y^2 = X^4 + 1$ with $\lambda \neq 0$ yields a non-trivial solution to the FERMAT equation $X^4 + Y^4 = Z^4$ and thus can not exist. □

Example 3.3. *Let $0 \neq \lambda \in \mathbb{Q}$. Then the curve $C_\lambda : Y^2 = F_\lambda(X)$, where*

$$\begin{aligned} F_\lambda :=& (4\lambda^{10} + 4\lambda^6)X^6 + (2\lambda^{11} + 24\lambda^7 + 8\lambda^3)X^5 + (\lambda^8 + 28\lambda^4 + 4)X^4 \\ & - (-2\lambda^9 - 32\lambda^5 + 8\lambda)X^3 - (\lambda^{10} + 4\lambda^6 - 28\lambda^2)X^2 + (8\lambda^7 + 48\lambda^3)X + 16\lambda^4 + 32, \end{aligned}$$

is a hyperelliptic curve of genus two with a $\mathbb{Q}$-rational seven-torsion point on its jacobian.

Proof : By the discussion above the curve is hyperelliptic of genus two for $\lambda \neq 0$. In Lemma 3.8 we know that the leading coefficient of F_λ is a square if and only if $\lambda = 0$. Therefore, we have for $\lambda \neq 0$ that the points at infinity of C_λ lie in one Galois orbit. So by construction C_λ admits a seven-torsion points on its jacobian. □

Following the arguments from the seven-torsion example, we now want to construct a hyperelliptic curve with a jacobian containing a rational eleven-torsion point. Since we have seen it is most likely that our strategy fails in general, we have to adjust it slightly. By the discussion above, the bottleneck of the method is the degree of the number field we are working in. But this degree can be reduced by a small change in the method.

Instead of looking at divisors $D := P + Q - D_\infty$, we now assume that our hyperelliptic curve has only one point at infinity. So we want to construct a degree five polynomial F such that $C : Y^2 = F(X)$ is a hyperelliptic curve of genus two with a jacobian admitting a torsion point on the image of the curve under the embedding given by this point at infinity. That is, we are now looking at a divisor of the form $D := P - P_\infty \in \mathrm{Jac}(C)[p](\mathbb{Q})$.

So a function f with principal divisor $\mathrm{div}(f) = pD$ lives in $\mathcal{L}(pP_\infty)$. Therefore, we can use the construction as above in a number field of degree $\frac{p-5}{2}$.

Let $K := \mathbb{Q}(\alpha)$ be a number field with $\alpha^3 = 2$. Then the following holds in K.

$$\left(\alpha^2 + \alpha - \frac{1}{2}\right)^2 = \alpha^4 + 2\alpha^3 - \alpha + \frac{1}{4} = (\alpha^3 - 2)(\alpha + 2) + \alpha + \frac{17}{4} = \alpha + \frac{17}{4}$$

Taking this relation and applying Hensel's Lemma, we get with

$$\begin{aligned} f_5 &:= -1 & f_2 &:= -\frac{1452831199375}{1048576} \\ f_4 &:= \frac{102384544793}{262144} & f_1 &:= -\frac{454968393185}{131072} \\ f_3 &:= \frac{63111601615}{262144} & f_0 &:= -\frac{666157168727}{524288}, \end{aligned}$$

the following theorem.

Theorem 3.9. *The curve $C : Y^2 = \sum_{i=0}^{5} f_i X^i =: F(X)$, where the f_i are as above, is a hyperelliptic curve of genus two and has a point of order eleven on the image of the curve in its jacobian.*

3.3.1. p-Torsion on Genus $p-5$ Hyperelliptic Curves

The construction in the preceding section can be used to construct series of hyperelliptic curves over $\mathbb{Q}$ of growing genus with a $\mathbb{Q}$-rational p-torsion point on the jacobian for a given prime p. For the construction we use the observation that the genus of the resulting curve only depends on the degrees of the polynomials a, b and u. Since the degree of a is bounded by the degree of b, we get that the genus of the resulting curve depends only on p if p is large compared to $\deg(b)$. Constructions of such series were not known until now. They allow us to explicitly write down an equation for a hyperelliptic curve with a rational point of order p on the jacobian for a given prime p.

Theorem 3.10. *Let $p > 5$ be a prime and set $b := X^4 + 2X^3 + 2 \in \mathbb{Q}[X]$ and $a_p := (X^2 + X + \lambda_2 b)^p \mod b^2$, where*

$$\lambda_2 = \frac{1}{4}X^3 - \frac{1}{2}X + \frac{1}{2}.$$

Assume that

$$F(X) := \frac{a_p^2 - (X^2-2)^p}{(X^4+2X^3+2)^2},$$

has no multiple roots in an algebraic closure of $\mathbb{Q}$. Then the curve

$$C : Y^2 = F(X)$$

is hyperelliptic of genus $g(C) = p-5$ defined over $\mathbb{Q}$ and has a $\mathbb{Q}$-rational p-torsion divisor whose first coordinate is in Mumford *representation given by $x^2 - 2$.*

Proof : Let us first observe that

$$\frac{a_p^2 - (X^2-2)^p}{(X^4+2X^3+2)^2}$$

is actually a polynomial. Since

$$(X^2+X)^2 \equiv X^2 - 2 \pmod{b},$$

we have

$$a_p^2 \equiv (X^2-2)^p \pmod{X^4+2X^3+2}.$$

Since λ_2 is constructed in such a way that this congruence holds modulo b^2, we get a polynomial in X by dividing out $(X^4+2X^3+2)^2$.

Let us now check the degree of the polynomial F. First we see that

$$\deg a_p \leq 7 = 2\deg(b) - 1.$$

So the degree of the numerator is $2p$. Therefore, the degree of F is given by $\deg(F) = 2p-8$. Since F is assumed to be a separable polynomial, we get that C is a hyperelliptic curve of genus

$$g = \frac{\deg(F)-2}{2} = \frac{2p-10}{2} = p-5.$$

For the last assertion we give a function $f \in \mathbb{Q}(C)$ with the correct principal divisor. Set $f := a_p(x) + b(x)y$ and then it is easy to verify that the norm of this function is just

$$\mathrm{N}_{\overline{\mathbb{Q}}(C)/\overline{\mathbb{Q}}(x)}(f) = (x^2-2)^p.$$

So f has a p-fold zero at exactly two points P, Q of the curve and $2p$ poles at infinity equally distributed on both branches. So the divisor $D := P + Q - D_\infty$ is non-trivial such that $pD = 0$ in the jacobian. □

For all primes up to 7919, which is the 1000-th prime, the polynomial F is irreducible over $\mathbb{Q}$ and hence it is separable. This was computed by using Magma. Supported by this numerical data, we conjecture that for all primes p the polynomial

$$F(X) := \frac{a_p^2 - (X^2-2)^p}{(X^4+2X^3+2)^2}$$

is separable. If this is indeed the case, then for every prime $p > 5$ there exist a hyperelliptic curve of genus $p-5$ with a $\mathbb{Q}$-rational divisor of order p. We now state one of these examples.

Example 3.4. *The genus eight hyperelliptic curve given by*

$$\begin{aligned} Y^2 = &- X^{18} + 4X^{17} + 14X^{16} - 72X^{15} - 76X^{14} + 584X^{13} + 168X^{12} \\ &- 2832X^{11} + 100X^{10} + 9184X^9 - 1352X^8 - 21056X^7 + 2692X^6 + 37760X^5 \\ &+ 12352X^4 - 22480X^3 - 3664X^2 + 18144X + 9104 \end{aligned}$$

has a 13-torsion point on its jacobian. The point $D := (x^2 - 2, 120x + 172)$ *has order* 13.

We now want to adapt the construction from Theorem 3.10 to obtain a family of genus $p-5$ hyperelliptic curves with a p-torsion point on their jacobians. For sake of simplicity, we fix the number field

$$K := \mathbb{Q}[X]/(X^4+2X^3+2)$$

in Theorem 3.10. With this number field we fix the u-coordinate of the p-torsion divisor by x^2-2 since for the image of this coordinate in the number field K we have a special quadratic relation. We use this to construct a function in $\mathbb{Q}(C)$ with the right poles

and zeros. In the following we construct a series of hyperelliptic curves which is for every occurring genus a family itself. For this, we take a parametrized u-coordinate of the potential p-torsion divisor $u(x) := x^2 + \lambda x + \mu$ and impose a quadratic relation on it. This relation gives us a quartic polynomial b. By Lemma 3.7 we can do the same construction in a parametrized family of $\mathbb{Q}$-algebras whenever $\gcd(b, u) = 1$.

Lemma 3.11. *Let $\lambda, \mu, \eta, \xi \in \mathbb{Q}$ be rational numbers and set*

$$b := X^4 + 2\eta X^3 + (2\xi + \eta^2 - 1)X^2 + (2\eta\,\xi - \lambda)X + \xi^2 - \mu.$$

Then we have

$$X^2 + \lambda X + \mu \equiv (X^2 + \eta X + \xi)^2 \pmod{b}.$$

Proof :

$$\begin{aligned}(X^2 + \eta X + \xi)^2 - (X^2 + \lambda X + \mu) =& X^4 + 2\eta X^3 + (2\xi + \eta^2 - 1)X^2 \\ &+ (2\eta\,\xi - \lambda)X + \xi^2 - \mu \\ \equiv& 0 \pmod{b}\end{aligned}$$

□

So in the case where the greatest common divisor of b and $X^2 + \eta X + \xi$ is one, we can use Hensel's Lemma to lift the congruence to a congruence modulo b^2 and construct a polynomial F as in the cases before. If the polynomial F is separable, we get the same result as in the Theorem 3.10. This gives us a family of hyperelliptic curves over $\mathbb{Q}$ of genus $p - 5$ with a p-torsion point on their jacobians with the constraints that

$$\gcd(b, X^2 + \eta X + \xi) = 1$$

and the computed polynomial F has a non-zero discriminant.

If $\lambda = \eta$ and $\mu = \xi$, then the condition on the greatest common divisor is violated. Since in this case,

$$b = (X^2 + \lambda X + \mu)(X^2 + \lambda X + (\mu - 1)) = u(u - 1).$$

We compute the family for $p = 7$. In this case the constructed curves are of genus two. Furthermore, we restrict ourselves to the case where $\lambda = 1$ and $\mu = 0$ to simplify the equations. We set

$$f_6(\eta, \xi) = \left(\eta\,\xi - \eta - \frac{1}{2}\xi^3 + \xi^2 + \xi - \frac{5}{2}\right)\left(\eta\,\xi - \eta - \frac{1}{2}\xi^3 + \xi^2 + \xi - \frac{1}{2}\right),$$

$$f_5(\eta, \xi) = \Bigg(\eta^3\xi - \eta^3 + \frac{1}{2}\eta^2\xi^3 + 3\eta^2\xi - \frac{7}{2}\eta^2 - \frac{3}{2}\eta\,\xi^5 + 4\eta\,\xi^4 - 3\eta\,\xi^3 + \frac{9}{2}\eta\,\xi^2 - 7\eta\,\xi + 3\eta$$

$$
\begin{aligned}
&+\frac{1}{2}\xi^7 - 2\xi^6 + \frac{3}{2}\xi^5 + \xi^4 + 2\xi^3 - \frac{3}{2}\xi^2 - \frac{13}{2}\xi + 2\Big),\\
f_4(\eta,\xi) = &\Big(\frac{1}{4}\eta^4 + \frac{7}{2}\eta^3\xi^2 - 5\eta^3\xi + 3\eta^3 - \frac{15}{4}\eta^2\xi^4 + 11\eta^2\xi^3 - \frac{13}{2}\eta^2\xi^2 + 4\eta^2\xi - 4\eta^2\\
&+\frac{1}{2}\eta\,\xi^6 - 3\eta\,\xi^5 + \frac{9}{2}\eta\,\xi^4 - 3\eta\,\xi^3 + 6\eta\,\xi^2 - 6\eta\,\xi + \frac{1}{2}\eta + \frac{1}{4}\xi^8 - \xi^7 + \frac{1}{2}\xi^6 + 2\xi^5\\
&-\frac{7}{4}\xi^4 - \frac{1}{2}\xi^3 + 1\frac{1}{4}\xi^2 - 6\xi + 1\Big),\\
f_3(\eta,\xi) = &\Big(\frac{5}{2}\eta^4\xi - 2\eta^4 - \eta^3\xi^3 + 5\eta^3\xi^2 - 2\eta^3\xi + \eta^3 - 2\eta^2\xi^5 + 4\eta^2\xi^4\\
&+\frac{3}{2}\eta^2\xi^3 - 7\eta^2\xi^2 + 8\eta^2\xi - 3\eta^2 + \eta\,\xi^7 - 4\eta\,\xi^6 + 3\eta\,\xi^5 + 6\eta\,\xi^4\\
&-10\eta\,\xi^3 + \frac{9}{2}\eta\,\xi^2 - \frac{1}{2}\eta\,\xi - \eta - \frac{1}{2}\xi^6 + 2\xi^5 - \frac{3}{2}\xi^4 - \frac{5}{2}\xi^3 + 4\xi^2 - 2\xi\Big),\\
f_2(\eta,\xi) = &\Big(\frac{1}{2}\eta^5 + \frac{9}{4}\eta^4\xi^2 - 2\eta^4\xi + \eta^4 - 4\eta^3\xi^4 + 10\eta^3\xi^3 - \frac{7}{2}\eta^3\xi^2 - 3\eta^3\xi + 2\eta^3\\
&+\frac{3}{2}\eta^2\xi^6 - 6\eta^2\xi^5 + 1\frac{1}{2}\eta^2\xi^4 + 5\eta^2\xi^3 - 10\eta^2\xi^2 + 4\eta^2\xi + \frac{1}{4}\eta^2\\
&-\eta\,\xi^5 + 4\eta\,\xi^4 - 4\eta\,\xi^3 - \frac{1}{2}\eta\,\xi^2 + \eta\,\xi + \frac{1}{4}\xi^4 - \xi^3 + \xi^2\Big),\\
f_1(\eta,\xi) = &\frac{3}{2}\eta^2\left(\eta - \xi^2 + 2\xi\right)\left(\eta^2\xi - \frac{2}{3}\eta^2 - \frac{2}{3}\eta\,\xi^3 + \frac{4}{3}\eta\,\xi^2 - \frac{1}{3}\eta + \frac{1}{3}\xi^2 - \frac{2}{3}\xi\right),\\
f_0(\eta,\xi) = &\frac{1}{4}\eta^4(\eta - \xi^2 + 2\xi)^2.
\end{aligned}
$$

Theorem 3.12. *Let $\eta, \xi \in \mathbb{Q}$ and let the $f_i(\eta,\xi)$ be as above. Assume*

$$C_{\eta,\xi} : Y^2 = \sum_{i=0}^{6} f_i(\eta,\xi)X^i$$

defines a hyperelliptic curve. Then $\mathrm{Jac}(C_{\eta,\xi})[7](\mathbb{Q})$ *is non-trivial.*

To decide when $C_{\eta,\xi}$ defines a hyperelliptic curve, we compute the discriminant of this family of curves. It is given by

$$\Delta(C_{\eta,\xi}) = c\eta^7(\eta - \xi + 1)^7(\eta - \xi^2 + \xi + 1)^7(\eta - \xi^2 + 2\xi)^7 r,$$

for some constant $c \in \mathbb{Q}^*$ and $r \in \mathbb{Q}(\eta,\xi)$. The polynomial r defines an affine irreducible singular genus ten curve. For any choices of η and ξ such that the discriminant does not vanish, $C_{\eta,\xi}$ is a hyperelliptic curve.

So far, we have only considered torsion divisors that do not lie on the image of the curve under Φ_{P_∞} in the jacobian since we assumed the u-coordinate of the torsion divisor to have degree equal to two. In the following we consider divisors with degree of the

u-coordinate equal to one. These divisors are exactly those which lie on the image of the curve under Φ_{P_∞}. As we have seen, the degree of the u-coordinate of the torsion divisor has an influence on the degree of the resulting polynomial F, hence, on the genus of the constructed curve. Since the goal is to construct large torsion in relation to the genus of the curve, we need solutions to the norm equation with a polynomial F of relatively small degree. In the next section we give an approach to reduce the genus of the resulting curve while the order of the torsion remains the same.

3.3.2. p-Torsion on the Image of Genus $\frac{p-7}{2}$ Curves

In this section we give a construction to explicitly generate hyperelliptic curves C of genus $g = \frac{p-7}{2}$ with a p-torsion point on the image of C in $\mathrm{Jac}(C)$. For this we construct a polynomial $b \in \mathbb{Q}[X]$ such that X is a square in $\mathbb{Q}[X]/(b)$ of a quadratic polynomial. For this, we consider the relation

$$X \equiv (X^2 + \mu X + \eta)^2 \pmod{b}.$$

This congruence holds for some polynomial b of degree $\deg(b) = 3$ if and only if the polynomial

$$h := X^4 + 2\mu X^3 + (2\eta + \mu^2)X^2 + (2\mu\eta - 1)X + \eta^2$$

has a rational root. We now give a condition when the polynomial h has a rational root. The polynomial h has a root at $\lambda \in \mathbb{Q}$ if and only if

$$0 = \eta^2 + 2\lambda\mu\eta - \lambda + 2\lambda^2\eta + \lambda^2\mu^2 + 2\lambda^3\mu + \lambda^4.$$

In this case we have

$$b = X^3 + (2\mu + \lambda)X^2 + (2\eta + \mu^2 + 2\lambda\mu + \lambda^2)X + (2\mu\eta - 1 + 2\lambda\eta + 2\lambda^2\mu + \lambda^3 + \lambda\mu^2).$$

Lemma 3.13. *There are only finitely many $\lambda, \mu, \eta \in \mathbb{Q}$ such that the polynomials b and X have a non-trivial common factor.*

Proof : Assume $\lambda, \mu, \eta \in \mathbb{Q}$ are given such that $X|b$. This is true if and only if the constant term in b is equal to zero. By the discussion above we get

$$\begin{aligned} 0 &= \eta^2 + 2\lambda\mu\eta - \lambda + 2\lambda^2\eta + \lambda^2\mu^2 + 2\lambda^3\mu + \lambda^4 \\ 0 &= 2\mu\eta - 1 + 2\lambda\eta + 2\lambda^2\mu + \lambda^3 + \lambda\mu^2. \end{aligned}$$

Combining these two conditions gives us a smooth genus seven curve. Therefore, by a theorem of FALTINGS [Fal83] there are only finitely many possibilities for $\lambda, \mu, \eta \in \mathbb{Q}$ to fulfill both conditions. □

If $\gcd(b, X) = 1$, i.e. $\lambda, \mu, \eta \in \mathbb{Q}$ do not correspond to a rational point on the curve in the lemma above, then we can use HENSEL's Lemma 3.6 to lift the congruence

$$X \equiv (X^2 + \mu X + \eta)^2 \pmod{b}$$

to a congruence modulo b^2. We get $X \equiv \widetilde{R}^2 \pmod{b^2}$ for

$$\begin{aligned}\widetilde{R} = &-\frac{1}{2\eta}\lambda X^6 + \left(-\frac{1}{2\eta}\lambda^2 - 2\frac{\mu}{\eta}\lambda - \frac{1}{2}\right)X^5 + \left(-\frac{1}{2\eta}\lambda^3 - 2\frac{\mu}{\eta}\lambda^2 + \frac{-3\mu^2 - 2\eta}{\eta}\lambda\right.\\
&\left.-3\frac{\mu}{2}\right)X^4 + \left(-\frac{\mu}{\eta}\lambda^3 + \frac{-5\mu^2 - 2\eta}{2\eta}\lambda^2 + \frac{-4\mu^3 - 10\mu\eta + 1}{2\eta}\lambda + \frac{-3\mu^2 - 2\eta}{2}\right)X^3\\
&+\left(\frac{-\mu^2 - 2\eta}{2\eta}\lambda^3 + \frac{-2\mu^3 - 6\mu\eta + 1}{2\eta}\lambda^2 + \frac{-\mu^4 - 8\mu^2\eta - 5\eta^2 + 2\mu}{2\eta}\lambda\right.\\
&\left.+\frac{-\mu^3 - 4\mu\eta + 3}{2}\right)X^2 + \left(\frac{-2\mu\eta + 1}{2\eta}\lambda^3 + \right.\\
&\left.\frac{-4\mu^2\eta - \eta^2 + 2\mu}{2\eta}\lambda^2 + \frac{-2\mu^3\eta - 6\mu\eta^2 + \mu^2 + 2\eta}{2\eta}\lambda + \frac{-2\mu^2\eta - \eta^2 + 3\mu}{2}\right)X\\
&-\frac{\eta}{2}\lambda^3 - \mu\eta\lambda^2 + \frac{-\mu^2\eta - 2\eta^2}{2}\lambda + \frac{-\mu\eta^2 + 2\eta}{2}.\end{aligned}$$

Then with Lemma 3.7 we can find a polynomial F which is the defining polynomial of a series of hyperelliptic curves admitting a p-torsion point on the jacobian. The genus of these curves is given by $\frac{p-7}{2}$ if $p > 10$, since we have $\deg(b) = 3$, hence $\deg(a) \leq 5$. For the prime $p = 11$ we have computed the family of genus two curves admitting a p-torsion divisor and get the following example. To state the example we set

$$\begin{aligned}a_0 = &\frac{1}{4}(2\lambda^3\mu^9\eta - \lambda^3\mu^8 - 16\lambda^3\mu^7\eta^2 + 18\lambda^3\mu^6\eta + 42\lambda^3\mu^5\eta^3 - 6\lambda^3\mu^5 - 63\lambda^3\mu^4\eta^2\\
&- 40\lambda^3\mu^3\eta^4 + 36\lambda^3\mu^3\eta + 54\lambda^3\mu^2\eta^3 - 9\lambda^3\mu^2 + 10\lambda^3\mu\eta^5 - 18\lambda^3\mu\eta^2 - 5\lambda^3\eta^4\\
&+ 4\lambda^2\mu^{10}\eta - 2\lambda^2\mu^9 - 33\lambda^2\mu^8\eta^2 + 36\lambda^2\mu^7\eta + 90\lambda^2\mu^6\eta^3 - 12\lambda^2\mu^6 - 132\lambda^2\mu^5\eta^2\\
&- 90\lambda^2\mu^4\eta^4 + 72\lambda^2\mu^4\eta + 126\lambda^2\mu^3\eta^3 - 18\lambda^2\mu^3 + 24\lambda^2\mu^2\eta^5 - 45\lambda^2\mu^2\eta^2\\
&- 16\lambda^2\mu\eta^4 + 2\lambda\mu^{11}\eta - \lambda\mu^{10} - 14\lambda\mu^9\eta^2 + 16\lambda\mu^8\eta + 22\lambda\mu^7\eta^3 - 6\lambda\mu^7 - 39\lambda\mu^6\eta^2\\
&+ 26\lambda\mu^5\eta^4 + 24\lambda\mu^5\eta - 36\lambda\mu^4\eta^3 - 9\lambda\mu^4 - 70\lambda\mu^3\eta^5 + 36\lambda\mu^3\eta^2 + 95\lambda\mu^2\eta^4\\
&- 18\lambda\mu^2\eta + 26\lambda\mu\eta^6 - 36\lambda\mu\eta^3 - 14\lambda\eta^5 + 3\mu^{10}\eta^2 - 4\mu^9\eta - 28\mu^8\eta^3 + \mu^8\\
&+ 46\mu^7\eta^2 + 91\mu^6\eta^4 - 30\mu^6\eta - 162\mu^5\eta^3 + 6\mu^5 - 120\mu^4\eta^5 + 126\mu^4\eta^2 + 192\mu^3\eta^4\\
&- 54\mu^3\eta + 55\mu^2\eta^6 - 108\mu^2\eta^3 + 9\mu^2 - 54\mu\eta^5 + 18\mu\eta^2 - 4\eta^7 + 9\eta^4)\end{aligned}$$

$$
\begin{aligned}
a_1 =& \frac{1}{2}(\lambda^3\mu^{10} - 6\lambda^3\mu^8\eta + 7\lambda^3\mu^7 + 7\lambda^3\mu^6\eta^2 - 19\lambda^3\mu^5\eta + 10\lambda^3\mu^4\eta^3 + 13\lambda^3\mu^4 \\
& - 9\lambda^3\mu^3\eta^2 - 15\lambda^3\mu^2\eta^4 + 3\lambda^3\mu^2\eta + 16\lambda^3\mu\eta^3 + 3\lambda^3\mu + 2\lambda^3\eta^5 - \lambda^3\eta^2 + 2\lambda^2\mu^{11} \\
& - 12\lambda^2\mu^9\eta + 14\lambda^2\mu^8 + 11\lambda^2\mu^7\eta^2 - 38\lambda^2\mu^6\eta + 37\lambda^2\mu^5\eta^3 + 26\lambda^2\mu^5 - 31\lambda^2\mu^4\eta^2 \\
& - 56\lambda^2\mu^3\eta^4 + 6\lambda^2\mu^3\eta + 61\lambda^2\mu^2\eta^3 + 6\lambda^2\mu^2 + 13\lambda^2\mu\eta^5 - 11\lambda^2\mu\eta^2 - 4\lambda^2\eta^4 \\
& + \lambda\mu^{12} - 4\lambda\mu^{10}\eta + 7\lambda\mu^9 - 12\lambda\mu^8\eta^2 - 5\lambda\mu^7\eta + 68\lambda\mu^6\eta^3 + 13\lambda\mu^6 - 81\lambda\mu^5\eta^2 \\
& - 75\lambda\mu^4\eta^4 + 29\lambda\mu^4\eta + 90\lambda\mu^3\eta^3 + 3\lambda\mu^3 + 12\lambda\mu^2\eta^5 - 26\lambda\mu^2\eta^2 + 2\lambda\mu\eta^4 \\
& + 6\lambda\mu\eta + 2\lambda\eta^6 + 2\lambda\eta^3 + 2\mu^{11}\eta - \mu^{10} - 17\mu^9\eta^2 + 20\mu^8\eta + 47\mu^7\eta^3 - 7\mu^7 \\
& - 75\mu^6\eta^2 - 43\mu^5\eta^4 + 45\mu^5\eta + 63\mu^4\eta^3 - 13\mu^4 - 26\mu^3\eta^2 + 14\mu^2\eta^4 + 3\mu^2\eta \\
& + 7\mu\eta^6 - 6\mu\eta^3 - 3\mu - 5\eta^5 - 3\eta^2) \\
a_2 =& \frac{1}{4}(6\lambda^3\mu^9 - 42\lambda^3\mu^7\eta + 39\lambda^3\mu^6 + 90\lambda^3\mu^5\eta^2 - 132\lambda^3\mu^4\eta - 60\lambda^3\mu^3\eta^3 + 60\lambda^3\mu^3 \\
& + 72\lambda^3\mu^2\eta^2 + 6\lambda^3\mu\eta^4 - 18\lambda^3\mu\eta + 3\lambda^3 + 13\lambda^2\mu^{10} - 96\lambda^2\mu^8\eta + 88\lambda^2\mu^7 \\
& + 220\lambda^2\mu^6\eta^2 - 326\lambda^2\mu^5\eta - 156\lambda^2\mu^4\eta^3 + 146\lambda^2\mu^4 + 216\lambda^2\mu^3\eta^2 + 6\lambda^2\mu^2\eta^4 \\
& - 80\lambda^2\mu^2\eta + 8\lambda^2\mu\eta^3 + 18\lambda^2\mu + 4\lambda^2\eta^5 + 8\lambda\mu^{11} - 56\lambda\mu^9\eta + 60\lambda\mu^8 + 102\lambda\mu^7\eta^2 \\
& - 204\lambda\mu^6\eta + 18\lambda\mu^5\eta^3 + 120\lambda\mu^5 + 27\lambda\mu^4\eta^2 - 132\lambda\mu^3\eta^4 - 46\lambda\mu^3\eta + 150\lambda\mu^2\eta^3 \\
& + 40\lambda\mu^2 + 42\lambda\mu\eta^5 - 24\lambda\mu\eta^2 - 15\lambda\eta^4 + 2\lambda\eta + \mu^{12} - 2\mu^{10}\eta + 6\mu^9 - 33\mu^8\eta^2 \\
& + 22\mu^7\eta + 146\mu^6\eta^3 + 4\mu^6 - 210\mu^5\eta^2 - 195\mu^4\eta^4 + 108\mu^4\eta + 274\mu^3\eta^3 - 16\mu^3 \\
& + 78\mu^2\eta^5 - 104\mu^2\eta^2 - 58\mu\eta^4 + 10\mu\eta - 4\eta^6 + 8\eta^3 + 1) \\
a_3 =& \frac{1}{2}(3\lambda^3\mu^8 - 20\lambda^3\mu^6\eta + 18\lambda^3\mu^5 + 40\lambda^3\mu^4\eta^2 - 54\lambda^3\mu^3\eta - 24\lambda^3\mu^2\eta^3 + 23\lambda^3\mu^2 \\
& + 22\lambda^3\mu\eta^2 + 2\lambda^3\eta^4 - 2\lambda^3\eta + 7\lambda^2\mu^9 - 51\lambda^2\mu^7\eta + 45\lambda^2\mu^6 + 117\lambda^2\mu^5\eta^2 \\
& - 155\lambda^2\mu^4\eta - 90\lambda^2\mu^3\eta^3 + 64\lambda^2\mu^3 + 93\lambda^2\mu^2\eta^2 + 15\lambda^2\mu\eta^4 - 21\lambda^2\mu\eta - 2\lambda^2\eta^3 \\
& + 2\lambda^2 + 5\lambda\mu^{10} - 38\lambda\mu^8\eta + 37\lambda\mu^7 + 91\lambda\mu^6\eta^2 - 135\lambda\mu^5\eta - 70\lambda\mu^4\eta^3 + 66\lambda\mu^4 \\
& + 77\lambda\mu^3\eta^2 + 5\lambda\mu^2\eta^4 - 27\lambda\mu^2\eta + 16\lambda\mu\eta^3 + 11\lambda\mu + 2\lambda\eta^5 - \lambda\eta^2 + \mu^{11} - 7\mu^9\eta \\
& + 8\mu^8 + 12\mu^7\eta^2 - 23\mu^6\eta + 7\mu^5\eta^3 + 15\mu^5 - 21\mu^4\eta^2 - 25\mu^3\eta^4 + 18\mu^3\eta + 51\mu^2\eta^3 \\
& - 2\mu^2 + 9\mu\eta^5 - 18\mu\eta^2 - 6\eta^4 - \eta) \\
a_4 =& \frac{1}{4}(2\lambda^3\mu^7 - 12\lambda^3\mu^5\eta + 12\lambda^3\mu^4 + 20\lambda^3\mu^3\eta^2 - 28\lambda^3\mu^2\eta - 8\lambda^3\mu\eta^3 + 10\lambda^3\mu \\
& + 4\lambda^3\eta^2 + 5\lambda^2\mu^8 - 34\lambda^2\mu^6\eta + 36\lambda^2\mu^5 + 70\lambda^2\mu^4\eta^2 - 110\lambda^2\mu^3\eta - 44\lambda^2\mu^2\eta^3 \\
& + 47\lambda^2\mu^2 + 50\lambda^2\mu\eta^2 + 4\lambda^2\eta^4 - 8\lambda^2\eta + 4\lambda\mu^9 - 30\lambda\mu^7\eta + 37\lambda\mu^6 + 72\lambda\mu^5\eta^2 \\
& - 140\lambda\mu^4\eta - 60\lambda\mu^3\eta^3 + 74\lambda\mu^3 + 108\lambda\mu^2\eta^2 + 12\lambda\mu\eta^4 - 42\lambda\mu\eta - 12\lambda\eta^3 + 9\lambda \\
& + \mu^{10} - 8\mu^8\eta + 12\mu^7 + 21\mu^6\eta^2 - 54\mu^5\eta - 20\mu^4\eta^3 + 36\mu^4 + 58\mu^3\eta^2 + 5\mu^2\eta^4 \\
& - 36\mu^2\eta - 14\mu\eta^3 + 16\mu + 8\eta^2).
\end{aligned}
$$

Example 3.5. *Let* $F_{\lambda,\mu,\eta} = -X^5 + \sum_{i=0}^{4} a_i X^i$, *with* $a_i \in \mathbb{Q}(\lambda,\mu,\eta)$ *as above and* $\eta^2 + 2\lambda\mu\eta - \lambda + 2\lambda^2\eta + \lambda^2\mu^2 + 2\lambda^3\mu + \lambda^4 = 0$, *have no multiple roots. Then the hyperelliptic curve* $C_{\lambda,\mu,\eta} : Y^2 = F_{\lambda,\mu,\eta}(X)$ *of genus two has a* $\mathbb{Q}$*-rational* 11*-torsion point on its jacobian.*

Remark. *In Example 3.5 we make the restriction*

$$\xi := \eta^2 + 2\lambda\mu\eta - \lambda + 2\lambda^2\eta + \lambda^2\mu^2 + 2\lambda^3\mu + \lambda^4 = 0$$

to simplify the defining equation slightly. This does not restrict the family in any sense. The family is constructed in such a way that the u*-coordinate of a point* $P \in C(\mathbb{Q})$ *is given by* $x - \xi$ *and* $D := P - P_\infty$ *is the* 11*-torsion divisor in the jacobian. The* Magma *code of the construction can be found in Appendix A.3.*

It is possible to change the degree of the polynomial b to four. This would give a family of curves with a point of order p of genus $\frac{p-9}{2}$. This would increase the degree of the resulting polynomial F by one. The leading coefficient of the polynomial is given by a rational function in the parameters. If it is possible to choose the parameters in such a way that the leading coefficient vanishes, we get the desired degree of the polynomial F. For $p = 13$ and genus two curves this was done by Leprévost.

We now reproduce the family constructed in [Lep91a] in a slightly more general way. Leprévost started with a degree four polynomial given by two independent parameters and obtained a one-parameter-family of hyperelliptic curves of genus two admitting a 13-torsion point. We start with a polynomial given by three parameters and end up with a two-parameter-family of hyperelliptic curves.

For this task we set

$$b := X^4 - (\lambda^2 - 2\mu)X^3 + (\mu^2 + 2\eta)X^2 + 2\mu\eta X + \eta^2 \in \mathbb{Q}(\lambda,\mu,\eta)[X]$$

and

$$R := X^3 - (\lambda^2 - 2\mu)x^2 + (\mu^2 + \eta)X + \mu\eta \in \mathbb{Q}(\lambda,\mu,\eta)[X].$$

Then by computing the remainder of R^2 modulo b one gets

$$\lambda^2\eta^2 X \equiv R^2 \pmod{b}.$$

The next step is to lift this relation to a congruence modulo b^2 by Hensel's Lemma. By setting

$$r_0 := \frac{\frac{3}{2}\lambda^2\mu\eta + \frac{1}{2}\mu^4 - \frac{3}{2}\mu^2\eta + \frac{1}{2}\eta^2}{\lambda^3\eta}$$

$$
\begin{aligned}
r_1 &:= \frac{3\lambda^2\mu^2\eta + \frac{3}{2}\lambda^2\eta^2 + \frac{3}{2}\mu^5 - 4\mu^3\eta + \frac{1}{2}\mu\eta^2}{\lambda^3\eta^2}\\
r_2 &:= \frac{-\frac{3}{2}\lambda^4\eta^2 + 2\lambda^2\mu^3\eta + 6\lambda^2\mu\eta^2 + \frac{3}{2}\mu^6 - \frac{3}{2}\mu^4\eta - 6\mu^2\eta^2 + \frac{3}{2}\eta^3}{\lambda^3\eta^3}\\
r_3 &:= \frac{-\frac{3}{2}\lambda^4\mu\eta^2 - \frac{1}{2}\lambda^2\mu^4\eta + 9\lambda^2\mu^2\eta^2 + 2\lambda^2\eta^3 + \frac{1}{2}\mu^7 + 3\mu^5\eta - 10\mu^3\eta^2}{\lambda^3\eta^4}\\
r_4 &:= \frac{-\frac{3}{2}\lambda^4\mu^2\eta - \frac{3}{2}\lambda^4\eta^2 - \lambda^2\mu^5 + 4\lambda^2\mu^3\eta + 7\lambda^2\mu\eta^2 + 2\mu^6 - \mu^4\eta - 9\mu^2\eta^2 + \frac{3}{2}\eta^3}{\lambda^3\eta^4}\\
r_5 &:= \frac{\frac{1}{2}\lambda^6\eta + \frac{1}{2}\lambda^4\mu^3 - 3\lambda^4\mu\eta - 2\lambda^2\mu^4 + 8\lambda^2\mu^2\eta + \lambda^2\eta^2 + 3\mu^5 - 6\mu^3\eta - \frac{3}{2}\mu\eta^2}{\lambda^3\eta^4}\\
r_6 &:= \frac{-\lambda^4\eta - \lambda^2\mu^3 + 4\lambda^2\mu\eta + 2\mu^4 - \frac{9}{2}\mu^2\eta + \frac{1}{2}\eta^2}{\lambda^3\eta^4}\\
r_7 &:= \frac{\frac{1}{2}\lambda^2\eta + \frac{1}{2}\mu^3 - \mu\eta}{\lambda^3\eta^4}.
\end{aligned}
$$

and $\widetilde{R} = \sum_{i=0}^{7} r_i x^i$, we obtain the congruence

$$x \equiv \widetilde{R}^2 \pmod{b^2}.$$

Using this congruence and setting $a := \mu\widetilde{R}^{13} \pmod{b^2}$, we directly get that b^2 divides $a^2 - \mu^2 X^{13}$ for all $\mu \in \mathbb{Q}^*$. We set

$$\mu := 2\lambda^3, \qquad\qquad F := \frac{a^2 - 4\lambda^6 X^{13}}{b^2}$$

and obtain

$$
\begin{aligned}
F =& (\lambda^4 + 2\lambda^2\mu + \mu^2)X^6 + (-2\lambda^2\mu^2 + 2\lambda^2\eta + 2\mu^3 + 2\mu\eta)X^5\\
&+ (-4\lambda^2\mu\eta + \mu^4 + 6\mu^2\eta + \eta^2)X^4 + (-2\lambda^2\eta^2 + 4\mu^3\eta + 6\mu\eta^2)X^3\\
&+ (6\mu^2\eta^2 + 2\eta^3)X^2 + 4\mu\eta^3 X + \eta^4.
\end{aligned}
$$

The leading coefficient of F vanishes if and only if $\mu = -\lambda^2$. So by setting $\mu := -\lambda^2$, we get

$$
\begin{aligned}
F =& -4\lambda^6 X^5 + (\lambda^8 + 10\lambda^4\eta + \eta^2)X^4\\
&+ (-4\lambda^6\eta - 8\eta^2\lambda^2)X^3 + (6\lambda^4\eta^2 + 2\eta^3)X^2 - 4\eta^3\lambda^2 X + \eta^4.
\end{aligned}
$$

For this polynomial F we can compute the discriminant by

$$\Delta(F) = 2^8\eta^{19}\lambda^4(-2^4\lambda^8 + 349\lambda^4\eta + 2^4\eta^2).$$

These considerations we combine to the following proposition.

Proposition 3.14 ([Lep91a]). *Let $\lambda, \eta \in \mathbb{Q}$ with $2^8\eta^{19}\lambda^4(-2^4\lambda^4 + 349\lambda^4\eta + 2^4\eta^2) \neq 0$. Then*

$$\begin{aligned} Y^2 = &-4\lambda^6X^5 + (\lambda^8 + 10\lambda^4\eta + \eta^2)X^4 + (-4\lambda^6\eta - 8\eta^2\lambda^2)X^3 \\ &+ (6\lambda^4\eta^2 + 2\eta^3)X^2 - 4\eta^3\lambda^2X + \eta^4 \end{aligned}$$

defines a hyperelliptic curve $C_{\lambda,\eta}$ of genus two with a point of order 13 in its jacobian.

Proof : By the discussion above, the condition on λ and η in the theorem just says that the discriminant of the polynomial is not zero. So F has no multiple roots and is of degree five, therefore, $Y^2 = F(X)$ defines a hyperelliptic curve of genus two. Furthermore, by the discussion above, we have the function $f := a(x) + b(x)y$ on $C_{\lambda,\eta}$ with norm $\mathrm{N}_{\overline{\mathbb{Q}}(C)/\overline{\mathbb{Q}}(x)}(f) = \varepsilon x^{13}$ for some $\varepsilon \in \mathbb{Q}^*$.

Therefore, the divisor

$$D := \left(0, \eta^2\right) - P_\infty$$

is a divisor of order 13 since $13D = \mathrm{div}(f)$ and D is non-trivial. □

We now want to compute which curves in this family are isomorphic to the family of hyperelliptic curves with a rational torsion point of order 13 given by Leprévost in [Lep91a]. First we observe that by specializing $C_{\lambda,\eta}$ with $\lambda = 1$, we obtain the family from Leprévost. We now compute the Igusa invariants of $C_{\lambda,\eta}$, which are given by

$$\begin{aligned} J_2(C_{\lambda,\eta}) =& 32\eta^3(\lambda^8 - \lambda^4\eta - \eta^2) \\ J_4(C_{\lambda,\eta}) =& 64\eta^6(\lambda^{16} - 23\lambda^{12}\eta + 50\lambda^8\eta^2 + 23\lambda^4\eta^3 + \eta^4) \\ J_6(C_{\lambda,\eta}) =& 64\eta^9(8\lambda^{24} - 173\lambda^{20}\eta + 300\lambda^{16}\eta^2 - 1118\lambda^{12}\eta^3 - 300\lambda^8\eta^4 - 173\lambda^4\eta^5 - 8\eta^6) \\ J_{10}(C_{\lambda,\eta}) =& 4096\eta^{19}(-16\lambda^{24} + 349\lambda^{20}\eta + 16\lambda^{16}\eta^2). \end{aligned}$$

Therefore, the absolute Igusa invariants of $C_{\lambda,\eta}$ are

$$\begin{aligned} \alpha(C_{\lambda,\eta}) &= \frac{\lambda^{16} - 23\lambda^{12}\eta + 50\lambda^8\eta^2 + 23\lambda^4\eta^3 + \eta^4}{16(\lambda^8 - \lambda^4\eta - \eta^2)^2} \\ \beta(C_{\lambda,\eta}) &= \frac{8\lambda^{24} - 173\lambda^{20}\eta + 300\lambda^{16}\eta^2 - 1118\lambda^{12}\eta^3 - 300\lambda^8\eta^4 - 173\lambda^4\eta^5 - 8\eta^6}{512(\lambda^8 - \lambda^4\eta - \eta^2)^3} \\ \gamma(C_{\lambda,\eta}) &= \frac{\eta^4(-16\lambda^{24} + 349\lambda^{20}\eta + 16\lambda^{16}\eta^2)}{131072(\lambda^8 - \lambda^4\eta - \eta^2)^5}. \end{aligned}$$

Using these invariants, we can show that every curve in the family $C_{\lambda,\eta}$ is isomorphic over $\mathbb{Q}$ to a curve in the family of Leprévost.

Proposition 3.15. *For all $\lambda, \eta \in \mathbb{Q}$ the hyperelliptic curve $C_{\lambda,\eta}$ is isomorphic to the hyperelliptic curve $C_{1,-\frac{\lambda^4}{\eta}}$, therefore, it is a member of the family of Leprévost.*

Proof : Since two hyperelliptic curves are isomorphic if and only if all three absolute Igusa invariants are the same, we look at the difference of the invariants of $C_{\lambda,\eta'}$ and $C_{1,\eta}$. This difference we denote by α', β' and γ'. If we can find λ, η, η' such that $\alpha' = \beta' = \gamma' = 0$, we can conclude that $C_{\lambda,\eta'}$ and $C_{1,\eta}$ are isomorphic. Since we are searching for zeros of α', β' and γ', it is enough to look at their numerators. We compute the greatest common divisor of these numerators. This computation shows that $\eta'\eta + \lambda^4$ divides all the numerators. □

Since the equations for this series of hyperelliptic curves with a 13-torsion point on the jacobian is rather complicated, we give the Magma code for the construction of this family in Appendix A.1.

In this section we constructed polynomials $b, u \in \mathbb{Q}(\mu, \lambda, \eta)[X]$ such that $\gcd(b, u) = 1$ and the polynomial u is a square modulo b. Thus we can apply Lemma 3.7 to find polynomials $F, a \in \mathbb{Q}(\mu, \lambda, \eta)[X]$ for any prime p and $\varepsilon \in \mathbb{Q}(\mu, \lambda, \eta)$ such that

$$a^2 - Fb^2 = \varepsilon u^p.$$

Whenever F is a separable, we obtain a hyperelliptic curve of genus $\frac{p-7}{2}$ with a rational p-torsion divisor on it.

The lifting method can be used to produce examples of hyperelliptic curves defined over a number field with a certain torsion point on the jacobian. The idea is analogous to the construction due to Leprévost, where the final step is to find rational solutions such that the leading coefficient vanishes. Instead of allowing only rational solutions, we now allow solutions in some number field.

3.3.3. 17-Torsion Attempt

In this section, we try to produce genus two curves with a 17-torsion point with the same approach. Unfortunately, we were not able to construct a curve defined over the rational numbers in this way. We are able to produce examples for curves defined over some number field of degree seven.

Again, the first step is to construct a polynomial b such that X has a square root modulo b. Since our goal is to construct a curve with a point of order 17 on the jacobian, this polynomial b has to be of degree six by the Riemann-Roch Theorem 1.4 and we assume b to be monic. So let

$$b := X^6 + pX^5 + qX^4 + rX^3 + sX^2 + tX + u'$$

and assume there exists a polynomial $R \in \mathbb{Q}[X]$ of degree three such that

$$R^2 \equiv \varepsilon X \pmod{b}.$$

We make the restriction on the degree of R to make the computation feasible. The congruence we have assumed gives us, that u' has to be the square of the constant term of R. Therefore, we can set

$$b := X^6 + pX^5 + qX^4 + rX^3 + sX^2 + tX + u^2,$$

which is our modulus, and

$$R := X^3 + r_2X^2 + r_1X + u$$

for some parameters r_2, r_1. By equating coefficients, we get for

$$r_2 := \frac{p}{2}, \qquad r_1 := \frac{q - \frac{1}{4}p^2}{2},$$
$$r := -\frac{1}{8}p^3 + \frac{1}{2}pq + 2u, \qquad s := \frac{1}{64}p^4 - \frac{1}{8}p^2q + pu + \frac{1}{4}q^2$$

that

$$R^2 \equiv \left(-\frac{1}{4}p^2u + qu - t\right) X \pmod{b}.$$

The polynomials R and b become

$$R = X^3 + \frac{1}{2}pX^2 + \left(-\frac{1}{8}p^2 + \frac{1}{2}q\right) X + u$$

and

$$\begin{aligned} b =& X^6 + pX^5 + qX^4 + \left(-\frac{1}{8}p^3 + \frac{1}{2}pq + 2u\right) X^3 \\ &+ \left(\frac{1}{64}p^4 - \frac{1}{8}p^2q + pu + \frac{1}{4}q^2\right) X^2 + tX + u^2. \end{aligned}$$

This congruence can now be lifted to a congruence modulo b^2. The Magma code to compute the polynomial $\widetilde{R}$ fulfilling this congruence can be found in Appendix A.4. Recall that we want to construct a polynomial of degree five which is the defining polynomial of our curve. But for achieving this, we need to have

$$\deg(\widetilde{R}^{17} \mod b^2) \leq 8.$$

Since $\deg(b) = 6$, we get $\deg(\widetilde{R}^{17} \mod b^2) \leq 11$. Therefore, we have to find parameters $p, q, t, u \in \mathbb{Q}$ such that the first three coefficients vanish. Since $\widetilde{R}$ and b are polynomials given in four parameters, we can hope for a one-dimensional space of parameters such that

$$\deg\left(\widetilde{R}^{17} \mod b^2\right) \leq 8.$$

We have computed $a := \widetilde{R}^{17} \mod b$. The result can be found in Appendix A.4.

Searching for parameters such that the first three coefficients of a vanish gives us the criterion that

$$t = \frac{15}{128}p^5 - \frac{7}{16}p^3q + \frac{3}{4}p^2u + \frac{3}{8}pq^2.$$

Now we are left to find rational points on the curve V given by

$$\begin{aligned} 0 &= -\frac{49}{512}p^6 + \frac{37}{128}p^4q - \frac{5}{8}p^3u - \frac{3}{32}p^2q^2 - \frac{1}{8}q^3 + u^2 \\ 0 &= -\frac{27}{512}p^7 - \frac{31}{128}p^5q - \frac{7}{32}p^4u + \frac{43}{32}p^3q^2 - 3p^2qu - \frac{9}{8}pq^3 + pu^2 + \frac{3}{2}q^2u. \end{aligned}$$

Remark. *An exhaustive search for rational points on V up to height one billion only gives one rational point $P = (0, 0, 0)$ on V. This point is the only singularity of V.*

Lemma 3.16. *View V as a zero dimension variety over the rational function field $\mathbb{Q}(p)$. Then $V/\mathbb{Q}(p)$ is the intersection of two elliptic curves.*

Proof : First observe that the two curves

$$\begin{aligned} C/\mathbb{Q}(p) &: -\frac{49}{512}p^6 + \frac{37}{128}p^4q - \frac{5}{8}p^3u - \frac{3}{32}p^2q^2 - \frac{1}{8}q^3 + u^2 \\ C'/\mathbb{Q}(p) &: -\frac{27}{512}p^7 - \frac{31}{128}p^5q - \frac{7}{32}p^4u + \frac{43}{32}p^3q^2 - 3p^2qu - \frac{9}{8}pq^3 + pu^2 + \frac{3}{2}q^2u \end{aligned}$$

are non-singular. Furthermore, they are both double covers of $\mathbb{P}^1(\mathbb{Q}(p))$ ramified at exactly four points. By the Riemann-Hurwitz Genus Formula 1.5, this gives us that C and C' are of genus one. So we are only left to construct a $\mathbb{Q}(p)$-rational point on them. For this task we set $u := ap^3$ and $q := bp^2$. Then the two equations become

$$\begin{aligned} 0 &= p^6\left(-\frac{49}{512} + \frac{37}{128}b - \frac{5}{8}a - \frac{3}{32}b^2 - \frac{1}{8}b^3 + a^2\right) \\ 0 &= p^7\left(-\frac{27}{512} - \frac{31}{128}b - \frac{7}{32}a + \frac{43}{32}b^2 - 3ba - \frac{9}{8}b^3 + a^2 + \frac{3}{2}b^2a\right). \end{aligned}$$

The two last factors of the right hand sides define elliptic curves over $\mathbb{Q}$. Therefore, we can find at least one rational point on each of them. The coordinates of these rational points give us a point over $\mathbb{Q}(p)$ lying on C (resp. on C'). Therefore, C and

C' are non-singular genus one curves with at least one rational point and hence elliptic curves. □

We are now left to compute the intersection of the two elliptic curves in the variables a, b to obtain the following theorem.

Theorem 3.17. *Let $K := \mathbb{Q}(\alpha)$, where α is a root in an algebraic closure of $\mathbb{Q}$ of the polynomial*

$$X^7 - \frac{917}{216}X^6 + \frac{1183}{576}X^5 + \frac{523}{1536}X^4 - \frac{2267}{110592}X^3 + \frac{305}{442368}X^2 + \frac{91}{7077888}X - \frac{13}{56623104}.$$

Then there exists a hyperelliptic curve of genus two defined over K with a K-rational 17-torsion divisor.

Proof : We specialize V to the fiber above $p = 1$. Then C is the intersection of two elliptic curves defined over $\mathbb{Q}$. Over K this intersection has K-rational points. Therefore, we can find parameters defined over K such that the first three coefficients but not all of the coefficients of the polynomial a vanish. Therefore, we find a polynomial F of degree five which defines our hyperelliptic curve C_p. □

Theorem 3.18. *For all parameters $p \in \mathbb{Q}$ the curve C_p is isomorphic to C_1.*

Proof : The absolute Igusa invariants are constant rational functions in $\mathbb{Q}(\alpha)(p)$. This was computed by Magma. We do not state them here because they are quite large. Therefore, the family C_p consist of exactly one isomorphism class of hyperelliptic curves. □

We see that for higher torsion the algebraic sets which are determined by the leading coefficients of the resulting polynomial become more and more difficult. It seems like this method reaches its limit fast. In the following section we take a step back and consider elliptic curves. The largest prime p such that there exists an elliptic curve with a point of order p is given by $p = 7$. The goal is to construct a one-dimensional family of elliptic curves admitting a point of order seven over the rational numbers.

3.3.4. Application to Elliptic Curves

In this section we use the method of Hensel's Lemma to construct elliptic curves defined over the rational numbers admitting a $\mathbb{Q}$-rational seven-torsion. This is the largest prime p such that there exist an elliptic curve E defined over $\mathbb{Q}$ with a $\mathbb{Q}$-rational p-torsion point on E.

Theorem 3.19. *Let* $F := X^3 + a_2X^2 + a_4X + a_6 \in \mathbb{Q}(\lambda)[X]$ *be given by*

$$\begin{aligned} a_2 :=& \frac{\frac{25}{16}\lambda^4 + \frac{13}{8}\lambda^3 + \frac{15}{16}\lambda^2 + \frac{3}{8}\lambda + \frac{1}{16}}{\left(\lambda + \frac{1}{2}\right)^2}, \\ a_4 :=& \frac{\frac{3}{4}\lambda^5 + \frac{5}{2}\lambda^4 + \frac{3}{2}\lambda^3 + \frac{1}{4}\lambda^2}{\lambda + \frac{1}{2}}, \\ a_6 :=& \frac{9}{4}\lambda^6 + \frac{3}{2}\lambda^5 + \frac{1}{4}\lambda^4. \end{aligned}$$

Then the curve $E/\mathbb{Q}(\lambda) : Y^2 = F(X)$ *is an elliptic curve. Furthermore, regarded as a family of curves* $\mathcal{E}_\lambda$, $\mathcal{E}_\lambda$ *is non-constant and for any smooth specialization to a curve* E_λ *over* $\mathbb{Q}$ *by choosing a parameter* $\lambda \in \mathbb{Q}$ *there is a* $\mathbb{Q}$*-rational seven-torsion point on* E_λ.

Proof : First we compute the discriminant of the defining polynomial F over $\mathbb{Q}(\lambda)$. This gives us

$$\Delta(F) = -\frac{63423\lambda^7\left(\lambda + \frac{1}{3}\right)^7\left(\lambda^3 + \frac{16}{29}\lambda^2 - \frac{1}{29}\lambda - \frac{1}{29}\right)}{512\left(\lambda + \frac{1}{2}\right)^5},$$

what is clearly non-zero in $\mathbb{Q}(\lambda)$. So the right hand side is a degree three polynomial with no multiple roots. This gives us the first statement of the theorem. That $\mathcal{E}_\lambda$ is non-constant as a family can be shown by computing the j-invariant of E. This is given by

$$j(E) = -\frac{117649\left(\lambda^2 + \frac{5}{7}\lambda + \frac{1}{7}\right)^3\left(\lambda^6 - 31\lambda^5 - 40\lambda^4 - 15\lambda^3 + \lambda + \frac{1}{7}\right)^3}{8118144\lambda^7\left(\lambda + \frac{1}{3}\right)^7\left(\lambda + \frac{1}{2}\right)^7\left(\lambda^3 + \frac{16}{29}\lambda^2 - \frac{1}{29}\lambda - \frac{1}{29}\right)}.$$

Again this is obviously non-constant as a rational function in λ over $\mathbb{Q}$. So we are left to show the existence of a seven-torsion point on E_λ for each $\lambda \in \mathbb{Q}$ such that $\Delta(E_\lambda)$ does not vanish. We do this by giving a $\mathbb{Q}(\lambda)$-rational point on E of order seven. Obviously the point $P := \left(0, \frac{3}{2}\lambda^3 + \frac{1}{2}\lambda^2\right)$ is a point on E. This is actually a point with the desired property. □

We can see that we obtain a smooth curve E_λ by specializing the family $\mathcal{E}_\lambda$ to the fiber above λ for $\lambda \in \mathbb{Q} \setminus \left\{0, -\frac{1}{2}, -\frac{1}{3}\right\}$.

We now clarify how the elliptic curve in the theorem is constructed. Let $b := X^2 + X + \lambda^2$ and $R := X^2 + \lambda X + \lambda$ be polynomials defined over $\mathbb{Q}(\lambda)$. Then for $\varepsilon := -2\lambda^3 + 3\lambda^2 - 1$ the following holds

$$\begin{aligned} R^2 &= X^4 + 2\lambda X^3 + (\lambda^2 + 2\lambda)X^2 + 2\lambda^2 X + \lambda^2 = b(X^2 + (2\lambda - 1)X + 1) + \varepsilon X \\ &\equiv \varepsilon X \pmod{b}. \end{aligned}$$

Since over $\mathbb{Q}(\lambda)$ the polynomial b has no root at zero, we can apply Hensel's Lemma 3.6 to lift the congruence to a congruence modulo b^2; that is, we can find a polynomial

$\widetilde{R} \in \mathbb{Q}(\lambda)[X]$ such that

$$\widetilde{R}^2 \equiv \varepsilon X \pmod{b^2}.$$

So there exists a function $f := a(x) + b(x)y \in \mathbb{Q}(\lambda, E)$, where $a := \left(\widetilde{R}^7 \mod b^2\right)$, such that $f \in \mathcal{L}(7\mathcal{O})$, where $\mathcal{O}$ is the point at infinity of E. This function f has a root of multiplicity 7 at the point P, mentioned in the proof of the theorem.

3.4. Relations among Divisors

In this section we want to present a method which is used to construct hyperelliptic curves with a point of high order on its jacobian described in [Fly90]. The idea of this method is to start with a parametrized family of curves and a section on it which is for some specialization a potential N-torsion divisor on the specialization.

The next step is crucial in this method because in this step we have to explicitly compute the MUMFORD representation of the image of the section under the multiplication-by-N-map. This can be a very hard task even for small integers N. If we succeed in the previous step, this gives us equations in the parameters of the family of curves. These equations define a variety and a rational point in this variety corresponds to a hyperelliptic curve in the family fulfilling the imposed conditions on the section.

Since the computation on ND for a section D becomes very hard for large N, it is of interest to reduce this task to a less hard one. The simplest way to achieve this is to compute $\left\lfloor \frac{N}{2} \right\rfloor D$ and $-\left\lfloor \frac{N+1}{2} \right\rfloor D$ instead which gives the same result. But even this becomes unfeasible for relatively small N already.

It appears that these two methods do no longer work if the computation of ND for $N > 5$ is required since the rational functions in the parameters of the family become too large in ND to handle them.

To avoid this problem the idea is to impose not only one relation but a whole set of relations implying the desired relation $ND = 0$. Here we have to take care that the set of relations do not imply $mD = 0$ for some $m|N$ because in this case we get only a torsion point of order dividing m.

3.4.1. Using Certain Normal Forms

We now give a method where a system of relations among divisors is constructed in such a way that it is possible to find curves which fulfill these relations. The idea is to look at a polynomial F defining the curve to be of certain shape. This special shape gives us two rational points on the curve and a certain relation among divisors. Imposing one more relation in a well chosen way implies the existence of the desired torsion divisor.

We work this through with the prime 13 following [CF96]. While in [CF96] the points on the curve giving the 13 torsion divisor have x-coordinate equal to zero and one, we allow all x-coordinates. But in the end we give an isomorphism between the family of [CF96] and the family constructed here.

Let us consider the curve

$$C_{A,\lambda,\mu,\eta} : Y^2 = A(X)^2 - \lambda(X-\mu)^2(X-\eta)^3$$

defined over the rational function field in three variables over the rational numbers $K := \mathbb{Q}(\lambda, \mu, \eta)$, where A is a quadratic polynomial over K. On this curve we have two sections, namely $P_\mu = (\mu, A(\mu))$ and $P_\eta = (\eta, A(\eta))$ together with the relation

$$2P_\mu + 3P_\eta - 5P_\infty = \operatorname{div}(y - A(x)).$$

Assume now that there exists a function $f := y - a(x) \in K(C_{A,\lambda,\mu,\eta})$ such that $\operatorname{div}(f) = 5P_\mu + 1P_\eta - 6P_\infty$ and $a \in \mathbb{Q}(\lambda, \mu, \eta)[X]$ with $\deg(a) = 3$ and a monic. This gives us

$$\begin{pmatrix} 2 & 3 \\ 5 & 1 \end{pmatrix} \begin{pmatrix} P_\mu - P_\infty \\ P_\eta - P_\infty \end{pmatrix} = \begin{pmatrix} 2P_\mu + 3P_\eta - 5P_\infty \\ 5P_\mu + P_\eta - 6P_\infty \end{pmatrix} = \begin{pmatrix} \mathcal{O} \\ \mathcal{O} \end{pmatrix}.$$

Since the matrix in this relation has determinant -13, we can multiply both sides with $-13M^{-1} \in \mathbb{Z}^{2\times 2}$, where M is the matrix from above, and we see that the divisors $P_\mu - P_\infty$ and $P_\eta - P_\infty$ are divisors of order 13.

We now want to determine the polynomial A under the above assumption of the existence of the function $f \in \mathbb{Q}(C)$ with the special divisor implying the 13-torsion element in the jacobian. Plugging in the polynomial a for y and using the fact that

$$\operatorname{div}(f) = 5P_\mu + 1P_\eta - 6P_\infty,$$

we get

$$a(x)^2 = A(x)^2 - \lambda(x-\mu)^2(x-\eta)^3 + (x-\mu)^5(x-\eta).$$

The last summand comes from the relation we impose on the divisors. This equation can be rearranged as follows

$$(a - A(x))(a + A(x)) = (x-\mu)^2(x-\eta)((x-\mu)^3 - \lambda(x-\eta)^2).$$

Then the only possibility to solve this for A is by setting

$$a - A(x) = (x-\mu)^2(x-\eta) \text{ and } a + A(x) = (x-\mu)^3 - \lambda(x-\eta)^2$$

since we need to assure $a(\mu) = A(\mu)$ and $a(\eta) = A(\eta)$. Solving for A gives us

$$A = \frac{1}{2}((\eta - \mu - \lambda)X^2 + 2(\mu^2 + \eta(\lambda - \mu))X + \eta\mu^2 - \mu^3 - \lambda\eta^2).$$

Theorem 3.20. *Assume the specialization of the polynomial*

$$F(X) := A^2 - \lambda(X-\mu)^2(X-\eta)^3$$

with rational parameters is separable. Then the jacobian of the hyperelliptic curve given by $C_{A,\lambda,\mu,\eta} : Y^2 = F(X)$ *has a* $\mathbb{Q}$*-point of order* 13.

Proof : The proof is clear due to the discussion above. □

Remark. *The one-parameter-family of hyperelliptic curves with the same property constructed in [CF96, chapter 8 section 3] by* Cassels *and* Flynn *is* $C_{A,\lambda,0,1}$.

We now show that the constructed family is actually one-dimensional. By the remark above it is clear that the family is at least of dimension one. So we are left to show that there exists for any curve in $C_{A,\lambda,\mu,\eta}$ an isomorphism to a curve in $C_{A,\lambda,0,1}$.

Lemma 3.21. *These curves are all isomorphic over* $\mathbb{Q}$ *to a member of* $C_{A,\lambda,0,1}$.

Proof : Let $\lambda, \mu, \eta \in \mathbb{Q}$ be chosen such that $C_{A,\lambda,\mu,\eta}$ is a hyperelliptic curve.

Since we have assumed that $C_{A,\lambda,\mu,\eta}$ is a hyperelliptic curve, we need $\lambda \neq 0$. Therefore, we can set $\lambda' := \frac{\mu-\eta}{\lambda}$. Because $\mu \neq \eta$, we have $\lambda' \neq 0$. Then we have

$$C_{A,\lambda,\mu,\eta} \cong C_{A,\lambda',0,1}.$$

This can be checked by computing the greatest common divisor of the difference of the numerators of the absolute Igusa invariants of $C_{A,\lambda,\mu,\eta}$ and $C_{A,\lambda',0,1}$ for example by using Magma. □

Corollary 3.22. *The family* $C_{A,\lambda,\mu,\eta}$ *is one-dimensional.*

Replacing the condition of the existence of a function with divisor $5P_\mu + 1P_\eta - 6P_\infty$ by the existence of a function f with divisor

$$\operatorname{div}(f) = 5\iota(P_\mu) + 1P_\eta - 6P_\infty = -5P_\mu + 1P_\eta + 4P_\infty + \operatorname{div}((X-\mu)^5),$$

where $\iota(P_\mu) = (\mu, -A(\mu))$, changes the determinant of our relation matrix to 17 and therefore, a solution for A gives us hyperelliptic curves admitting a point of order 17 on their jacobians.

Since the x-coordinates of P_μ and $\iota(P_\mu)$ are the same, the equation

$$(a - A(x))(a + A(x)) = (x-\mu)^2(x-\eta)((x-\mu)^3 - \lambda(x-\eta)^2)$$

still has to hold. But the change of signs in the y-coordinate of P_μ gives us the following restrictions

$$v(\mu) = -A(\mu), \qquad v(\mu) \neq A(\mu), \qquad v(\eta) = A(\eta), \qquad v(\eta) \neq -A(\eta).$$

Therefore, $(x-\mu) \mid (a+A(x))$, $(x-\mu) \nmid (a-A(x))$, $(x-\eta) \mid (a-A(x))$ and $(x-\eta) \nmid (a+A(x))$ have to hold and we can write

$$a + A(x) = (x-\mu)^2(x-\alpha) \text{ and } a - A(x) = (x-\eta)q(x)$$

for some $\alpha \in \mathbb{Q}(\lambda, \mu, \eta)$ and $q \in \mathbb{Q}(\lambda, \mu, \eta)[X]$. Solving for A and q, we get

$$A = \frac{1}{2}((X-\mu)^2(X-\alpha) - (X-\eta)q)$$

and

$$q = \frac{(X-\mu)^3 - \lambda(X-\eta)^2}{X-\alpha}.$$

Since q is assumed to be a polynomial, we get $(\alpha-\mu)^3 - \lambda(\alpha-\eta)^2 = 0$. Therefore,

$$\lambda = \frac{(\alpha-\mu)^3}{(\alpha-\eta)^2}.$$

So by setting

$$F_{A,\lambda,\mu,\eta} := A^2 - \frac{(\lambda-\mu)^3}{(\lambda-\eta)^2}(X-\mu)^2(X-\eta)^3,$$

where

$$A = \frac{1}{2}\left((X-\mu)^2(X-\lambda) - (X-\eta)\frac{(X-\mu)^3 - \frac{(\lambda-\eta)^3}{(\lambda-\eta)^2}(X-\eta)^2}{X-\lambda}\right),$$

we obtain the following example of a family of hyperelliptic curves with a point of order 17 on the jacobian.

Theorem 3.23. *Assume the specialization of the polynomial $F_{A,\lambda,\mu,\eta}$ with rational parameters is separable. Then the jacobian of the hyperelliptic curve given by $C_{A,\lambda,\mu,\eta}$: $Y^2 = F_{A,\lambda,\mu,\eta}(X)$ has a point of order 17.*

Again the original family constructed by Cassels and Flynn in [CF96] can be obtained by $C_{A,\lambda,0,1}$

Ogawa [Oga94] takes the method one step further to construct a family of curves admitting a 23-torsion divisor. He replaces the form of the defining polynomial by the following one

$$C_{A,\lambda,\mu,\eta} : Y^2 = A(X)^2 - \lambda(X-\mu)^4(X-\eta).$$

If there exists a function $f \in \mathbb{Q}(C_{A,\lambda,\mu,\eta})$ with divisor $\operatorname{div}(f) = -3P_\mu + 5P_\eta - 2P_\infty$, we get that $P_\mu - P_\infty$ is a divisor of order 23. For this construction we have to allow functions f of the form $f = a(x) + b(x)y$ with polynomials $a, b \in \mathbb{Q}[X]$ with $\deg(b) \leq 1$

and $\deg(a) \leq 4$.

Leprévost uses this technique to construct torsion divisors of order $15, 17, 19$ and 21 in [Lep91b].

The so far known record for prime-torsion is constructed by Leprévost in 1993 in [Lep93] by a similar technique. Instead of using only one special form for the defining polynomial F, he imposes two special forms given by polynomials A_1, A_2 of degree three. Letting the polynomials A_1, A_2 be of degree three gives us a polynomial F of degree six. Therefore, the hyperelliptic curve we construct has two points at infinity which we denote by P_∞^+ and P_∞^- and their difference by D. But even more is true. Since the leading term of F is the square of the leading coefficient of A_i, for $i = 1, 2$, both points at infinity are $\mathbb{Q}$-rational.

Consider the curve $C : Y^2 = F(X)$ where

$$F(X) = A_1^2 + \lambda_1(X-\mu)^3(X-\eta)^2 = A_2(X)^2 + \lambda_2(X-\mu)^2(X-\eta)^3$$

and let $P_\rho := (\rho, A(\rho)), D_\rho := P_\rho - P_\infty^+$, for $\rho \in \{\mu, \eta\}$. Taking the difference of the two possibilities to write F and taking care that the solution does not give us an inseparable polynomial F, we get

$$\begin{aligned} A_1 &= \frac{1}{2}\left((X-\mu)^2\left(\lambda_1(X-\mu) - \lambda_2(X-\eta)\right) - (X-\eta)^2\right) \\ A_2 &= \frac{1}{2}\left((X-\mu)^2\left(\lambda_1(X-\mu) - \lambda_2(X-\eta)\right) + (X-\eta)^2\right). \end{aligned}$$

Now we impose one more way to describe the polynomial. This gives us three relations of three different divisors, therefore, we get a point of order dividing the determinant of a three-by-three matrix. The goal now is to take the third way to write F in such a manner that the absolute value of the determinant is equal to 29. Since everything is constructed in such a way, that our divisor in question is not of order one, its order is exactly 29.

So let us now look at the divisors of $y - A_1(x)$ and $\frac{y-A_2(x)}{(x-\mu)^2}$. We have

$$\begin{aligned} \operatorname{div}\left(y - A_1(x)\right) &= 3P_\mu + 2P_\eta - 3P_\infty^+ - 2P_\infty^- = 3D_\mu + 2D_\eta - 2D \\ \operatorname{div}\left(\frac{y - A_2(x)}{(x-\mu)^2}\right) &= -2P_\mu + 3P_\eta - 1P_\infty^+ = -2D_\mu + 3D_\eta + 0D. \end{aligned}$$

This gives us the following relation matrix

$$\begin{pmatrix} 3 & 2 & -2 \\ -2 & 3 & 0 \\ P & Q & R \end{pmatrix} \begin{pmatrix} D_\mu \\ D_\eta \\ D \end{pmatrix} = \begin{pmatrix} \mathcal{O} \\ \mathcal{O} \\ \mathcal{O} \end{pmatrix}.$$

This matrix M has determinant $\det(M) = 13R + 4Q + 6P$ which is -29 if

$$R := -3, Q := 1, P := 1.$$

So searching for a representation of F given by

$$F(X) = A_3^2 + \lambda_3(X - \mu)(X - \eta)$$

gives the desired 29-torsion divisor.

Again taking the difference of two representations, we get

$$\begin{aligned} A_1 &= \frac{1}{2}\left(\frac{g}{u} - \lambda_1 u(X - \mu)(X - \eta)(X - x_0)\right) \\ A_3 &= \frac{1}{2}\left(\frac{g}{u} + \lambda_1 u(X - \mu)(X - \eta)(X - x_0)\right), \end{aligned}$$

where $x_0 \in \mathbb{Q} \setminus \{\mu, \eta\}$, $\lambda_3 := \lambda_1(x_0 - \mu)(x_0 - \eta)$,$u \in \mathbb{Q}^*$ and

$$g := x^2 + (-2\mu - \eta + x_0)x + \mu^2 + 2\mu\eta - 2\mu x_0 - \eta x_0 + x_0^2.$$

By comparing the two solutions for A_1, we see that the solutions are equal if we set

$$\lambda_1 := -\frac{1}{2(\mu - \eta)}, \qquad \lambda_2 := -\lambda_1, \qquad u := -2 \qquad \text{and } x_0 := 2\mu - \eta.$$

This gives us the following family of curves.

Theorem 3.24 ([Lep93])**.** *The jacobian of*

$$C_{\mu,\eta} : Y^2 = A_1^2 + \lambda_1(X - \mu)^3(X - \eta)^2$$

defined over $\mathbb{Q}(\mu, \eta)$, with A_1 and λ_1 as above, has a $\mathbb{Q}(\mu, \eta)$-rational point of order 29.

Remark. *All specializations of $C_{\mu,\eta}$ lie in the same $\mathbb{Q}$-isomorphism class. This can be seen by computing the absolute* Igusa *invariants of $C_{\mu,\eta}$. These are given by*

$$\alpha(C_{\mu,\eta}) = \frac{253}{5776}, \beta(C_{\mu,\eta}) = \frac{34357}{1755904} \text{ and } \gamma(C_{\mu,\eta}) = -\frac{61}{39617584}.$$

Since these invariants are all in $\mathbb{Q}$, we have that $C_{\mu,\eta}$ is just the constant family $C_{0,1}$.

We use the same method to obtain the following result.

Theorem 3.25. *Let $K := \mathbb{Q}(\alpha)$ be the number field given by the relation*

$$\alpha^4 + 2\alpha^3 - 11\alpha^2 + \frac{5}{2}\alpha - \frac{81}{8}.$$

Then there exists a curve C defined over K with a K-rational 31-torsion point on its jacobian.

Proof : We start as in the construction by LEPRÉVOST with two possibilities to write the defining polynomial F of C which give us the relation matrix

$$\begin{pmatrix} 3 & 2 & -2 \\ -2 & 3 & 0 \\ P & Q & R \end{pmatrix} \begin{pmatrix} D_\mu \\ D_\eta \\ D \end{pmatrix} = \begin{pmatrix} \mathcal{O} \\ \mathcal{O} \\ \mathcal{O} \end{pmatrix}$$

with D_μ, D_η, D as above. For $P = 0$, $Q = 2$ and $R = 3$ this matrix M has determinant $\det(M) = -31$. Imposing the third line of relations for F gives us a possibility to write

$$F = A_3(X)^2 + \lambda_3(X-1)^2$$

for some polynomial $A_3 \in K[X]$ of degree three and λ_3 some unit in K. This gives us that

$$(A_3 - A_1)(A_3 + A_1) = \lambda_1(X-1)^2(X-x_0)(X^2 + x_0X + x_0^2)$$

for $x_0 \in K$ such that $\lambda_3 = \lambda_1 x_0^3$. One possibility to solve this for A_1 and A_3 gives us

$$\begin{aligned} 2A_1 &= \frac{X^2 + x_0X + x_0^2}{u} - \lambda_1 u(X-1)^2(X-x_0) \\ 2A_3 &= \frac{X^2 + x_0X + x_0^2}{u} + \lambda_1 u(X-1)^2(X-x_0) \end{aligned}$$

for some unit $u \in K^*$. Again we have to ascertain that there exist $x_0, u, \lambda_1, \lambda_2$ such that both ways of writing A_1 are allowed. This leads to the task to determine the points in the zero-dimensional scheme given by the equations

$$\begin{aligned} 0 &= -u\lambda_1 - \lambda_1 + \lambda_2 \\ 0 &= x_0u^2\lambda_1 + 2u^2\lambda_1 - u\lambda_2 + u + 1 \\ 0 &= -2x_0u^2\lambda_1 + x_0 - u^2\lambda_1 - 2u \\ 0 &= x_0^2 + x_0u^2\lambda_1 + u. \end{aligned}$$

This has a K-rational point $(x_0, u, \lambda_1, \lambda_2) \in K^4$ given by the coordinates

$$\begin{aligned} x_0 &= -\frac{284}{2579}\alpha^3 - \frac{720}{2579}\alpha^2 + \frac{2666}{2579}\alpha - \frac{1063}{2579}, \\ u &= -\frac{528}{2579}\alpha^3 - \frac{1048}{2579}\alpha^2 + \frac{6918}{2579}\alpha + \frac{2092}{2579}, \\ \lambda_1 &= \frac{92}{2579}\alpha^3 - \frac{130}{2579}\alpha^2 + \frac{553}{2579}\alpha + \frac{417}{2579}, \end{aligned}$$

$$\lambda_2 = \alpha.$$

With this choice of parameters we obtain

$$\begin{aligned} F = &\frac{1}{20632}(384\alpha^3 + 1700\alpha^2 - 1280\alpha - 1287)X^6 \\ &+ \frac{1}{10316}(-444\alpha^3 - 2288\alpha^2 + 6638\alpha + 2697)X^5 \\ &+ \frac{1}{10316}(-368\alpha^3 + 3099\alpha^2 - 17686\alpha + 911)X^4 \\ &+ \frac{1}{5158}(92\alpha^3 - 130\alpha^2 + 8290\alpha - 4741)X^3 \\ &+ \frac{1}{2}(-\alpha + 3)X^2 - X + \frac{1}{4} \end{aligned}$$

and the curve $C : Y^2 = F(X)$ has the divisor $(0, A_1(0)) - P_\infty^+$ of order 31 on it. □

In the following, we combine the ideas of Flynn and Leprévost. This combination of the two methods gives us a tool to construct new and already known examples of hyperelliptic curves with a point of prescribed order.

3.4.2. A New Approach

We introduce a new approach which is closely following the ideas of Flynn and Leprévost but is in some sense a combination of these two approaches.

The problem with the approach of Flynn is that we are only allowed to use a two by two matrix where the absolute values of the entries of the first line sum up to five and the absolute values of the entries of the second line sum up to six (resp. eight in the variant of Ogawa).

The problem of the construction of Leprévost is that we have to allow two points at infinity, therefore, we are no longer able to guarantee a success of the method since we have no possibility to assure that we have the right pole order at both points. But since we are allowed to use a three by three matrix, we can construct larger torsion than with the method of Flynn.

Our goal is now to construct a method which allows us to use a three by three relation matrix. This makes it possible to obtain large determinants but stick to a degree five model of the curve with only one point at infinity. So if we can find a solution of this system we can be sure that the multiplicities of the poles at infinity are correct.

Assume we are given a three by three matrix

$$M := \begin{pmatrix} m_{11} & m_{12} & m_{13} \\ m_{21} & m_{22} & m_{23} \\ m_{31} & m_{32} & m_{33} \end{pmatrix} \in \mathbb{Z}^{3\times 3}$$

such that

$$m_{11}, m_{12}, m_{13} > 0, m_{11} + m_{12} + m_{13} = 5$$

and

$$|m_{21}| + |m_{22}| + |m_{23}| = |m_{31}| + |m_{32}| + |m_{33}| = 6$$

and consider the hyperelliptic curve $C : Y^2 = F(X)$ with

$$F = A^2 - \lambda X^{m_{11}}(X-1)^{m_{12}}(X-\mu)^{m_{13}},$$

where $A \in \mathbb{Q}[X]$ is a polynomial of degree two, $\lambda \in \mathbb{Q}^*$ and $\mu \in \mathbb{Q} \setminus \{0, 1\}$. Then we see directly that we have three $\mathbb{Q}$-rational points on C given by

$$P_0 := (0, A(0)), P_1 := (1, A(1)) \text{ and } P_\mu := (\mu, A(\mu)).$$

Let $D_\rho := P_\rho - P_\infty, \rho \in \{0, 1, \mu\}$ be the images of these points in the jacobian. Then we have

$$m_{11}D_0 + m_{12}D_1 + m_{13}D_\mu = \mathcal{O}.$$

To construct the last two lines of the relation matrix, we assume the existence of elements f_i in the function field of C with principal divisor

$$\operatorname{div}(f_i) = m_{i1}P_0 + m_{i2}P_1 + m_{i3}P_\mu - (|m_{i1}| + |m_{i2}| + |m_{i3}|)P_\infty$$

for $i = 2, 3$. If a coefficient of M is negative, we replace the corresponding point in the relation by its hyperelliptic involution. Since we have assumed that the sum of the absolute values of the last two lines in M is equal to six, we get that a function with the correct divisor has to be in $\mathcal{L}(6P_\infty)$, therefore, it is of the form $f_i = y - a_i(x)$, where a_i is a polynomial in X of degree three for $i = 2, 3$. If those functions f_2 and f_3 exist in $\mathbb{Q}(C)$, this gives us that D_ρ for $\rho \in \{0, 1, \mu\}$ is of finite order $N \neq 1$ with $N | \det(M)$. If N is prime, we can be sure that there exists a point of exact order N on $\operatorname{Jac}(C)$. So we are now left to check when such functions f_2 and f_3 exist.

Let us start with a function f_2 which has a principal divisor given by the second line

of M. Such a function exists if and only if

$$a_2^2 = F(X) + \varepsilon X^{|m_{21}|}(X-1)^{|m_{22}|}(X-\mu)^{|m_{23}|}$$

for some $\varepsilon \in \mathbb{Q}^*$. This relation can be rewritten as

$$(a_2 - A)(a_2 + A) = \varepsilon X^{|m_{21}|}(X-1)^{|m_{22}|}(X-\mu)^{|m_{23}|} - \lambda X^{m_{11}}(X-1)^{m_{12}}(X-\mu)^{m_{13}}.$$

The right hand side of this equation is a polynomial of degree six and the factors on the left hand side are both polynomials of degree three, since $\deg(a_2) = 3$ and $\deg(A) = 2$. Therefore, f_2 exists if and only if the right hand side admits a factorization into two polynomials of degree three, say

$$(a_2 - A) = q \in \mathbb{Q}[X] \text{ and } (a_2 + A) = q' \in \mathbb{Q}[X]$$

such that the following conditions are fulfilled:

1. $X - \rho$, $\rho \in \{0, 1, \mu\}$, divides $a_2 + A$ if and only if the signs of the coefficients in M corresponding to the divisor D_ρ are different.
2. $X - \rho$, $\rho \in \{0, 1, \mu\}$, divides $a_2 - A$ if and only if the signs of the coefficients in M corresponding to the divisor D_ρ are the same.
3. If $(X - \rho)|q$, then $(X - \rho) \nmid q'$ for $\rho \in \{0, 1, \mu\}$.

The first two conditions assure that we take care of the possible hyperelliptic involutions occurring in the divisors and the last condition says that the resulting polynomial F has no multiple roots. Having found such a factorization, we find the polynomial A by using the fact that

$$2A = (a_2 + A) - (a_2 - A) = q' - q.$$

We have to make sure that $\deg(A) = 2$ so the leading coefficients of $a_2 - A$ and $a_2 + A$ have to be equal. The easiest way to achieve this is to take $\varepsilon = 1$ and q and q' monic. In our examples we always make this choice.

Proceeding for f_2 in the same way we obtain a second equation for A. Thus, the coefficients of both possibilities to write A have to be the same. Comparing the coefficients gives us a set of rational functions in the parameters. A simultaneous zero of these functions yields a solution.

Remark. *The condition $m_{1i} > 0$ for $i = 1, 2, 3$ is only needed to make the description of the method easier since this rules out some extra cases which would be needed to be considered. The construction works perfectly well also for one of the $m_{1i} = 0$ as presented in the following.*

Algorithm 3 Relations among Divisors for Genus 2

Input: 3×3 Matrix $M = \begin{pmatrix} m_{11} & m_{12} & m_{13} \\ m_{21} & m_{22} & m_{23} \\ m_{31} & m_{32} & m_{33} \end{pmatrix}$ with integral coefficients such that $m_{1j} > 0$, $\sum_j m_{1j} = 5$ and $\sum_j |m_{ij}| = 6$ for $i = 2, 3$.

Output: Hyperelliptic curve C with a point P of order dividing $\det M$ on its jacobian.

function PTORSION(M)
  $p_1 \leftarrow X, p_2 \leftarrow X - 1, p_3 \leftarrow X - \mu$
  for $i = 2, 3$ **do**
    if $\sum_{j \text{ s.t. } \operatorname{sign}(m_{ij})=1}(|m_{1j} - m_{ij}|) > 3$ **then return** 0
    end if
    if $\sum_{j \text{ s.t. } \operatorname{sign}(m_{ij})=-1}(|m_{1j} - m_{ij}|) > 3$ **then return** 0
    end if
    for $j = 1, 2, 3$ **do**
      $q \leftarrow 1$
      $q' \leftarrow 1$
      if $\operatorname{sign}(m_{ij}) = 1$ **then**
        $q' \leftarrow q' p_j^{|m_{1j} - m_{ij}|}$
      else
        $q \leftarrow q p_j^{|m_{1j} - m_{ij}|}$
      end if
    end for
    if $\max(\deg(q), \deg(q')) = 3$ **then**
      ▷ We only state the easiest case. The others are analogous.
      if $\deg(q) \geq \deg(q')$ **then**
        $q' \leftarrow \frac{\varepsilon_i \prod_j p_j^{|m_{ij}|} - \lambda \prod_j p_j^{m_{1j}}}{q}$
      else
        $q \leftarrow \frac{\varepsilon_i \prod_j p_j^{|m_{ij}|} - \lambda \prod_j p_j^{m_{1j}}}{q'}$
      end if
    else
      ▷ These cases we omit in the pseudo-code.
    end if
    $A_i \leftarrow \frac{q' - q}{2}$
  end for
  $S \leftarrow \text{Scheme}(\text{Coefficients}(A_2 - A_1))$ ▷ S is a scheme in the introduced parameters.
  $\text{Sol} \leftarrow \text{RationalPoints}(S)$
  The elements in Sol are tuples of parameters such that we find a solution
  $F \leftarrow A_2^2 - \lambda \prod_j p_j^{m_{1j}}$.
  return $C : Y^2 = F(X)$
end function

We now give some examples which are found by using this method. The first example is demonstrated step by step.

Example 3.6. *Set* $A := -\frac{9}{2}X^2 + 8X - 4$ *and* $F := A^2 - 4X^3(X-1)^2$*, then the hyperelliptic curve*

$$C : Y^2 = F(X)$$

has a $\mathbb{Q}$*-rational* 29*-torsion divisor on it. The curve* C *is isomorphic to the curve in Theorem 3.24.*

Proof : We give the proof by explicitly constructing the curve. Let

$$M := \begin{pmatrix} 3 & 2 & 0 \\ 3 & -1 & 2 \\ -1 & -4 & -1 \end{pmatrix}$$

be the matrix we want to use in the construction. This matrix has determinant

$$\det(M) = 29.$$

The first line gives us that the polynomial F has the form

$$F = A^2 - \lambda X^3(X-1)^2$$

for some quadratic polynomial A and $\lambda \in \mathbb{Q}^*$. Assuming the existence of a function $f_2 := y - a_2(x) \in \mathbb{Q}(C)$ such that

$$\operatorname{div}(f_2) = 3P_0 + \iota(P_1) + 2P_\mu - 6P_\infty,$$

gives us the following equation

$$\begin{aligned}(a_2 - A)(a_2 + A) &= X^3(X-1)(X-\mu)^2 - \lambda X^3(X-1)^2 \\ &= X^3(X-1)\left((X-\mu)^2 - \lambda(X-1)\right).\end{aligned}$$

Since the sign of the first coefficient in the first and the second line is the same and $\deg(a_2 - A) = 3$, we get

$$a_2 - A = X^3 \text{ and } a_2 + A = (X-1)\left((X-\mu)^2 - \lambda(X-1)\right).$$

Therefore, we obtain

$$A = \frac{1}{2}\left((X-1)\left((X-\mu)^2 - \lambda(X-1)\right) - X^3\right).$$

Now we take the third line into account. So we assume the existence of a function $f_3 = y - a_3(x) \in \mathbb{Q}(C)$ such that $\operatorname{div}(f_3) = \iota(P_0) + 4\iota(P_1) + \iota(P_\mu) - 6P_\infty$. This gives us the equation

$$\begin{aligned}(a_3 - A)(a_3 + A) &= \varepsilon X(X-1)^4(X-\mu) - \lambda X^2(X-1)^2 \\ &= X(X-1)^2\left(\varepsilon(X-1)^2(X-\mu) - \lambda X^2\right).\end{aligned}$$

Since the signs of the first two entries in the third line of M are different to the first two coefficients in the first line, we get

$$a_3 - A = \frac{\left(\varepsilon(X-1)^2(X-\mu) - \lambda X^2\right)}{b} \text{ and } a_3 + A = X(X-1)^2 b$$

for some $b \in \mathbb{Q}^*$ which gives us

$$A = \frac{1}{2}\left(X(X-1)^2 b - \frac{\left(\varepsilon(X-1)^2(X-\mu) - \lambda X^2\right)}{b}\right).$$

Since we want A to be of degree two, we need that the coefficient of the degree three term vanishes which is true if and only if $\varepsilon = b^2$. So taking the difference of this two ways to write A, we get the equations

$$\begin{aligned}0 &= \mu^2 + \mu b + \lambda \\ 0 &= -\mu^2 - 2\mu b - 2\mu - 2\lambda \\ 0 &= \mu b^2 + 2\mu b + \lambda b + \lambda + b\end{aligned}$$

which have only one solution where μ, b and λ are non-zero given by

$$\lambda = 4, \qquad \mu = 2, \qquad b = -4.$$

This gives us

$$A = -\frac{9}{2}X^2 + 8X - 4 \text{ and } F := A^2 - 4X^3(X-1)^2.$$

Since we have by construction $\gcd(A, X, (X-1)) = 1$, we get that F has no multiple roots and is of degree five. So it defines a hyperelliptic curve C of genus two. By construction of C we have three functions in $\mathbb{Q}(C)$ given by f_2, f_3 and $y - A(x)$ which give us that

$$M \cdot \begin{pmatrix} D_0 \\ D_1 \\ D_\mu \end{pmatrix} = \begin{pmatrix} \operatorname{div}(Y - A(X)) \\ \operatorname{div}(f_2) \\ \operatorname{div}(f_3) \end{pmatrix}.$$

Since the determinant of M is equal to 29, we have that the three non-trivial divisors D_0, D_1 and D_μ are of order 29.

The existence of an isomorphism to the curve constructed by Leprévost is easily constructed by an affine change of variables. □

Allowing not only parameters from $\mathbb{Q}$ but from some number field, we are able to construct a hyperelliptic curve of genus two defined over a quadratic number field K with a K-rational 37-torsion divisor in the same way.

Theorem 3.26. *Let $K := \mathbb{Q}(\alpha)$ be the number field given by the relation $\alpha^2 + \frac{9}{4}\alpha + 4 = 0$. Set $A := \frac{1}{10}(-13\alpha - 29)X^2 + (3\alpha + 4)X + \frac{1}{10}(-17\alpha - 16)$ and*

$$F := A^2 - \alpha X^3(X-1)^2.$$

Then the curve

$$C_{/K} : Y^2 = F(X)$$

has a K-rational 37-torsion divisor.

Proof : We use the matrix

$$M := \begin{pmatrix} 3 & 2 & 0 \\ 3 & -1 & 2 \\ -1 & 4 & 1 \end{pmatrix}$$

and proceed as in the proof of Example 3.6. □

If we use the above described method with a matrix with composite determinant, we find the following two examples of large torsion.

Example 3.7 (39-torsion)**.** *The matrix*

$$M := \begin{pmatrix} -3 & -2 & 0 \\ -3 & 0 & 3 \\ -1 & -5 & 0 \end{pmatrix}$$

gives a curve C with a 39-torsion divisor. This curve is given by the equation

$$Y^2 = \frac{243}{8}X^5 + \frac{27297}{256}X^4 - \frac{2673}{4}X^3 + \frac{17253}{16}X^2 - 729X + \frac{729}{4}.$$

This curve is not isomorphic to the example of Elkies *[Elk14].*

Reducing the curve modulo the prime of good reduction $p = 5$, we get that the local L-function at $p = 5$ of C is

$$L_{\overline{C}} = 25X^4 + 5X^3 + 7X^2 + X + 1.$$

The Galois *group of the splitting field of $L_{\overline{C}}$ is isomorphic to D_4. Therefore, C is absolutely simple by Theorem 1.21.*

Example 3.8 (40-torsion)**.** *The matrix*

$$M := \begin{pmatrix} 2 & 3 & 0 \\ 2 & 1 & 3 \\ -2 & 3 & 1 \end{pmatrix}$$

gives a curve with a 40-torsion divisor which is isomorphic to the example given by Elkies *on his homepage [Elk14].*

3.4.3. Torsion Depending on the Genus

The construction of the families of genus two curves can be generalized to higher genus. Let us assume we have a curve $C^g_{A,\lambda,\mu,\eta}$ given by

$$C^g_{A,\lambda,\mu,\eta} : Y^2 = A(X)^2 - \lambda(X-\mu)^g(X-\eta)^{g+1} =: F(X),$$

where A is a polynomial of degree g for some positive integer g and $A(\mu) \neq 0 \neq A(\eta)$. Then $C^g_{A,\lambda,\mu,\eta}$ is a hyperelliptic curve of genus g, since the degree of F is $2g+1$ and F is separable. Set $P_\rho := (\rho, A(\rho))$ for $\rho \in \{\mu, \eta\}$, then

$$\operatorname{div}(y - A(x)) = gP_\mu + (g+1)P_\eta - (2g+1)P_\infty.$$

Imposing the additional relation

$$(2g+1)P_\mu + P_\eta - (2g+2)P_\infty = \mathcal{O}$$

gives us the following linear system of equations in the jacobian

$$\begin{pmatrix} g & g+1 \\ 2g+1 & 1 \end{pmatrix} \begin{pmatrix} P_\mu - P_\infty \\ P_\eta - P_\infty \end{pmatrix} = \begin{pmatrix} \mathcal{O} \\ \mathcal{O} \end{pmatrix}.$$

The matrix in the relation has determinant $-2g^2-2g-1$. Therefore, the divisor $P_\mu - P_\infty$ is a torsion divisor of order dividing $2g^2+2g+1$ if there is a possibility to solve the system of relations. It turns out that

$$A := \frac{1}{2}\left((X-\mu)^g(X-\eta) - (X-\mu)^{g+1} - \lambda(X-\eta)^g\right)$$

is a solution. Summing up the discussion above, we get the following theorem.

Proposition 3.27 ([Fly91]). *The family of genus g hyperelliptic curves given by*

$$Y^2 = A(X)^2 - \lambda(X-\mu)^g(X-\eta)^{g+1},$$

where $A = \frac{1}{2}\left((X-\mu)^g(X-\eta) - (X-\mu)^{g+1} - \lambda(X-\eta)^g\right)$ has a $(2g^2+2g+1)$-torsion divisor on it.

Remark. *The family in the previous chapter with a 13-torsion divisor is the same as the family in the theorem for $g = 2$.*

The number field analogon was already constructed in 1971 in the paper [Yam71] of Yamamoto by considering real quadratic number fields with a large *regulator*. The regulator of a real quadratic number field is the logarithm of the fundamental unit.

Proposition 3.28 ([Yam71, Thm. 3.2]). *Let $p > q$ be primes and set*

$$D_g := (p^g q + p + 1)^2 - 4p.$$

Then there exist a constant c_0 depending only on p and q such that for large enough D_g we have

$$\log \varepsilon_g > c_0(\log(\sqrt{D_g}))^3,$$

where ε_g is the fundamental unit of the real quadratic number field $K_g := \mathbb{Q}\left(\sqrt{D_g}\right)$.

Transferring this idea to the function field setting, one obtains the above described family of hyperelliptic curves of genus g with a torsion divisor of order $2g^2+2g+1$.

Remark. *The hyperelliptic curve of genus g defined by*

$$C_g : Y^2 = (\lambda^g X^g(X-1) + \lambda X + 1)^2 - 4\lambda X$$

is isomorphic to the family of curves in Proposition 3.27.

This remark shows a strong connection between results for real quadratic number fields and hyperelliptic curves. Later in this thesis we elaborate more results that can be transferred from number fields to algebraic curves.

Using the same approach but taking $-(2g+1)$ as the lower left entry of the matrix gives a family with a $(2g^2+3g+1)$-torsion point. This construction is done by Leprévost in [Lep91b].

We now construct in the same manner a series of hyperelliptic curves with a torsion point on the jacobian of order quadratic in the genus. This series is in some sense an extremal series since it attains the largest torsion order possible with this method. Unfortunately this implies that it is no longer possible to find a solution to the equations

in the parameters for all g simultaneously. Therefore, we are only able to give examples of curves in this series up to genus four.

A relation matrix of the form

$$\begin{pmatrix} 2g & 1 \\ 1 & 2g+1 \end{pmatrix}$$

gives a torsion divisor of order dividing $4g^2 + 2g - 1$. We first regard the resulting equation

$$(a + A)(a - A) = X(X - 1)((X - 1)^{2g} - \lambda X^{2g-1})$$

for $g = 2$. We factor the right hand side in the following way

$$\begin{aligned} a + A &= X(X - 1)(X + \alpha) \\ a - A &= X^3 + bX^2 + cX + d, \end{aligned}$$

where $b, c, d, \alpha \in \mathbb{Q}$ and $\alpha \neq 0, 1$. This gives us that the relations

$$\begin{aligned} \alpha + b &= -(4 + \lambda) \\ \alpha b + c &= 6 \\ \alpha c + d &= -4 \\ \alpha d &= 1 \end{aligned}$$

have to hold. By solving these equations, we get

$$\begin{aligned} \lambda &= 4 - \frac{\alpha^4 + 6\alpha^2 + 4\alpha + 1}{\alpha^3} \\ b &= -\alpha - (4 + \lambda) \\ c &= \alpha^2 + \alpha(4 + \lambda) + 6 \\ d &= -\alpha^3 - \alpha^2(4 + \lambda) - 6a - 4. \end{aligned}$$

and solving for A gives us the following theorem.

Theorem 3.29. *Assume α is a rational number such that $F := A^2 - \lambda X^4(X - 1)$, where*

$$A := \frac{1}{2}((\alpha - b - 1)X^2 - (\alpha + c)X - d)$$

and b, c, d, λ as above, has no multiple roots. Then the hyperelliptic curve

$$C_\alpha : Y^2 = F(X)$$

of genus two has a divisor of order 19 *in its jacobian.*

Proof : The proof follows directly from the discussion above. □

We now show that the family C_α of hyperelliptic curves is non-constant.

Theorem 3.30. *There are infinitely many pairwise non-isomorphic hyperelliptic curves of genus two with a divisor of order* 19 *in their jacobians.*

Proof : The first absolute IGUSA invariant $\alpha(C_\alpha)$ of the curve C_α given in Theorem 3.29 regarded over the rational function field in the variable α over $\mathbb{Q}$ is given by

$$\alpha(C_\alpha) = \frac{h}{\widetilde{h}^2},$$

where

$$\begin{aligned} h =& \frac{1}{16}\alpha^{24} + \frac{1}{2}\alpha^{23} + \frac{1}{2}\alpha^{22} - \frac{23}{4}\alpha^{21} - \frac{79}{4}\alpha^{20} - \frac{49}{4}\alpha^{19} \\ &+ \frac{289}{8}\alpha^{18} + \frac{93}{4}\alpha^{17} - \frac{1223}{8}\alpha^{16} - \frac{917}{4}\alpha^{15} + \frac{2271}{8}\alpha^{14} + \frac{5307}{4}\alpha^{13} \\ &+ \frac{33799}{16}\alpha^{12} + \frac{8705}{4}\alpha^{11} + \frac{18201}{8}\alpha^{10} + \frac{13935}{4}\alpha^{9} + \frac{86551}{16}\alpha^{8} + \frac{25303}{4}\alpha^{7} \\ &+ 5292\alpha^6 + 3166\alpha^5 + \frac{21583}{16}\alpha^4 + \frac{1607}{4}\alpha^3 + \frac{641}{8}\alpha^2 + \frac{39}{4}\alpha + \frac{9}{16} \text{ and} \\ \widetilde{h} =& \alpha^{12} + 4\alpha^{11} + 8\alpha^{10} - 6\alpha^9 - 34\alpha^8 + 14\alpha^7 \\ &+ 127\alpha^6 + 70\alpha^5 - 133\alpha^4 - 192\alpha^3 - 101\alpha^2 - 26\alpha - 3. \end{aligned}$$

This invariant is non-constant, therefore, it is possible to find infinitely many pairwise non-isomorphic specializations with the desired property. □

The discriminant of C_α is given by

$$\Delta = -\frac{(\alpha+1)^{27}h}{\alpha^{36}},$$

where

$$\begin{aligned} h =& \alpha^{11} + 4\alpha^{10} - 12\alpha^9 - 54\alpha^8 - 18\alpha^7 + 70\alpha^6 \\ &- 155\alpha^5 - 639\alpha^4 - 719\alpha^3 - 358\alpha^2 - 84\alpha - 9 \end{aligned}$$

has no rational roots. Therefore, C_α is a hyperelliptic curve for all $\alpha \in \mathbb{Q} \setminus \{0, -1\}$.

There is a one-dimensional family of hyperelliptic curves of genus two with a $\mathbb{Q}$-rational torsion point of order 19 on the jacobian constructed in [Lep91b]. We now show that this family is non-isomorphic to our family.

We compute the absolute Igusa invariants of both families and compute the algebraic set defined by the numerators of the differences of these invariants (see Magma code in A.2). Since there are three absolute Igusa invariants, this gives us an algebraic set defined by three polynomials in the parameters α for our family and α' for the family of Leprévost. All three polynomials are irreducible, therefore, each of them defines an irreducible plane algebraic curve. Since they are all irreducible, the only possibility to have a common component is to be actually equal. But since they are not equal, we get that they can only intersect in a finite set of points, therefore, only finitely many curves in our family can actually lie in the family of Leprévost. Therefore, the families are not isomorphic.

Remark. *It does not seem that with this set of relations one can expect to easily get results for $g > 4$ since the matrix only gives a degree two factor of $a - A$ as a polynomial in X and for a success we need $\deg(a - A) = g + 1$. So for growing g we get more and more relations that have to hold.*

Despite this remark we are able to do the computation for $g = 3$ and $g = 4$ and give example curves. Furthermore, we conjecture that the construction can be carried over even to arbitrary genus.

Example 3.9. *The hyperelliptic curve of genus three given by*

$$\begin{aligned} C : Y^2 =& \frac{46656}{3125}X^7 + \frac{407097961}{39062500}X^6 + \frac{281238453}{3906250}X^5 - \frac{22959453}{312500}X^4 \\ & - \frac{2767361}{15625}X^3 + \frac{381951}{2500}X^2 + \frac{3093}{6250}X + \frac{1}{2500} \end{aligned}$$

admits a $\mathbb{Q}$-rational divisor of order 41.

Remark. *We get a one-dimensional family of curves of genus three with a 41-torsion divisor. The family is parametrized by the curve given by the polynomial*

$$X^4 + 6X^3Y + 15X^2Y^2 - 3X^2Y + 20XY^3 - 12XY^2 - Y^5 + 15Y^4 - 15Y^3 + Y^2.$$

Example 3.10. *The hyperelliptic curve of genus four given by*

$$\begin{aligned} C : Y^2 =& \frac{6561}{128}X^9 + \frac{22518337}{65536}X^8 - \frac{21217877}{16384}X^7 + \frac{27500023}{16384}X^6 \\ & - \frac{4742069}{4096}X^5 + \frac{1960231}{4096}X^4 - \frac{113003}{1024}X^3 + \frac{5969}{512}X^2 + \frac{59}{128}X + \frac{1}{256} \end{aligned}$$

has a $\mathbb{Q}$-rational point of order 71 on its jacobian.

For $g > 4$ it becomes unfeasible to search for rational points in the parameter space. So we can only state some conjectures about the existence of more curves of this type.

Let $g \geq 5$. Assume there exists a monic polynomial $h \in \mathbb{Q}[X]$ with $\deg(h) = g-1$ and $\lambda \in \mathbb{Q} \setminus \{0\}$ such that h divides the polynomial

$$f := (X-1)^{2g} - \lambda X^{2g-1} \in \mathbb{Q}[X].$$

Then there exists a family of curves C_g of genus g over $\mathbb{Q}$ with a $\mathbb{Q}$-rational divisor of order N with $1 < N \mid (4g^2 + 2g - 1)$.

First assume

$$h = x^{g-1} + \sum_{i=0}^{g-2} h_i X^i \in \mathbb{Q}(h_0, \ldots, h_{g-2})[X],$$

so h is given by $g-1$ parameters. If we now divide f by h and look at the remainder

$$R := f \mod h,$$

we get $\deg(R) = g-2$. So the coefficients of R give us $g-1$ $\mathbb{Q}$-rational equations in the g parameters $\lambda, h_0, \ldots, h_{g-2}$. These equations should cut out a one-dimensional affine algebraic set S in the g-dimensional affine space $\mathbb{A}^g$ with coordinates $\lambda, h_0, \ldots, h_{g-2}$. So at least over some finite field extension K of $\mathbb{Q}$ we expect some K-rational points on S.

Let us start with the hyperelliptic curve of genus g given by the polynomial

$$F := A^2 - \lambda X^{2g}(X-1)$$

for some polynomial A of degree $\deg(A) \leq g$. We now construct the polynomial A in such a way that there exists a function $f := a(x) + y \in \mathbb{Q}(C)$ with divisor

$$P_0 + (2g+1)P_1 - (2g+2)P_\infty,$$

where $P_0 := (0, A(0))$ and $P_1 := (1, A(1))$. This is completely analogous to the considerations for $g \leq 4$. This gives us

$$(a + A) = X(X-1)h \text{ and } (a - A) = \frac{(X-1)^{2g} - \lambda X^{2g-1}}{h}$$

for some polynomial $h \in \mathbb{Q}[X]$ of degree $\deg(h) = g-1$ with

$$h \mid ((X-1)^{2g} - \lambda X^{2g-1})$$

for some number $\lambda \in \mathbb{Q}^*$. If such a polynomial h exists, we can solve for A and get

$$A := \frac{(X-1)^{2g} - \lambda X^{2g-1} - h^2 X(X-1)}{2h}.$$

With this solution, the curve given by

$$C_g : Y^2 = A^2 - \lambda X^{2g}(X-1),$$

would have a $\mathbb{Q}$-rational divisor of order dividing $4g^2 + 2g - 1$.

In the next section we describe the point of view of Patterson, Van der Poorten and Williams to this method. They give a connection to the computation of continued fraction expansions of functions in the function field of a series of curves and the series of curves described so far in this section.

3.4.4. Generalization of the Method

In [PvdPW08] Patterson, Van der Poorten and Williams generalized the method described above. Let $K = \mathbb{Q}$ or K be a finite field, then they start with pairwise relatively prime square-free polynomials $A_1, A_2, A_3 \in K[X]$ with $A_i(0) \neq 0 \neq A_i(1)$ for $i = 1, 2, 3$. Further set

$$f_1 := A_1(X-1)^{g+1-a_1}, f_2 := A_2(X-1)^k X^{g+1-k-a_2}, f_3 := A_3 X^{g+1-a_3},$$

such that $a_i \geq \deg(A_i)$ for $i = 1, 2, 3$ and

$$\deg((f_1 + f_2 - f_3)^2 + 4f_1f_3) = 2g + 1 \text{ or } 2g + 2.$$

Assume further the A_i are chosen in such a way that

$$A_1|(f_2 - f_3), A_2|(f_1 + f_3) \text{ and } A_3|(f_1 + f_2).$$

Proposition 3.31. *The curve*

$$C : Y^2 = (f_1 + f_2 - f_3)^2 + 4f_1f_3 =: F(X)$$

is hyperelliptic of genus g and has a rational point of order N on its jacobian, where $N \geq g^2$.

Proof : For the proof we refer to [PvdPW07a]. □

Since this theorem does not give us a way to explicitly construct such families, we state here a more constructive formulation.

Theorem 3.32 ([PvdPW08, Thm. 1])**.** *Let $K = \mathbb{Q}$ or a finite field, let further*

$f, r, l, m, q, d \in K[X]$ and $k \in \mathbb{N}$ such that f is irreducible, r, l, m are square-free and

$$\gcd(qr, ml) = \gcd(f, qrml) = \gcd(m, l) = 1, q|(mf^k - l).$$

Set

$$C_n : Y^2 = \frac{1}{d^2}\left(\left(qrf^n + \frac{mf^k - l}{q}\right)^2 + 4lrf^n\right).$$

Then $\operatorname{ord}(P_\infty^+ - P_\infty^-) = an^2 + bn + c$ *on the jacobian of* C_n *for some* $a, b, c \in \mathbb{Z}$ *independent of* n *with* $a \neq 0$.

Remark. *One directly sees that the families in the preceding sections are special cases of this family.*

The proof of this theorem directly uses the continued fraction expansion of the function y. This concept we want to present in the next section. Then the proof is completely analogous to a similar result about the fundamental unit in a series of real quadratic number fields which can be found in [PvdPW07b] by the same authors as [PvdPW08].

3.5. Continued Fractions, Pell's Equation and Torsion

We already have seen, that the norm of certain functions in the function field of a curve plays an important role for the construction of curves with a torsion divisor. In this section we consider a special norm equation, namely Pell's Equation, and describe methods to find solutions to this equation.

Let $C : Y^2 = F(X)$ be a hyperelliptic curve of genus g and $\deg(F) = 2g + 2$ defined over some field K. Assume that in the coordinate ring

$$\mathcal{O}(C) = {}^{K[X,Y]}\!/_{(Y^2 - F(X))}$$

of C there exists a non-trivial unit. That is, a function $f = a(x) + yb(x) \in \mathcal{O}(C)^* \setminus K^*$ such that $a^2 - Fb^2 \in K^*$, where a, b are polynomials in X. Then the point $P_\infty^+ - P_\infty^- \in \mathrm{Jac}(C)(K)$ is of finite order. Since we have $a^2 - Fb^2 \in K^*$, the function f is not allowed to have zeros outside the set $\{P_\infty^+, P_\infty^-\}$ and has obviously only poles at infinity. Therefore, $\mathrm{supp}(\mathrm{div}(f)) = \{P_\infty^+, P_\infty^-\}$. But since $\mathrm{div}(f)$ is a degree zero divisor, we need to have $\mathrm{div}(f) = NP_\infty^+ - NP_\infty^-$ for some integer N. It is easy to see that $N \neq 0$ since otherwise f would have to be a constant, what is not allowed.

We can even say more about the connection between Pell's Equation and the order of $P_\infty^+ - P_\infty^-$. Assume N is the exact order of $P_\infty^+ - P_\infty^-$. Then there exists a function

$$f \in \mathcal{L}(ND_\infty) \setminus \mathcal{L}((N-1)D_\infty).$$

This means that either $\deg(a) = N$ or $\deg(b) = N - (g + 1)$.

This was used by Leprévost, Pohst and Schöpp in [LPS04] to construct curves with a divisor of order $5, 7$ and 10.

Lemma 3.33. *Let $a, b, F \in K[X]$ be polynomials of degree $N, N - (g + 1)$ and $2g + 2$ respectively, where N and g are positive integers and F has no multiple roots. Assume that*

$$a^2 - Fb^2 \in K^*.$$

Then the divisor $P_\infty^+ - P_\infty^-$ on the hyperelliptic curve of genus g given by

$$C : Y^2 = F(X)$$

is of order dividing N.

Remark. *By the discussion above the converse statement also holds.*

Unfortunately, this lemma gives us no tool to construct such polynomials a, b and F

satisfying such a relation. So we want to develop a tool which makes it at least in theory possible to construct such polynomials.

The idea is to adapt the theory of real quadratic number fields. Let $K := \mathbb{Q}(\alpha)$ be a real quadratic number field with reduced α. Then we know that $\mathcal{O}_K^*$ can be decomposed in a torsion part and a free part of $\mathbb{Z}$-rank equal to one. The generator of the free part is called *fundamental unit* of $\mathcal{O}_K$ [Neu99, Th. 7.4]. By computing the continued fraction expansion of α, which is periodic, it is possible to compute solutions of PELL's Equation associated with $\mathcal{O}_K$. Therefore, we find units in $\mathcal{O}_K$.

We follow [Art24] to introduce a continued fraction expansion for curves defined over a field K. Another nice reference to this subject for hyperelliptic curves is [Ste99]. So let C/K be a curve with a K-rational point P_∞ on it. This point corresponds to a valuation on $K(C)$. Then there exists a function $x \in K(C)$ such that the completion of $K(C)$ with respect to the valuation corresponding to P_∞ is just the field of power series $K((x^{-1}))$ in x^{-1} over K. Let now $f \in K(C)$ be any function, then there exists a polynomial $h \in K(C)$ such that $(f-h)(P_\infty) = 0$. If we write f as a power series in $K((x^{-1}))$, h is just the part of f with negative exponents, so it is a polynomial in x. We write $[f] := h$. The corresponding object in number fields is the integral part of a real number. So now we are able to define the continued fraction expansion of f analogous to the continued fraction expansion of a real number. We write $f = [a_0, a_1, \ldots]$ with

$$\begin{aligned} f_0 &:= f \\ f_{n+1} &:= \frac{1}{f_n - [f_n]} \\ a_n &:= [f_n]. \end{aligned}$$

In [AR80] ADAMS and RAZAR use continued fraction expansions on elliptic curves defined over a field K of characteristic not equal to two to connect this expansion to the points of finite order. They start with an elliptic curve E given in short WEIERSTRASS form and a rational point P on it. This point P they use to construct a birationally equivalent curve E_P with two points at infinity. Then they show that the divisor given by the difference of the two points at infinity is of finite order if and only if the continued fraction expansion of $y \in K(E)$ is periodic.

VAN DER POORTEN used continued fractions in [vdP04b] to construct all possible torsion occurring on elliptic curves. Moreover he was able to show that 11-torsion is not possible on elliptic curves.

This construction can be used for hyperelliptic curves of genus $g \geq 2$ given by a even degree polynomial F to determine whether the difference of the two points at infinity is of finite order.

Lemma 3.34 ([AR80, Th. 5.1]). *Let $C : Y^2 = F(X)$ be a hyperelliptic curve defined over some field K of genus g and F a polynomial of even degree. Then $\mathcal{O}(C)^* \neq K^*$ if and only if the continued fraction expansion of $y \in \mathcal{O}(C)$ is periodic.*

With Lemma 3.33 we get the following proposition.

Proposition 3.35. *Let $C : Y^2 = F(X)$ by a hyperelliptic curve with a polynomial F of even degree. If the continued fraction expansion of $y \in \mathcal{O}(C)$ is periodic, then*

$$P_\infty^+ - P_\infty^- \in \mathrm{Jac}(C)_{tors}.$$

Some examples where continued fractions are used to construct rational torsion points on elliptic curves and jacobians hyperelliptic curves can be found in [AR80], [vdP04b], [vdP04a] and [vdP05]. All these examples have in common that they need to start with a very special form of curve to make the computations feasible.

We have already seen in the description of the continued fraction expansion in hyperelliptic function fields that there are a lot of analogies to real quadratic number fields. In both cases the continued fraction expansion of a generator of the ring of integers in the field gives us a solution of Pell's equation if such a solution exists in the case of hyperelliptic function fields. Therefore, such a solution gives a non-trivial unit in the ring of integers.

Having these analogies in mind, it is not very surprising that some of the methods which are used to construct real quadratic number fields with large regulators are applicable to the function field case. The property of a large regulator in a real number field translates to the existence of a torsion point of large order. We have already seen one example in Proposition 3.27. This result by Flynn is closely related to the construction of Yamamoto of an infinite series of real quadratic number fields with regulator larger than some constant times the cube of the square root of the discriminant. The central theorem in his construction is the following.

Proposition 3.36 ([Yam71, Thm. 3.1]). *Let S be a set of n primes and assume that there exist infinitely many number fields L such that for all $p \in S$ the prime p is decomposed into two relatively prime primes in $\mathcal{O}_L$.*

Then there exists a constant $c(n, S)$ such that

$$\log \varepsilon > c \left(\sqrt{\Delta(L)} \right)^{n+1}$$

for sufficiently large discriminant $\Delta(L)$, where ε is the fundamental unit of L.

Yamamoto was able to construct such a family for $n = 2$ (see Prop. 3.28).

This result can be generalized in different ways. For instance Halter-Koch is able show in [HK89] the same result by replacing the set of primes by a set of positive integers fulfilling certain properties. With this generalized result he constructs infinite sequences of real quadratic number fields with regulator larger than $\left(\log\sqrt{D}\right)^4$ for sufficiently large discriminant D.

Another way of improving the result of Yamamoto is achieved by Reiter in [Rei85], where he makes the term "sufficiently large discriminant" explicit.

In order to transfer these results to function fields of hyperelliptic curves over the rational numbers, we have to overcome some difficulties. First of all we know that the continued fraction expansion of y needs not to be periodic, since the difference of the two points at infinity has not always finite order. Therefore, we have to require that this specific divisor has finite order.

One crucial fact used in the number field case is that the continued fraction expansion of every reduced quadratic irrationality is periodic. This gives us a decomposition of the set of all quadratic irrationalities A into h disjoint sets, say $A_1, \ldots, A_h$, where each set contains exactly the irrationalities that occur in the same continued fraction expansion and h is the class number of the number field. For function fields over an infinite base field like $\mathbb{Q}$ we can not hope for an equivalent result since for example the divisor $P_\infty^+ - P_\infty^-$ can be of infinite order. So we are not able to decompose the set of all quadratic irrationals into these nice subsets.

In order to prove an analogous result to Proposition 3.36, we need that for all $1 \leq i \leq h$ the relation $\varepsilon = \prod_{\alpha \in A_i} \alpha$ holds (see [Yam71, Prop. 1.2]).

Another possibility to solve the Pell's equation is to use Hensel's Lemma 3.6. We have computed an example for seven-torsion which gives us a one-dimensional family.

Theorem 3.37. *Set*

$$\begin{aligned} F_\lambda := &\left(\frac{1}{4}\lambda^4 + \lambda^2 + 1\right) X^6 + \left(\frac{1}{2}\lambda^5 + \frac{3}{2}\lambda^3 + \lambda\right) X^5 \\ &+ \left(\frac{1}{4}\lambda^6 - \frac{5}{4}\lambda^2 - 1\right) X^4 + \left(\lambda^3 + \frac{3}{2}\lambda\right) X^3 \\ &+ \left(\frac{1}{2}\lambda^6 + \frac{7}{4}\lambda^4 + \frac{5}{2}\lambda^2 + \frac{9}{4}\right) X^2 + \left(-\frac{1}{2}\lambda^5 - \frac{3}{2}\lambda^3 - 2\lambda\right) X \\ &+ \frac{1}{4}\lambda^6 + \lambda^4 + 2\lambda^2 + 1. \end{aligned}$$

For all $\lambda \in \mathbb{Q}$ the hyperelliptic curve $C_\lambda : Y^2 = F_\lambda(X)$ has the $\mathbb{Q}$-rational seven-torsion divisor $P_\infty^+ - P_\infty^-$ on its jacobian.

Proof : First, we compute the discriminant of C_λ, which is given by

$$\begin{aligned}\Delta(C_\lambda) =& -2^4\left(\lambda^2+2\right)^{14} \\ &\cdot\left(\lambda^{14}+21\lambda^{12}+160\lambda^{10}+\frac{1301}{2}\lambda^8+\frac{3167}{2}\lambda^6+\frac{37337}{16}\lambda^4+1921\lambda^2+676\right).\end{aligned}$$

We see that for all $\lambda \in \mathbb{Q}$ the curve C_λ is hyperelliptic of genus two, since the discriminant has no $\mathbb{Q}$-rational roots. So we are left to show that there exists a function

$$f \in \mathcal{L}(7P_\infty^-) \setminus \mathcal{L}(6P_\infty^-)$$

such that $\mathrm{N}_{\overline{\mathbb{Q}}(C)/\overline{\mathbb{Q}}(x)}(f) \in \overline{\mathbb{Q}}^*$. Set

$$\begin{aligned}a :=& \left(-\frac{1}{2}\lambda^2-1\right)X^7+\left(-\frac{3}{2}\lambda^3-\frac{5}{2}\lambda\right)X^6+\left(-\frac{3}{2}\lambda^4-\lambda^2+\frac{3}{2}\right)X^5 \\ &+\left(-\frac{1}{2}\lambda^5+\frac{1}{2}\lambda^3+\frac{1}{2}\lambda\right)X^4+\left(-\lambda^4-\frac{7}{2}\lambda^2-\frac{5}{2}\right)X^3+\left(-\lambda^5-\frac{3}{2}\lambda^3-\frac{1}{2}\lambda\right)X^2 \\ &+\left(\frac{1}{2}\lambda^4+\lambda^2+\frac{1}{2}\right)X-\frac{1}{2}\lambda^5-\frac{3}{2}\lambda^3-2\lambda, \\ b :=& X^4+2\lambda X^3+\left(\lambda^2-1\right)X^2+\lambda^2+1\end{aligned}$$

then $f := a(x)+b(x)y$ does the right thing. □

The polynomial F_λ in Theorem 3.37 is constructed by lifting the congruence

$$X^3+\lambda X^2+\lambda \equiv -1 \pmod{b}$$

with Hensel's Lemma 3.6 to a congruence modulo b^2.

Corollary 3.38. *There are infinitely many hyperelliptic curves defined over $\mathbb{Q}$ of genus two with two points at infinity such that the difference of these two points is of order seven.*

Proof : The absolute Igusa invariants can be found in Appendix A.5. Since these absolute invariants are non-constant functions in the rational function field $\mathbb{Q}(\lambda)$, the assertion follows.

□

In his Maters Thesis [Kos14] at the Rijksuniversiteit Groningen, Koster gives a lot of examples for solutions of the Pell equation.

3.6. Division Polynomials

To determine the N-torsion points on an elliptic curve it is possible to use the so-called *N-th division polynomial*. The polynomial has exactly the x-coordinates of the N-torsion points as roots.

Definition 3.1. *Let $E : Y^2 = X^3 + AX + B$ be an elliptic curve. Define*

$$\begin{aligned}
\Psi_1 &:= 1 \\
\Psi_2 &:= 2Y \\
\Psi_3 &:= 3X^4 + 6AX^2 + 12BX - A^2 \\
\Psi_4 &:= 4Y(X^6 + 5AX^4 + 20BX^3 - 5A^2X^2 - 4ABX - 8B^2 - A^2) \\
\Psi_{2m+1} &:= \Psi_{m+2}\Psi_m^3 - \Psi_{m-1}\Psi_{m+1} \text{ for } m \geq 2 \\
\Psi_2\Psi_{2m} &= \frac{m}{2Y}(\Psi_{m+2}\Psi_{m-1}^2 - \Psi_{m-2}\Psi_{m+1}^2) \text{ for } m > 2.
\end{aligned}$$

These polynomials are called the N-th division polynomials.

Remark. *For odd N it is possible to regard Ψ_N as a polynomial in X (cf. [Sil09]).*

These polynomials have some nice properties. The first important fact is that they encode the multiplication-by-N map on the elliptic curve.

Lemma 3.39. *Let $P := (x, y)$ be a point on the elliptic curve $E : Y^2 = X^3 + AX + B$. Then*

$$[N]P = \left(x - \frac{\Psi_{N-1}\Psi_{N+1}}{\Psi_N^2}(P), \frac{\Psi_{N+2}\Psi_{N-1}^2 - \Psi_{N-2}\Psi_{N+1}^2}{4Y\Psi_N^3}(P) \right).$$

Furthermore, the roots of the N-th division polynomial are exactly the x-coordinates of the elements in $E[N]$.

In [Can94], Cantor constructs polynomials with similar properties for higher genus hyperelliptic curves. Let $P = (x, y) \in C(\mathbb{Q})$ be a point on a hyperelliptic curve given by $C : Y^2 = F(X)$, where $\deg(F) = 2g + 1$. The goal is to compute $NP - NP_\infty$ for an integer N. This result can be easily extended to all reduced divisors of the form $\sum_{i=1}^r a_i P_i - (\sum_i a_i)P_\infty$ by computing the multiple for every single point P_i and then sum up the results using Cantors algorithm.

The idea is to use the Padé approximation of y expanded as a power series in x. That is a approximation given by polynomials A_N, B_N and a formal power series C_N in x such that $A_N(x) - B_N(x)y = x^N C_N$ in the ring of formal power series in x and the degrees of A_N and B_N are bounded by $\deg(A_N) \leq \frac{N+g}{2}$ and $\deg(B_N) \leq \frac{N-g-1}{2}$. For simplicity of the formulae Cantor made an affine change of variables to move the point of interest to a point with x-coordinate equal to zero. This can be achieved in the following way.

Assume our hyperelliptic curve is given by $C : Y^2 = F(X)$, where $\deg(F) = 2g + 1$, and $P = (x(P), y(P)) \in C(\mathbb{Q})$ is the point we are interested in. Then $X \mapsto x(P) - X$ gives us an isomorphic model of the curve passing through $P_0 := \left(0, (-1)^{g+1}\right)$.

Assume we have found such an approximation $A_N(x) - B_N(x)y = x^N C_N$ for y. Let us consider the principal divisor given by the function $f := A_N(x) - B_N(x)y \in K(C)$. This divisor is of the form $\operatorname{div}(f) = D + NP - (N + h)P_\infty$, where D is some effective divisor of degree h given by the polynomial

$$D_N := \frac{A_N^2 - B_N^2 F}{X^N}.$$

Thus, we have that the divisor $D + hP_\infty$ is the negative of $N(P - P_\infty)$.

These considerations yield that for $P := (0, y(P)) \in C(\mathbb{Q})$ and an integer $3 \leq N \in \mathbb{Z}$ the u-coordinate in Mumford representation of $N(P - P_\infty)$ is given by D_N.

As noted above, it is always possible by a suitable change of variables to assume the point of interest has x-coordinate equal to zero.

Definition 3.2. *Let f be a smooth function and m, n be positive integers. Then the rational function*

$$R := \frac{\sum_{i=0}^{m} a_i x^i}{1 + \sum_{i=1}^{n} b_i x^i}$$

*with $f^{(k)}(0) = R^{(k)}(0)$ for $0 \leq k \leq n + m$ is called (m, n)-*Padé approximant *of f.*

For properties of Padé approximants we refer to [BGM96].

Theorem 3.40. *Set $m_N := \lfloor \frac{N+g}{2} \rfloor$ and $n_N := \lfloor \frac{N-g-1}{2} \rfloor$ and (A_N, B_N) the (m_N, n_N)* Padé *approximant of y. Then there exists a formal power series C_N such that*

$$A_N - yB_N = x^N C_N.$$

In the paper [Can94] Cantor gives nice determinant relations and recursive formulas to compute the polynomial D_N which gives us the u-coordinate in the Mumford representation of $N(P - P_\infty)$.

Theorem 3.41 ([Can94, Th. 8.35])**.** *Let $N \geq g + 1$ be an integer and $P := (x(P), y(P))$ be a point on the curve $C : Y^2 = F(X)$. Then $N(P - P_\infty)$ can be represented in* Mumford *representation by*

$$N(P - P_\infty) = \left(\delta_N \left(\frac{x(P) - X}{4y(P)^2} \right), \varepsilon_N \left(\frac{x(P) - X}{4y(P)^2} \right) \right),$$

where δ_N, ε_N are the polynomials given in [Can94, p.133, formula 8.7].

Remark. *The polynomials δ_N, ε_N are directly connected to the (m_N, n_N)-*PADÉ *approximant of y as a power series in x.*

Using PADÉ approximation to compute a rational function that is a good approximant of the power series expansion of y is not the only possibility to construct division polynomials. Essentially every method to approximate y as a power series up to precision N, that is, finding a rational function $\frac{a}{b}$ in x such that $a + by = x^N c$ with a power series c, solves the task. For example using a continued fraction expansion of y and its convergents is another possibility to construct division polynomials (see Section 3.5). The reason for using PADÉ approximation is that there exist nice recurrence formulas for the computation. Therefore, this approach makes the computation of such an approximant easier.

Another possibility to construct division polynomials for hyperelliptic curves of the form $C : Y^2 = X^5 + \sum_{i=0}^{4} a_i X^i$ is to use the hyperelliptic sigma function and some of its logarithmic derivatives. This function was used by GRANT in [Gra90] to define an embedding of the jacobian of the curve in $\mathbb{P}^8$. This construction can be found in [Kan05] by KANAYAMA and [Ôni02] by ÔNISHI. We will not go in further detail in this area since for large N the computation of the N^{th}-division polynomials is not feasible.

3.7. Torsion on Split Jacobians

In this section we want to present a method to construct large torsion subgroups on jacobian varieties which are isogenous to a product of elliptic curves. We follow [HLP00] by Howe, Leprévost and Poonen. In this paper they construct jacobians of genus two and three hyperelliptic curves defined over $\mathbb{Q}$ with a rational torsion subgroup of order 128 for genus two and order 864 for genus three. Their approach is to start with two (resp. three) non-isomorphic elliptic curves admitting a large torsion subgroup and then construct an isogeny of low degree to a jacobian of a hyperelliptic curve.

Proposition 3.42. *Let $E/K, E/K'$ be elliptic curves defined over the field K and let L be the separable closure of K. Let $G \subset (E \times E')[2](L)$ be the graph of an isomorphism of the two-torsion subgroups of E and E' that is not the restriction of an isomorphism of E and E'. Then the abelian variety ${}^{(E \times E')}\!/_{G}$ is L-isomorphic to the jacobian of a curve C defined over L.*

Using this proposition, one can explicitly construct an affine model of the genus two hyperelliptic curve C mentioned in [HLP00, Prop. 4]. They obtain in this way the following result.

Proposition 3.43 ([HLP00, Thm. 1])**.** *Let G be one of the following groups*

$$\mathbb{Z}/20\mathbb{Z}, \mathbb{Z}/21\mathbb{Z}, \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}, \mathbb{Z}/30\mathbb{Z}, \mathbb{Z}/35\mathbb{Z}, \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}, \mathbb{Z}/40\mathbb{Z},$$
$$\mathbb{Z}/45\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}, \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}, \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}, \mathbb{Z}/60\mathbb{Z}, \mathbb{Z}/63\mathbb{Z}, \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z},$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z},$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}.$$

Then there exist infinitely many hyperelliptic curves C of genus two with split jacobian such that $G \hookrightarrow \mathrm{Jac}(C)_{tors}(\mathbb{Q})$.

Using the same approach but with an isomorphism of the three-torsion subgroups of the elliptic curves, Howe produces in [How14] a hyperelliptic curve such that the jacobian has a 70-torsion point. This is the so-far-known record for the torsion order of a jacobian of a genus two hyperelliptic curve.

Proposition 3.44 ([How14, Thm. 1])**.** *Set*

$$C : Y^2 + (2X^3 - 3X^2 - 41X + 110)Y = X^3 - 51X^2 + 425X + 179.$$

Then there exist a $\mathbb{Q}$-rational divisor of order 70 on C.

3.8. Torsion in Jacobians of Superelliptic Curves

In this section we describe the construction of superelliptic curves with a divisor of given order. First we concentrate on curves of the form $C : Y^3 = F(X)$, where F is a cube free polynomial. Obviously for such curves $[K(C) : K(x)] = 3$. So we have three embeddings of $K(C)$ in the algebraic closure of $K(x)$. If ζ_3 denotes a primitive third root of unity and we choose a cube root y of F, we get that the non-trivial embeddings are given by $\sigma(y) = \zeta_3 y$ and σ^2.

Definition 3.3. *Let C be a non-singular curve of genus $g > 1$ defined over a field K with function field $K(C)$. C is called* superelliptic *if there exist $x, y \in K(C)$ such that $y^n = F(x)$ for some $2 \leq n \in \mathbb{N}$ and $F \in K[X]$.*

Definition 3.4. *For an element $\sum_{i=m}^{\infty} a_i X^{-i} =: \phi \in \overline{\mathbb{Q}}((X^{-1}))$ in the field of* Laurent series *over $\mathbb{Q}$ with $a_m \neq 0$ we write*

$$\begin{aligned} \deg(\phi) &:= -m \\ |\phi| &:= 2^{-m} \\ \operatorname{sgn}(\phi) &:= a_m. \end{aligned}$$

Furthermore, we set $\deg(0) := -\infty$ and $|0| = 0$.

Furthermore, let $\overline{\mathbb{Q}}(C)$ be the function field of degree three of a curve C and let $x \in \overline{\mathbb{Q}}(C)$ be a transcendental element such that $\overline{\mathbb{Q}}(C)/\overline{\mathbb{Q}}(x)$ is separable. Further, let σ be a non-trivial automorphism of $\overline{\mathbb{Q}}(C)/\overline{\mathbb{Q}}(x)$. If we have exactly one embedding $\overline{\mathbb{Q}}(C) \hookrightarrow \overline{\mathbb{Q}}((X^{-1}))$, then we define

$$|\sigma(\alpha)| := \left| \frac{\mathrm{N}_{K(C)/K(x)}(\alpha)}{\alpha} \right|^{\frac{1}{2}}.$$

Lemma 3.45. *Let $\alpha, \beta \in \overline{\mathbb{Q}}((X^{-1}))$. Then $|\alpha\beta| = |\alpha||\beta|$ and $|\alpha + \beta| \leq \max\{|\alpha|, |\beta|\}$, with equality if and only if $\operatorname{sgn}(\alpha) \neq -\operatorname{sgn}(\beta)$ and $|\alpha| = |\beta|$.*

The goal of this section is to prove the following theorem.

Theorem 3.46. *Set $E_k := X^k + 1, M_k := E_k^3 + 1, F_k := \frac{M_k^3 - 1}{E_k^3}$ and $C_k : Y^3 = F_k$. Write $g(C_k)$ for the genus of C_k. Then on C_k there exist a $\mathbb{Q}$-rational torsion divisor of order $\frac{g(C_k)}{2} + 1$.*

The proof is split into several lemmas. These lemmas are the characteristic zero analogs to the ones of [Sch00].

Lemma 3.47. *Let $C/K : Y^3 = F(X)$ be a superelliptic curve and $K(C)$ its function field. If F is square free, then the ring of integers in $K(C)$ is generated by $1, y, y^2$ as a $K[x]$-module.*

Lemma 3.48. *Set $E_k := X^k + 1, M_k := E_k^3 + 1$ and $F_k := \frac{M_k^3 - 1}{E_k^3}$. Then F_k is a square-free polynomial.*

Proof : First we compute

$$\begin{aligned} F_k &= \frac{M_k^3 - 1}{E_k^3} & &= \frac{(E_k^3 + 1)^3 - 1}{E_k^3} \\ &= \frac{E_k^9 + 3E_k^6 + 3E_k^3}{E_k^3} & &= E_k^6 + 3E_k^3 + 3. \end{aligned}$$

Now assume $P \in \mathbb{Q}[X]$ such that $P^2 \mid F_k$. This happens if and only if $P \mid \gcd(F_k, F_k')$, where G' denotes the formal derivative of $G \in \mathbb{Q}[X]$. We see

$$F_k' = (E_k^6 + 3E_k^3 + 3)' = 6E_k^5 E_k' + 9E_k^2 E_k' = 3E_k^2 E_k'(2E_k^3 + 3) = 3kE_k^2 X^{k-1}(2E_k^3 + 3)$$

and since $\gcd(F_k, E_k) = \gcd(F_k, X) = 1$ we get $P \mid \gcd(F_k, 2E_k^3 + 3)$. So we have

$$\begin{aligned} P \mid \gcd(F_k, 2E_k^3 + 3) &\Rightarrow P \mid F_k \text{ and } P \mid (2E_k^3 + 3) \\ &\Rightarrow P \mid (F_k - (2E_k^3 + 3)) \\ &\Rightarrow P \mid (E_k^3(E_k^3 + 1)) \\ &\overset{P \mid (2E_k^3+3) \Rightarrow P \nmid E_k}{\Rightarrow} P \mid (E_k^3 + 1) \Rightarrow P \in \mathbb{Q}^*, \end{aligned}$$

since also $P \mid (E_k^3 + \frac{3}{2})$ by assumption. So $\gcd(F_k, F_k') = 1$, therefore, F_k is a square-free polynomial. □

Lemma 3.49. *Let F_k be as before and $C_k : Y^3 = F_k$. Then the genus of C_k is $g(C_k) = 6k - 2$.*

Proof : This follows directly from the Riemann-Hurwitz Genus Formula 1.5. □

We now show that for any choice of a positive integer k the polynomial F_k is square free. This gives us that for any k the ring of integers in the function field of C_k is generated by $1, y$ and y^2.

The goal is to show that there exists a non-trivial unit in $\mathcal{O}(C_k)$. If such a unit exists, we get that the principal divisor is only supported at infinity. In the following lemma we compute the places at infinity.

Lemma 3.50. *Let C_k be as above. Then there are two $\mathbb{Q}$-rational places, denoted by $P_{\infty,0}$ and D_∞ above infinity.*

Proof : In order to determine the the places above infinity we introduce new variables $U := \frac{1}{X}$ and $V := \frac{Y}{X^{2k}}$. Then

$$V^3 = \left(1 + U^k\right)^6 + 3\left(U^k + U^{2k}\right)^3 + 3U^{6k}$$

defines a curve that is birational equivalent to C_k. With the equation above we get $v^3 - 1 = (v-1)(v^2+v+1)$ lies in the ideal above $u\mathbb{Q}[u]$, where u, v are the images of U, V in the function field of the curve. Thus we get $(u) = (u, v-1)(u, v^2+2+1) \in \mathbb{Q}[u, v]$. This proves the statement. □

As we have already seen in the methods for hyperelliptic curves, there is a close connection between the existence of non-trivial units in the coordinate ring and the existence of a rational torsion divisor. We now show, that there exists a non-trivial unit in $\mathcal{O}(C_k)$. This gives us a rational function supported only at infinity. But since we have exactly two rational places at infinity, we get a torsion point on the jacobian.

Lemma 3.51. *Let C_k be as before. Then $\phi := M_k - E_k y \in \mathcal{O}(C_k)$ is a unit and*

$$\phi^{-1} = M_k^2 + M_k E_k y + E_k^2 y^2.$$

Proof : We have

$$\mathrm{N}_{\overline{\mathbb{Q}}(C_k)/\overline{\mathbb{Q}}(x)}(\phi) = M_k^3 - E_k^3 F_k = 1.$$

This proves the fact that ϕ is a unit. Furthermore, we compute

$$\begin{aligned}\phi(M_k^2 + M_k E_k y + E_k^2 y^2) &= M_k^3 - F_k E_k^3 + (M_k^2 E_k - M_k^2 E_k)y + (E_k^2 M_k - E_k^2 M_k)y^2 \\ &= \mathrm{N}_{\overline{\mathbb{Q}}(C_k)/\overline{\mathbb{Q}}(x)}(\phi) = 1.\end{aligned}$$

□

In the following we want to show that the unit we have found is actually a fundamental unit. For this we need some helpful lemmas for the computations in the function field.

Lemma 3.52. *Let $\alpha \in \overline{\mathbb{Q}}(C_k)$ be given by $\alpha := A + By + Cy^2$ with $A, B, C \in \overline{\mathbb{Q}}(x)$. Then*

$$\begin{aligned}A &= \frac{1}{3}\left(\alpha + \alpha^\sigma + \alpha^{\sigma^2}\right), \\ B &= \frac{1}{3y}\left(\alpha + \zeta_3^2\alpha^\sigma + \zeta_3\alpha^{\sigma^2}\right), \\ C &= \frac{1}{3y^2}\left(\alpha + \zeta_3\alpha^\sigma + \zeta_3^2\alpha^{\sigma^2}\right),\end{aligned}$$

where ζ_3 is a primitive third root of unity and σ is the automorphism defined by $y \mapsto \zeta_3 y$.

Proof : The first assertion follows directly from the fact $3A = \mathrm{Tr}(\alpha)$. The other two assertions follow directly from the fact that $1 + \zeta_3 + \zeta_3^2 = 0$. □

Lemma 3.53. *Let C_k be as before. Then we have $|M_k| = |E_k y|$.*

Proof : By assumption we have $(E_k y)^3 = M_k^3 - 1$, therefore, $|(E_k y)^3| = |M_k^3|$. This gives the result. □

Lemma 3.54. *Let C_k be as before. Then $|E_k| < |y|$.*

Proof : By construction we have $E_k^3 F_k = M_k^3 - 1$. Taking the derivative with respect to X, we get $3E_k^2 E_k' = 3M_k^2 M_k'$. Since $\gcd(E_k, M_k) = 1$, this implies $E_k^2 \mid M_k'$. So we compute

$$|E_k|^2 \leq |M_k'| < |M_k| = |E_k y|,$$

which proves the lemma. □

Lemma 3.55. *Let C_k and ϕ be as before. Then ϕ is not a power in $\mathcal{O}(C_k)$.*

Proof : Assume there exists a unit $\varepsilon \in \mathcal{O}(C_k)^*$ such that $\phi = \varepsilon^a$ for some $a \in \mathbb{N}$. By Lemma 3.47 there exist polynomials $A, B, C \in \mathbb{Q}[x]$ such that $\varepsilon = A + By + Cy^2$. Then $A \neq 0$ since otherwise $y \in \mathcal{O}(C_k)^*$ would have to hold. But this is obviously not true.

We now consider two cases. In the first case we assume $|\phi| > 1$. Then we get $|\varepsilon| = |\phi|^{\frac{1}{a}}$. Since $|\phi| > 1$, we know $|\phi^\sigma| < 1$, using the fact that ϕ is a unit. But this gives us $|\phi| = |M_k|$ because $|\phi| = |\phi + \phi^\sigma + \phi^{\sigma^2}| = |M_k|$. Now we can use Lemma 3.54 and Lemma 3.53 to deduce $|\phi| < |y|^{\frac{2}{a}}$.

In the second case we assume $|\phi| < 1$. But since ϕ is a unit, we get $|\phi^{-1}| > 1$. The same arguments as before and Lemma 3.51 give us $|\phi^{-1}| = |M_k|^2$. So we have $|\varepsilon^\sigma| = |\phi^\sigma|^{\frac{1}{a}}$. Using the fact that by definition for a unit $|\phi^\sigma| = |\phi|^{-\frac{1}{2}}$, we again obtain $|\phi^\sigma| < |y|^{\frac{2}{a}}$.

Using this fact, we now give estimates for $|B|$ and $|C|$. Applying Lemma 3.52, we get

$$|B| = |y|^{-1}|\varepsilon + \zeta_3^2\varepsilon^\sigma + \zeta_3\varepsilon^{\sigma^2}| = |y|^{-1}\max\{|\varepsilon|, |\varepsilon^\sigma|\},$$
$$|C| = |y|^{-2}|\varepsilon + \zeta_3\varepsilon^\sigma + \zeta_3^2\varepsilon^{\sigma^2}| = |y|^{-2}\max\{|\varepsilon|, |\varepsilon^\sigma|\}.$$

By the discussion above we have $\max\{|\varepsilon|, |\varepsilon^\sigma|\} < |y|^{\frac{2}{a}}$. So

$$|B| < |y|^{\frac{2}{a}-1} \text{ and}$$
$$|C| < |y|^{\frac{2}{a}-2}.$$

Assume $B \neq 0$, then $1 \leq |B| < |y|^{\frac{2}{a}-1}$. Therefore, $\frac{2}{a} - 1 > 0$. But this is only true for $a = 1$ and this gives us ϕ is not a power.

If $B = 0$, we can deduce $C \neq 0$ so $1 \leq |C| < |y|^{\frac{2}{a}-2}$. This gives a contradiction since $2a \geq 2$ for all positive integers a. This proves that ϕ is not a power in $\mathcal{O}(C_k)$. □

We are now ready to give the proof of the theorem.

Proof of Theorem 3.46: By Lemma 3.51 we have a unit ϕ in $\mathcal{O}(C_k)$. Therefore, we have $\operatorname{supp}(\operatorname{div}\phi) \subset \{P_{\infty,0}, D_\infty\}$ by Lemma 3.50. Since $\deg(D_\infty) = 2 = 2\deg(P_{\infty,0})$ and

$$\phi \in \mathcal{L}(3kD_\infty) \setminus \mathcal{L}((3k-1)D_\infty) \text{ or } \phi^{-1} \in \mathcal{L}(3kD_\infty) \setminus \mathcal{L}((3k-1)D_\infty),$$

we get $\operatorname{div}(\phi) = \pm 3k(2P_{\infty,0} - D_\infty)$. Therefore, the divisor $D_0 := 2P_{\infty,0} - D_\infty$ has to be of order dividing $3k$. But since by Lemma 3.55 ϕ is not a power in $\mathcal{O}(C_k)$, we get that $\operatorname{ord}(D_0) = 3k = \frac{g(C_k)}{2} + 1$. □

This series of superelliptic curves C_k defined over the rational numbers is the first known series of superelliptic curves with a torsion point of order linear in the genus. In the following short section we describe a strategy that gives for a fixed prime p a superelliptic curve with a point of order p on the jacobian. The construction is analogous to the hyperelliptic case in Section 3.3.

3.9. Torsion in Superelliptic Curves via Hensel Lifting

We now describe a possibility to find solutions to norm equations in function fields of degree larger than two. Let us assume we have a superelliptic curve $C/\mathbb{Q}$ defined by $Y^k - F(X)$ for some positive integer k. Then functions of the form $a(x) + b(x)y \in \mathbb{Q}(C)$, where $a, b \in \mathbb{Q}[X]$, have a norm given by

$$\mathrm{N}_{\overline{\mathbb{Q}}(C)/\overline{\mathbb{Q}}(x)} = a(x)^k - b(x)^k F.$$

Since we are interested in functions such that the norm is some p^{th}-power for a prime p with $p \nmid k$, we assume $a(x)^k - b(x)^k F = \lambda x^p$ for some $\lambda \in \mathbb{Q}^*$. Hence, solving for F yields

$$F = \frac{a^k - \lambda X^p}{b^k}.$$

So we can search for a polynomial b such that X is a k^{th}- power modulo b and lift this congruence to a congruence modulo b^k.

Using this construction with $b = 1$ we obtain the following easy theorem.

Theorem 3.56. *Let p be a prime and k a positive integer such that $p \nmid k$ and $p > k$ and $\lambda \in \mathbb{Q} \setminus \{0\}$. Then set $C_{p,k,\lambda} : Y^k = (X-1)^k - \lambda X^p$. Then $g(C_{p,k,\lambda}) = \frac{1}{2}(k-1)(p-1)$ and $C_{p,k,\lambda}$ admits a torsion divisor of order p.*

Proof : The statement about the genus of the curve follows directly from the RIEMANN-HURWITZ Genus Formula 1.5. Furthermore, the curves $C_{p,k,\lambda}$ all have one point P_∞ at infinity. The function $\phi := (x-1) - y$ has norm

$$\mathrm{N}_{\overline{\mathbb{Q}}(C_{p,k,\lambda})/\overline{\mathbb{Q}}(x)} = \lambda x^p.$$

So we get $\mathrm{div}(\phi) = p(0,(-1)^k) - pP_\infty$. Therefore, $\mathrm{ord}((0,(-1)^k) - P_\infty)$ divides p. Since p is prime and $\mathrm{ord}((0,(-1)^k) - pP_\infty) \neq 1$, the theorem is proven. □

We see that the approach using HENSEL's Lemma also works for the construction of superelliptic curves with a torsion point on the jacobian. Since we have to restrict to a very special form of function in the function field, one can expect that here other methods are more fruitful.

3.10. A Family of Curves with a Torsion Divisor Quadratic in the Genus

In this section we construct a family of curves defined over $\mathbb{Q}$ given by an polynomial $F(X,Y)$ with $\deg_Y(F) = 3$. This family is special in the sense, that it is neither a family of hyper- nor superelliptic curves. This work is analogous to the number field considerations of KÜHNER in [Küh95].

We set $F_k := Y^3 - X^kY^2 - (X-1)Y - X^k$ for $k > 0$ and consider the curve C_k over $\mathbb{Q}$ defined by F_k.

Lemma 3.57. *The genus of C_k is $g(C_k) = 2k - 2$.*

Proof : This follows directly from the RIEMANN-HURWITZ Genus Formula 1.5. □

Lemma 3.58. *Let $k > 1$. Then C_k has two singular places at infinity. One place is inert and is denoted by P_∞, above the other one there are lying two points which are conjugates of each other. The degree two divisor defined by the sum these two points we denote by D_∞.*

Proof : We consider the projective closure of C_k by taking the homogenization of F_k. This is defined by

$$Y^3Z^{k-1} - X^kY^2 - XYZ^k + YZ^{k+1} - X^kZ^2.$$

So we get the two points $(1:0:0)$ and $(0:1:0)$ at infinity. We now determine the behavior of the points at infinity. For this purpose we introduce the variable $U := \frac{1}{X}$ and consider the curve C_k' defined by

$$U^kY^3 - Y^2 - (U^{k-1} - U^k)Y - 1.$$

Then C_k' and C_k are birationally equivalent and we have that $y^2 + 1$ lies in the ideal $u\mathbb{Q}[u,y]$, where u, y are the images of U, Y in the function field of C_k'. This proves the statement.

□

This lemma shows that the unit rank in the coordinate ring $\mathcal{O}(C_k)$ is at most one. This fact is used later to show the existence of the torsion divisor. We now show that there exists a non-trivial unit in the coordinate ring. Hence, the unit rank has to be equal to one.

Proposition 3.59. *The element*

$$\varepsilon := y\left(\frac{y}{y-x^k}\right)^k$$

is a unit in $\mathcal{O}(C_k)$.

We split the proof of the proposition into two lemmas. First we show that the inverse of ε is integral over $\mathbb{Q}(x)$.

Lemma 3.60. ε^{-1} *is an integral element in* $\mathbb{Q}(C_k)$.

Proof : In $\mathbb{Q}(C)$ we have

$$\frac{y-x^k}{y} = 1 - x^k y^{-1} = -y^2 + x^k y + x,$$

where the last equation follows from the fact that $x^k = y^3 - x^k y^2 - (x-1)y$ in $\mathbb{Q}(C_k)$. So we compute

$$\varepsilon^{-1} = \frac{1}{y}\left(\frac{y-x^k}{y}\right)^k = \frac{(-y^2+x^k y+x)^k}{y}.$$

But since x^k is divisible by y, we get an element in $\mathcal{O}(C_k)$. □

Lemma 3.61. ε^{-1} *is a unit in* $\mathcal{O}(C_k)$*, more precisely we have* $\mathrm{N}_{\overline{\mathbb{Q}}(C_k)/\overline{\mathbb{Q}}(x)}(\varepsilon^{-1}) = -1$.

Proof : Set $\alpha := y - x^k$. Then we compute

$$\begin{aligned}\alpha^2 &= y^2 - 2x^k y + x^{2k}\\ \alpha^3 &= y^3 - 3x^k y^2 + 3x^{2k} y - x^{3k}\\ &= -2x^k y^2 + (3x^{2k} + x - 1)y - x^{3k} + x^k.\end{aligned}$$

Therefore, we get

$$\alpha^3 + 2x^k\alpha^2 - (-x^{2k} + x - 1)\alpha - x^{k+1} = 0.$$

So the norm of α has to be $\mathrm{N}_{\overline{\mathbb{Q}}(C_k)/\overline{\mathbb{Q}}(x)}(\alpha) = -x^{k+1}$. This enables us to compute the norm of ε^{-1}.

$$\begin{aligned}\mathrm{N}_{\overline{\mathbb{Q}}(C_k)/\overline{\mathbb{Q}}(x)}(\varepsilon^{-1}) &= \frac{1}{\mathrm{N}_{\overline{\mathbb{Q}}(C_k)/\overline{\mathbb{Q}}(x)}(y)}\left(\frac{\mathrm{N}_{\overline{\mathbb{Q}}(C_k)/\overline{\mathbb{Q}}(x)}(y-x^k)}{\mathrm{N}_{\overline{\mathbb{Q}}(C_k)/\overline{\mathbb{Q}}(x)}(y)}\right)^k\\ &= -\frac{1}{x^k}\left(\frac{-x^{k+1}}{-x^k}\right)^k = -1\end{aligned}$$

□

In combination these two lemmas provide a proof of Proposition 3.59. Using the fact that there exists a non-trivial unit in $\mathcal{O}(C_k)$ and by counting the pole order at infinity of this unit, we get a torsion point on the jacobian of C_k.

Proposition 3.62. *The curve C_k defined by the polynomial*

$$F_k := Y^3 - X^k Y^2 - (X-1)Y - X^k$$

admits a $\mathbb{Q}$-rational torsion divisor of order dividing k^2.

Proof : We have already seen that there exists a non-trivial unit $\varepsilon \in \mathcal{O}(C_k)$. So the divisor $\operatorname{div}(\varepsilon)$ is only supported at infinity. But since we have exactly two $\mathbb{Q}$-rational divisors at infinity, we get $\operatorname{div}(\varepsilon) = m(P_\infty - D_\infty)$ for some $m \in \mathbb{Z}$. Therefore, the divisor $P_\infty - D_\infty$ is of finite order. Let us now compute the pole order of ε^{-1} at D_∞. First observe that x has a simple pole at D_∞ and y has no pole at D_∞. Therefore, we get for ε a k^2-fold pole at D_∞. This gives us that m has to be a divisor of k^2. □

In the number field analogon it is possible to show that the unit in the proposition above is actually a fundamental unit. But the proof of Kühner in [Küh95] uses the explicit computation of the Voronoi Algorithm (see for example [Buc85]). This algorithm makes essential use of the geometry of numbers established by Minkowski. Since in the function field case we do not have such a tool, it is much more difficult to formulate the analogous algorithm. For a special case of cubic function fields we refer to [SS00] where Scheidler and Stein describe the algorithm for purely cubic fields over finite fields. For cubic function fields over finite fields with a trace zero generator we refer to [Sch04]. We now show that in a general function field of degree three with unit rank equal to one it is also possible to use the Voronoi Algorithm to compute a fundamental unit. Afterwards we use the algorithm to prove that the order of the divisor in the proposition above is exactly k^2. The proofs in this section are following closely the ideas of [LSY03] and [SS00].

We give a description of the Voronoi Algorithm which works for base fields $K = \mathbb{F}_q$, with $\gcd(q, 6) = 1$, or $K = \mathbb{Q}$. The basic idea of this algorithm is to compute for a fractional ideal in $\mathcal{O}(C)$ a chain of *minima*. For this process we first need some definitions. We always assume that there exist exactly one embedding $K(C) \hookrightarrow K((X^{-1}))$.

Definition 3.5. *Let $\mathfrak{A} \subset K(C)$ be a fractional ideal. Then we call $\alpha \in \mathfrak{A}$ a* minimum *of $\mathfrak{A}$ if for all $\beta \in \mathfrak{A} \setminus \{0\}$ with $|\beta| \leq |\alpha|$ and $|\sigma(\beta)| \leq |\sigma(\alpha)|$, $\beta = \lambda\alpha$ for some $\lambda \in \mathbb{Q}^*$.*

Definition 3.6. *Let $\mathfrak{A}$ be a fractional ideal and $\theta \in \mathfrak{A}$ a minimum in $\mathfrak{A}$. Then $\phi \in \mathfrak{A}$ is called* minimum adjacent to θ in $\mathfrak{A}$ *if*

1. *ϕ is a minimum in $\mathfrak{A}$,*
2. *$|\theta| < |\phi|$,*
3. *for all $\alpha \in \mathfrak{A}$ with $|\theta| < |\alpha| < |\phi|$, $|\sigma(\alpha)| \geq |\sigma(\theta)|$.*

In the following we want to show that for a fractional ideal $\mathfrak{A}$ and a minimum $\theta \in \mathfrak{A}$ always a minimum adjacent to θ exists.

Definition 3.7. *Let $\alpha \in K(C)$ be a rational function on C. Set*

1. *$\zeta_\alpha := \sigma_1(\alpha) + \sigma_2(\alpha)$,*
2. *$\xi_\alpha := \frac{1}{3}(2\alpha - \zeta_\alpha)$,*
3. *$\eta_\alpha := \sigma_1(\alpha) - \sigma_2(\alpha)$,*

where σ_1, σ_2 are the two non-trivial automorphisms of $K(C)$.

Lemma 3.63. *Let $\mathfrak{A} = \langle 1, \mu, \nu \rangle$ be a fractional ideal. Then*

$$\Delta(\mathfrak{A}) = \frac{9}{4}(\xi_\mu \eta_\nu - \xi_\nu \eta_\mu)^2.$$

Proof : By definition we have

$$\begin{aligned}
(\xi_\mu \eta_\nu - \xi_\nu \eta_\mu)^2 =& \frac{1}{9}((2\mu - \sigma_1(\mu) - \sigma_2(\mu))(\sigma_1(\nu) - \sigma_2(\nu)) \\
& - (2\nu - \sigma_1(\nu) - \sigma_2(\nu))(\sigma_1(\mu) - \sigma_2(\mu))))^2 \\
=& \frac{4}{9}(\sigma_1(\mu)\sigma_2(\nu) + \sigma_2(\mu)\nu + \mu\sigma_1(\nu) \\
& - \sigma_1(\mu)\nu - \sigma_2(\mu)\sigma_1(\nu) - \mu\sigma_2(\nu))^2 \\
=& \frac{4}{9} \det \begin{pmatrix} 1 & 1 & 1 \\ \mu & \sigma_1(\mu) & \sigma_2(\mu) \\ \nu & \sigma_1(\nu) & \sigma_2(\nu) \end{pmatrix}^2 \\
=& \frac{4}{9}\Delta(\mathfrak{A}).
\end{aligned}$$

□

Lemma 3.64. *Let $\mathfrak{A} = \langle 1, \mu, \nu \rangle$ be a fractional ideal with*

$$|\xi_\mu| > |\xi_\nu|, |\eta_\mu| < 1 \leq |\eta_\nu| \text{ and } |\zeta_\mu|, |\zeta_\nu| < 1.$$

and 1 is a minimum in $\mathfrak{A}$. Then $|\Delta(\mathfrak{A})| > 1$.

Proof : Since by assumption $|\zeta_\mu|, |\eta_\mu| < 1$, we get $|\sigma(\mu)| < 1$ for a non-trivial automorphism σ. Since 1 is a minimum in $\mathfrak{A}$ and μ is not a unit in K, we get $|\mu| > 1$. So we have

$|\xi_\mu| = |\mu| > 1$. Now, if $|\xi_\mu\eta_\nu| = |\xi_\nu\eta_\mu|$, it is possible to exchange μ and ν by constant multiples such that $\operatorname{sgn}(\xi_\mu\eta_\nu) \neq \operatorname{sgn}(\xi_\nu\eta_\mu)$. So we can compute

$$|\Delta(\mathfrak{A})| = |(\xi_\mu\eta_\nu - \xi_\nu\eta_\mu)^2| = \max\{|\xi_\mu\eta_\nu|, |\xi_\nu\eta_\mu|\}^2 \geq |\xi_\mu\eta_\nu|^2 > 1 \qquad \square$$

The next lemma we do not prove and refer instead to the algorithm given in [SS00, Algorithm 4.1] for the purely cubic case over finite fields which transfers completely to our case.

Lemma 3.65. *Let $\mathfrak{A}$ be a fractional ideal such that 1 is a minimum in $\mathfrak{A}$. Then there exists $\mu, \nu \in \mathfrak{A}$ such that $\mathfrak{A} = \langle 1, \mu, \nu\rangle$ and*

$$|\xi_\mu| > |\xi_\nu|, |\eta_\mu| < 1 \leq |\eta_\nu| \text{ and } |\zeta_\mu|, |\zeta_\nu| < 1.$$

The form of a basis mentioned in the lemma above makes it quite easy to compute the minimum adjacent to 1 in a fractional ideal. The next lemma clarifies why we only need to consider minima adjacents to 1 in fractional ideals.

Lemma 3.66. *Let $\mathfrak{A}$ be a fractional ideal such that 1 and θ are minima in $\mathfrak{A}$. Then 1 is a minimum in $\left(\frac{1}{\theta}\right)\mathfrak{A}$ and if $\widetilde{\theta}$ is a minimum adjacent to 1 in $\left(\frac{1}{\theta}\right)\mathfrak{A}$, then $\widetilde{\theta}\theta$ is a minimum adjacent to θ in $\mathfrak{A}$.*

The proof of this lemma is straightforward. Now we compute the minimum adjacent to 1 in a fractional ideal with such a reduced basis as above.

Proposition 3.67. *Let $\mathfrak{A} = \langle 1, \mu, \nu\rangle$ be a fractional ideal with*

$$|\xi_\mu| > |\xi_\nu|, |\eta_\mu| < 1 \leq |\eta_\nu| \text{ and } |\zeta_\mu|, |\zeta_\nu| < 1$$

and 1 is a minimum in $\mathfrak{A}$. Then μ is a minimum adjacent to 1 in $\mathfrak{A}$.

Proof : First we show that μ is a minimum in $\mathfrak{A}$. For this, we assume there exists $\beta = a + b\mu + c\nu \in \mathfrak{A}$ such that

$$|\beta| \leq |\mu| \text{ and } |\sigma(\beta)| \leq |\sigma(\mu)|.$$

In order to show that $c = 0$ has to hold we assume $c \neq 0$. Then by choice of the basis we have $|c\eta_\nu| \geq 1$. If we assume $|b\eta_\mu| \neq |c\eta_\nu|$, then we can compute

$$1 \leq |c\eta_\nu| \leq \max\{|b\eta_\mu|, |c\eta_\nu|\} = |b\eta_\mu| + |c\eta_\nu| = |\eta_\beta| \leq |\sigma(\beta)| \leq |\sigma(\mu)| < 1.$$

This gives us a contradiction. So, $|b\eta_\mu| = |c\eta_\nu|$. Therefore, we have

$$|b| > |b\eta_\mu| = |c\eta_\nu| > |c|.$$

Combining these estimates, we get

$$|\beta| = |\xi_\beta| = |b\xi_\mu + c\xi_\nu| = |b\xi_\mu| \geq |\xi_\mu| = |\mu| \geq |\beta|,$$

which implies that the only inequality has to be an equality, therefore, $|b\xi_\mu| = |\xi_\mu|$. But this implies $|b| = 1$. Therefore, $1 \leq |c| < 1$, which is a contradiction. Therefore, our assumption was false and $c = 0$. If $c = 0$, the last computation still holds true and $b \in K^*$. So we can write $\beta = b\left(\frac{a}{b} + \mu\right)$. This yields

$$|a| = |\sigma(\beta) - \sigma(\mu)| \leq \max\{|\sigma(\beta)|, |\sigma(\mu)|\} < 1$$

and since a has to be a polynomial, we have $a = 0$. But this means μ is a minimum in $\mathfrak{A}$. By choice of the basis we have $1 < |\mu|$ and the last axiom of the definition of a minimum adjacent follows from the same argumentation as the fact that μ is a minimum in $\mathfrak{A}$. This gives us that μ is a minimum adjacent to 1 in $\mathfrak{A}$. □

Definition 3.8 (Voronoi Algorithm)**.** *Set* $\mathfrak{A}_0 := \mathcal{O}(C)$ *and* $\mathfrak{A}_{k+1} := \left(\frac{1}{\mu_k}\right)\mathfrak{A}_k$*, where* $\mathfrak{A}_k = \langle 1, \mu_k, \nu_k\rangle$ *and*

$$|\xi_{\mu_k}| > |\xi_{\nu_k}|, |\eta_{\mu_k}| < 1 \leq |\eta_{\nu_k}| \text{ and } |\zeta_{\mu_k}|, |\zeta_{\nu_k}| < 1,$$

for $k > 0$*. Define the sequence* $(\theta_k)_{k\geq 0}$ *by* $\theta_k := \prod_{i=0}^{k-1} \mu_i$ *to be the* Voronoi Algorithm *in* $\mathcal{O}(C)$*.*

Theorem 3.68. *Assume the unit rank in* $K(C)$ *is equal to one. Then the* Voronoi *Algorithm computes a fundamental unit* ε *in* $\mathcal{O}(C)$*.*

Proof : First observe that 1 is a minimum in $\mathcal{O}(C)$. Therefore, every unit is a minimum in $\mathcal{O}_C$. If we now consider the sequence $(|\theta_k|)_{k\geq 0}$, we see that this is a strictly increasing sequence. Assume now θ is a minimum with non-negative degree in $\mathcal{O}(C)$. Then there has to exist an index i such that $|\theta_i| \leq |\theta| < |\theta_{i+1}|$. Now we can assume $|\sigma(\theta_i)| > |\sigma(\theta)|$ by the properties of a minimum since otherwise we directly get that θ is a constant multiple of θ_i. But since θ_{i+1} is a minimum adjacent to θ_i, this implies by the properties of a minimum adjacent that θ has to be a constant multiple of θ_i. Therefore, in the Voronoi Algorithm every non-negative minimum of $\mathcal{O}(C)$ must occur. But if there exists a non-trivial unit ε in $\mathcal{O}(C)$, then either ε or ε^{-1} must occur in the Voronoi Algorithm. So the first unit in the sequence is a fundamental unit. □

Remark. *The condition on the unit rank in Theorem 3.68 is fulfilled if and only if the divisor* $2P_\infty - D_\infty$ *is of finite order in* $\mathrm{Jac}(C)(K)$.

So we can now compute the VORONOI Algorithm for $\mathcal{O}(C_k)$ with

$$C_k : Y^3 - X^k Y^2 - (X-1)Y - X^k.$$

This gives us for $0 \leq s \leq k-1$

$$\begin{aligned}
\theta_0 &= 1 \\
\theta_{3s+1} &= y\left(\frac{y}{y-x^k}\right)^s \\
\theta_{3s+2} &= y^2\left(\frac{y}{y-x^k}\right)^s \\
\theta_{3s+3} &= \left(\frac{xy}{y-x^k}\right)^s \\
\theta_{3k+1} &= y\left(\frac{y}{y-x^k}\right)^k
\end{aligned}$$

and by computing norms we get θ_{3k+1} is the first unit in the sequence. Therefore, it has to be a fundamental unit. This gives us the following theorem. For the computation of the VORONOI Algorithm see [Küh95] or [Ada95].

Theorem 3.69. *The curve* C_k *defined by the polynomial*

$$F_k := Y^3 - X^k Y^2 - (X-1)Y - X^k$$

admits a $\mathbb{Q}$*-rational torsion divisor of exact order* k^2.

In the same manner it is possible to validate the following example. The number field case can be found in [Ada95].

Example 3.11. *The curve*

$$C_k : Y^3 - (X^k + X - 1)Y^2 - (X^k - 1)Y - X^k$$

admits a divisor of order k^2. *The fundamental unit in* $\mathcal{O}(C_k)$ *is given by*

$$\varepsilon = y\left(\frac{y^2}{y-x^k}\right)^k.$$

With these applications of the VORONOI Algorithm which result in new series of curves with a point of large order on the jacobian, we conclude the construction of curves with a point of prescribed order in the jacobian.

4. Torsion in a Certain Family of Hyperelliptic Curves

4.1. Two-Torsion in a Subfamily of a one-dimensional Family

In this section we want to compute in some family of hyperelliptic curves of genus two the two-torsion subgroup of its jacobian.

We consider the family of hyperelliptic curves given by the affine model

$$C_{\lambda^2} : Y^2 = X^5 - 5X^3 + 5X + \lambda^2 =: F_{\lambda^2}.$$

This is a one-dimensional family of hyperelliptic curves with a jacobian admitting RM by $\mathbb{Q}(\sqrt{5})$ (see Section 2.17). Since all curves in this family are given by a polynomial of degree five, they have a $\mathbb{Q}$-rational WEIERSTRASS-point at infinity. Since the two-torsion points on a jacobian are given by unordered pairs of WEIERSTRASS-points a jacobian of a curve in this family has a $\mathbb{Q}$-rational has a rational two-torsion point if and only if one more WEIERSTRASS-point is defined over $\mathbb{Q}$ or a pair of conjugate WEIERSTRASS-points over a quadratic extension of $\mathbb{Q}$. So determining the two-torsion points on a jacobian is the same as finding a linear or quadratic factor of the polynomial F_{λ^2}.

Let us consider first the case of a linear factor. If we assume x_0 is a root of F_{λ^2}, we get $0 = x_0^5 - 5x_0^3 + 5x_0 + \lambda^2$ and therefore the search for a linear factor of F_{λ^2} is equivalent to the search of $\mathbb{Q}$-rational points on the hyperelliptic curve

$$C : Y^2 = -X^5 + 5X^3 - 5X$$

of genus two.

If we do not require the parameter λ of the family to be a square, this hyperelliptic curve has to be replaced by a curve of genus zero with infinitely many $\mathbb{Q}$-rational points.

In Section 1.4.7 we describe a method to find all rational points on a hyperelliptic curve. For this method we need that the rank of the jacobian of the curve is less or equal to one. We now show that $\mathrm{rank}(\mathrm{Jac}(C)(\mathbb{Q}))$ actually is equal to one. First of all we see

that

$$\mathrm{Jac}(C)_{tors}(\mathbb{Q}) \cong {}^{\mathbb{Z}}\!/_{2\mathbb{Z}},$$

by reducing the curve modulo the primes $p_1 := 3$ and $p_2 := 7$. These are primes of good reduction since they do not divide the discriminant $\Delta(C) = 50000$ of C. In the jacobians of the reduced curves we have the following numbers of points

$$\#\,\mathrm{Jac}(\overline{C})(\mathbb{F}_{p_1}) = 14 \text{ and } \#\,\mathrm{Jac}(\overline{C})(\mathbb{F}_{p_1}) = 46.$$

We conclude that the $\mathbb{Q}$-rational torsion subgroup has to be either trivial or isomorphic to ${}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$. But since we have two $\mathbb{Q}$-rational Weierstrass points on C the torsion subgroup can not be trivial. We now use this fact to show that there is a point of infinite order on $\mathrm{Jac}(C)$. Consider the affine point $P := (-1, 1) \in C(\mathbb{Q})$. Then its image on $\mathrm{Jac}(C)$ under Φ_{P_∞} is given in Mumford representation by $D := (x + 1, 1)$ (see Definition 1.41). Using Cantor's Algorithm 1 we can compute

$$2(P - P_\infty) = \left(x^2 + 2x + 1, \frac{5}{2}x + \frac{7}{2}\right).$$

This is obviously non-zero in $\mathrm{Jac}(C)$ and since $\#\,\mathrm{Jac}(C)_{tors}(\mathbb{Q}) = 2$ the point $(P - P_\infty)$ has to be of infinite order. This yields $\mathrm{rank}(\mathrm{Jac}(C)(\mathbb{Q})) \geq 1$. To prove that the rank is bounded from above by one, we perform a two-descent on $\mathrm{Jac}(C)(\mathbb{Q})$. For details of two-descent on jacobians of hyperelliptic curves we refer to [Sto01]. We consider the exact sequence

$$0 \to {}^{\mathrm{Jac}(C)(\mathbb{Q})}\!/_{\mathrm{Jac}(C)[2](\mathbb{Q})} \to \mathrm{Sel}_2(\mathbb{Q}, \mathrm{Jac}(C)) \to Ш_2(\mathbb{Q}, \mathrm{Jac}(C)) \to 0,$$

where $\mathrm{Sel}_2(\mathrm{Jac}(C))$ is the *Two-Selmer Group* and $Ш_2(\mathrm{Jac}(C))$ is the two-part of the Tate-Shafarevich *Group*.

So we get by computing $\mathrm{Sel}_2(\mathrm{Jac}(C))$ an upper bound on the rank of the jacobian of C by the formula

$$\begin{aligned}\mathrm{rank}(\mathrm{Jac}(C)(\mathbb{Q})) &\leq \dim_{\mathbb{F}_2} \mathrm{Sel}_2(\mathbb{Q}, \mathrm{Jac}(C)) - \dim_{\mathbb{F}_2} \mathrm{Jac}(C)[2] \\ &= \dim_{\mathbb{F}_2} \mathrm{Sel}_2(\mathbb{Q}, \mathrm{Jac}(C)) - 1.\end{aligned}$$

To compute $\mathrm{Sel}_2(\mathbb{Q}, \mathrm{Jac}(C))$, we first need to factor the polynomial

$$F := -X^5 + 5X^3 - 5X = -X(X^4 - 5X^2 + 5),$$

where the degree four factor is irreducible. This gives us

$$L := \mathbb{Q}[X]/(-X^5+5X^3-5X) \cong \mathbb{Q}[X]/(X) \times \mathbb{Q}[X]/(X^4-5X^2+5) =: L_1 \times L_2.$$

Let θ denote the image of X in L.

By [Sto01, Corollary 4.7] we have to find the primes p such that $p^2|\Delta(C)$. Since $\Delta(C) = 50000$, the only primes are $p_1 = 2$ and $p_2 = 5$. Then set $S := \{\infty, 2, 5\}$ and compute for any $p \in S$ the factorization of $-X^5+5X^3-5X$ over $\mathbb{Q}_p$.

$$\begin{aligned}\mathbb{R} : -X^5+5X^3-5X =& X\left(X-\sqrt{\frac{5+\sqrt{5}}{2}}\right)\left(X+\sqrt{\frac{5+\sqrt{5}}{2}}\right)\\ &\cdot\left(X-\sqrt{\frac{5-\sqrt{5}}{2}}\right)\left(X+\sqrt{\frac{5-\sqrt{5}}{2}}\right).\end{aligned}$$

For $p = 5$ we get that $-X^4+5X^2-5$ is irreducible over $\mathbb{Q}_5$ by Eisenstein. For $p = 2$ we get the same factorization as over $\mathbb{Q}$ since the degree four factor is irreducible over $\mathbb{F}_2$.

For $p \in S$ we set

$$L_p := \mathbb{Q}_p/(F) = \mathbb{Q}_p(\theta_p).$$

Then we get for each p a homomorphism

$$\delta_p : \mathrm{Jac}(C)(\mathbb{Q}_p) \to L_p^*/(L_p^*)^2$$

given by $\sum_P n_P P \mapsto \prod_P (x(P)-\theta_p)^{n_P}$. These homomorphisms have $\mathrm{Jac}(C)(\mathbb{Q}_p)[2]$ as kernel by [Sto01]. For each $p \in S$ we now compute

$$J_p := \delta_p(\mathrm{Jac}(C)(\mathbb{Q}_p)).$$

We start with $p = \infty$. The defining polynomial F has five real roots and by [Sto01, Lemma 4.8], J_∞ is generated by $\delta_\infty(P - P_\infty)$ for $P \in C(\mathbb{R})$. Furthermore, by the same lemma we have $\dim_{\mathbb{F}_2}(J_\infty) = 2$. Then we find a basis by $(0,1,1,0,0)$ and $(0,0,0,1,1)$. Using the algorithm of [Sto01, Section 6], we compute a basis for J_p for $p = 2, 5$. By [Sto01, Lemma 4.4], we get $\dim_{\mathbb{F}_2}(J_2) = 3$ and $\dim_{\mathbb{F}_2}(J_5) = 1$. So for $p = 5$ it is enough to compute the image of $(0,0) \in C(\mathbb{Q}_5)$ to obtain a basis for J_5. For $p = 2$ we find three points on $C(\mathbb{Q}_2)$ given by $P_1 = (0,0), P_2 = \left(-\frac{1}{4}, \sqrt{F(-\frac{1}{4})}\right)$ and $P_3 := (-1, \sqrt{F(-1)})$. It is easy to show that the images of these points are linear independent. Now we are left with finding a basis for a subgroup H of $L^*/(L^*)^2$ which contains the group $\mathrm{Sel}_2(\mathbb{Q}, \mathrm{Jac}(C))$. This task is performed by using [Sto01, Lemma 4.9], which relates H

to the class group of L. Putting these information together we obtain

$$\begin{aligned}\dim_{\mathbb{F}_2} \mathrm{Sel}_2(\mathbb{Q}, \mathrm{Jac}(C)) = &\dim_{\mathbb{F}_2} H + \dim_{\mathbb{F}_2}(J_2 \oplus J_5 \oplus J_\infty) \\ &- \dim_{\mathbb{F}_2}(\mathrm{res}(H) + (J_2 \oplus J_5 \oplus J_\infty)) = 2,\end{aligned}$$

where

$$\mathrm{res} : {L^*}/{(L^*)^2} \to {L_2^*}/{(L_2^*)^2} \oplus {L_5^*}/{(L_5^*)^2} \oplus {L_\infty^*}/{(L_\infty^*)^2}.$$

Since $\dim_{\mathbb{F}_p} \mathrm{Jac}(C)[2](\mathbb{Q}) = 1$, we have

$$\mathrm{rank}(\mathrm{Jac}(C)(\mathbb{Q})) \leq 1.$$

The computations can be checked by MAGMA with the following code.

```
R<x> := PolynomialRing(Rationals());
C := HyperellipticCurve(-x^5 + 5*x^3 - 5*x);
J := Jacobian(C);
SetVerbose("Selmer", 3);
TwoSelmerGroup(J);
```

By the considerations above it is easy to verify the correctness of the output. For a hyperelliptic curve of genus two with a rank one jacobian the CHABAUTY Method (see Section 1.4.7) works to determine the full set of $\mathbb{Q}$-rational points on C. But we need to find a generator of

$${\mathrm{Jac}(C)}/{\mathrm{Jac}(C)_{tors}}.$$

Since we already know the point D of infinite order, we check whether there exists a point $Q \in \mathrm{Jac}(C)$ and an integer $N \in \mathbb{Z}$ such that $N \cdot Q = D$. This is done by computing the canonical height of D. For this we use the formulae of Lemma 1.15 in order to get a point in projective space. For this point we can compute the canonical height by Definition 1.47.

$$\hat{h}(D) \approx 0.940427942028833295425884666867$$

Assume there exists a point $Q \in \mathrm{Jac}(C)(\mathbb{Q})$ and an integer N such that $D = NQ$ then we get by Theorem 1.27

$$\hat{h}(D) = N^2 \hat{h}(Q).$$

Therefore there has to exist a point in $\mathrm{Jac}(C)(\mathbb{Q}) \setminus \mathrm{Jac}(C)_{tors}$ with height less than the computed height of the point D. A complete search shows that such a point can not exist.

The next step is to find all rational points on the curve C.

Lemma 4.1. *The $\mathbb{Q}$-rational points on the affine part of C are given by the set*

$$\{(0,0),(-1,1),(-1,-1)\}.$$

Proof : First we observe that $\{(0,0),(-1,1),(-1,-1)\} \subset C(\mathbb{Q})$ by checking that these points fulfill the affine equation of the curve. Since by the discussion above the rank of $\mathrm{Jac}(C)(\mathbb{Q})$ is one, we can apply Theorem 1.23 with the prime $p = 7$, the smallest prime of good reduction greater than four, and conclude by counting points on $\overline{C}(\mathbb{F}_p) = 8$ that $\#C(\mathbb{Q}) \leq 10$. This means we have to use more local information to obtain the result. For this we follow [BS10] and consider the curve modulo different primes. The curve C has at $p = 13$ good reduction and we easily find $\#C(\mathbb{F}_p) = 14$. It is possible to find a differential ω_p on $\mathrm{Jac}(C)(\mathbb{Q}_{13})$ annihilating $\mathrm{Jac}(C)(\mathbb{Q})$ which does not vanish on $C(\mathbb{F}_{13})$. This implies that there exists for any $\overline{P} \in C(\mathbb{F}_{13})$ there exists at most one point $P \in C(\mathbb{Q})$ that reduces to $\overline{P}$. Let N be a multiple of $\mathrm{Jac}(C)(\mathbb{F}_p)$, then we have an injection $C(\mathbb{Q}) \hookrightarrow {}^{\mathrm{Jac}(C)(\mathbb{Q})}\!/_{N\,\mathrm{Jac}(C)(\mathbb{Q})}$. Therefore, the preimages of the points on $C(\mathbb{F}_p)$ are exactly the rational points of $C(\mathbb{Q})$. This completes the proof. □

The statement of this lemma means that there exists a root of the polynomial F_{λ^2} only for the parameters $\lambda = 0$, $\lambda = -1$.

Since a quadratic factor of F_{λ^2} gives rise to a pair of conjugated Weierstrass points we check the possible quadratic factors of F_{λ^2} depending on the parameter λ. So we assume

$$F_{\lambda^2} = (x^2 + ax + b)(x^3 + cx^2 + dx + e) \text{ with } a, b, c, d, e \in \mathbb{Q}.$$

By comparing coefficients, we get

$$\begin{aligned} a + c &= 0, \\ b + d + ac &= -5, \\ ad + e + bc &= 0, \\ ae + bd &= 5, \\ be &= \lambda^2. \end{aligned}$$

We now take the first four equations to define an algebraic set V in $\mathbb{A}^5$. By the following isomorphism we make V into an plane algebraic curve defined over $\mathbb{Q}$.

$$\begin{aligned} &c \mapsto X, && d \mapsto Y, && e \mapsto XY - (X^2 - Y - 5)X, \\ &b \mapsto X^2 - Y - 5, && a \mapsto -X. \end{aligned}$$

The plane curve $\widetilde{V}$ is given by

$$\widetilde{V} = \mathcal{V}(X^4 - X^2Y - 5X^2 - Y^2 - 5Y - 5) \subset \mathbb{A}^2.$$

By the RIEMANN-HURWITZ Genus Formula, the genus of $\widetilde{V}$ is zero. It has singularities at $P_1 := (1, -3)$ and $P_2 := (-1, -3)$. These are the only $\mathbb{Q}$-rational points of $\widetilde{V}$.

Now we are able to compute the e and b coordinate of the pre-images of these $\mathbb{Q}$-rational points and ϕ and then compute the images of this points under the morphism $V \to \mathbb{P}^1$ which maps be to λ^2. A short computation shows $b(\phi^{-1}(P_1)) = b(\phi^{-1}(P_2)) = -1$ and $e(\phi^{-1}(P_1)) = -e(\phi^{-1}(P_2)) = 2$. Therefore, for no $\lambda \in \mathbb{Q}$ there exists a quadratic factor of F_{λ^2}. Summing up the discussion above, we get the following theorem.

Theorem 4.2. $\mathrm{Jac}(C_{\lambda^2})(\mathbb{Q})[2]$ *is non-trivial if and only if* $\lambda^2 = 0$ *or* $\lambda^2 = 1$. *In this cases*

$$\mathrm{Jac}\left(C_{\lambda^2}\right)[2](\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}.$$

We see in this section that already for a fairly simple one-dimensional family of hyperelliptic curves the determination of the curves with a two-torsion point on their jacobian needs a huge machinery of theory. In the next section we search this family for elements with a three-torsion point on the jacobian. We will see that already in this case a complete determination of the parameters with the desired properties is no longer possible.

4.2. Three-Torsion in a one-dimensional Family

We now want to determine the curves in the family which admit a $\mathbb{Q}$-rational point of order three. First we observe that a three-torsion point on the image of the curve is not possible since this would mean that we have a decomposition of F_λ into a square and a cube of a linear polynomial. That is,

$$F_\lambda = g^2 + \varepsilon(X - a)^3$$

for some $a \in \mathbb{Q}$, $\varepsilon \in \mathbb{Q}^*$ and $g \in \mathbb{Q}[X]$. But since $\deg(F_\lambda) = 5$, such a decomposition is impossible.

So we can assume that a three-torsion point is given by a quadratic polynomial as its u-coordinate.

Theorem 4.3. *There exist only finitely many* $\lambda \in \mathbb{Q}$ *such that the jacobian of the hyperelliptic curve*

$$C_\lambda : Y^2 = X^5 - 5X^3 + 5X + \lambda$$

admits a point of order three.

Proof : Assume $\lambda \in \mathbb{Q}$ such that D with u-coordinate x^2+ax+b is of order three on $\mathrm{Jac}(C_\lambda)(\mathbb{Q})$. Then there exists a function $\tilde{g} \in \mathcal{L}(6P_\infty)$ which has a triple zero at $\mathrm{supp}(D)$. That is, there exists a polynomial $g \in \mathbb{Q}[X]$ with $\deg(g)=3$ such that $\tilde{g}=g(x)+y$ and $g^2-F_\lambda = \varepsilon(x^2+ax+b)^3$. If we set $g := \sum_{i=0}^3 g_i x^i$, we get $\varepsilon = g_3^2$ since $\deg(F_\lambda)=5$ and $g_3 \neq 0$. Solving the relation $g^2-F_\lambda = g_3^2(x^2+ax+b)^3$, we obtain

$$
\begin{aligned}
a =& \frac{2g_2g_3-1}{3g_3^2},\\
b =& \frac{2g_1g_3^3-\frac{1}{3}g_2^2g_3^2+\frac{4}{3}g_2g_3-\frac{1}{3}}{3g_3^4},\\
\lambda =& \frac{g_0^2g_3^{10}-\frac{8}{27}g_1^3g_3^9+\frac{4}{27}g_1^2g_2^2g_3^8-\frac{16}{27}g_1^2g_2g_3^7+\frac{4}{27}g_1^2g_3^6-\frac{2}{81}g_1g_2^4g_3^7}{g_3^{10}}\\
&+\frac{\frac{16}{81}g_1g_2^3g_3^6-\frac{4}{9}g_1g_2^2g_3^5+\frac{16}{81}g_1g_2g_3^4-\frac{2}{81}g_1g_3^3+\frac{1}{729}g_2^6g_3^6-\frac{4}{243}g_2^5g_3^5}{g_3^{10}}\\
&+\frac{\frac{17}{243}g_2^4g_3^4-\frac{88}{729}g_2^3g_3^3+\frac{17}{243}g_2^2g_3^2-\frac{4}{243}g_2g_3+\frac{1}{729}}{g_3^{10}},\\
0 =& 2g_0g_3^5-\frac{2}{3}g_1g_2g_3^4+\frac{4}{3}g_1g_3^3+\frac{4}{27}g_2^3g_3^3-\frac{14}{9}g_2^2g_3^2+\frac{10}{9}g_2g_3+5g_3^4-\frac{5}{27},\\
0 =& 2g_0g_2g_3^4-\frac{1}{3}g_1^2g_3^4-\frac{4}{9}g_1g_2^2g_3^3-\frac{8}{9}g_1g_2g_3^2+\frac{2}{9}g_1g_3+\frac{1}{9}g_2^4g_3^2-\frac{4}{9}g_2^3g_3+\frac{1}{9}g_2^2,\\
0 =& 2g_0g_1g_3^8-\frac{8}{9}g_1^2g_2g_3^7+\frac{4}{9}g_1^2g_3^6+\frac{8}{27}g_1g_2^3g_3^6-\frac{4}{3}g_1g_2^2g_3^5+\frac{8}{9}g_1g_2g_3^4-\frac{4}{27}g_1g_3^3\\
&-\frac{2}{81}g_2^5g_3^5+\frac{17}{81}g_2^4g_3^4-\frac{44}{81}g_2^3g_3^3+\frac{34}{81}g_2^2g_3^2-\frac{10}{81}g_2g_3-5g_3^8+\frac{1}{81}.
\end{aligned}
$$

The first relation in the g_i gives us

$$
g_0 = \frac{-\frac{2}{3}g_1g_2g_3^4+\frac{4}{3}g_1g_3^3+\frac{4}{27}g_2^3g_3^3-\frac{14}{9}g_2^2g_3^2+\frac{10}{9}g_2g_3+5g_3^4-\frac{5}{27}}{2g_3^5},
$$

since g_3 is non-zero by assumption. We now show that the curve X defined by

$$
\begin{aligned}
0 =& -\frac{1}{3}g_1^2g_3^5-\frac{10}{9}g_1g_2^2g_3^4+\frac{4}{9}g_1g_2g_3^3+\frac{2}{9}g_1g_3^2+\frac{7}{27}g_2^4g_3^3-2g_2^3g_3^2\\
&+\frac{11}{9}g_2^2g_3+5g_2g_3^4-\frac{5}{27}g_2,\\
0 =& -14g_1^2g_2g_3^7+16g_1^2g_3^6+4g_1g_2^3g_3^6-26g_1g_2^2g_3^5+18g_1g_2g_3^4+45g_1g_3^7-3g_1g_3^3\\
&-\frac{2}{9}g_2^5g_3^5+\frac{17}{9}g_2^4g_3^4-\frac{44}{9}g_2^3g_3^3+\frac{34}{9}g_2^2g_3^2-\frac{10}{9}g_2g_3-45g_3^8+\frac{1}{9}
\end{aligned}
$$

has genus greater than one. Since by a theorem of Faltings [Fal83] a curve of genus larger than one can only have finitely many rational points, this completes the proof of

the theorem.

The curve X is the complete intersection of a smooth degree seven and a smooth degree ten surface in $\mathbb{P}^3$. Therefore, its genus is equal to

$$g(X) = \frac{1}{2} \cdot 7 \cdot 10(7 + 10 - 4) + 1 > 1$$

by [Har77, Chapter I, Exercise 7.2 (d)]. □

In a point search in MAGMA up to height 10^9, no $\mathbb{Q}$-rational points were found. Motivated by this remark and by the Example 3.1 we conjecture that for all curves in the family

$$C_\lambda : Y^2 = X^5 - 5X^3 + 5X + \lambda$$

there is no $\mathbb{Q}$-rational point of order three in the jacobian.

4.3. Five-Torsion in a one-dimensional Family

Since already for three-torsion we are not able to give a complete answer, we restrict ourselves in the five-torsion case to curves with a five-torsion point on the image of the curve on its jacobian. The main difficulty in finding parameters which yield a curve with the desired properties is the determination of rational points on certain varieties. This is assumed to be a very difficult task in general.

Theorem 4.4. *For all jacobians of the hyperelliptic curves*

$$C_\lambda : Y^2 = X^5 - 5X^3 + 5X + \lambda, \lambda \in \mathbb{Q}$$

there exists no $\mathbb{Q}$-rational five-torsion on the image of the curve under Φ_{P_∞}.

Proof : Assume $P := (x(P), y(P))$ is a point on the curve C_λ such that the divisor $D := P - P_\infty$ is of order five. This holds if and only if there exists a function $f \in \mathcal{L}(5P_\infty)$ which has only at P a root of multiplicity five. Since f has to be of the form $f = a(x) + y$ for some polynomial $a \in \mathbb{Q}[X]$ with $\deg(a) \leq 2$, this holds if and only if

$$a^2 - F_\lambda = \varepsilon(X - x(P))^5$$

for some $x(P) \in \mathbb{Q}$ and $\varepsilon \in \mathbb{Q}^*$. Since the degree of a^2 is less or equal to four and $\deg(F_\lambda) = \deg\left((X - x(P))^5\right) = 5$, we get $\varepsilon = -1$. By letting $a = a_0 + a_1X + a_2X^2$ and comparing coefficients in the equation over $\mathbb{Q}$, one gets that

$$F_\lambda = X^5 - 5X^3 + 5X + a_0^2 - \frac{1}{3125}a_2^{10}$$

and

$$\begin{aligned} 2a_1a_2 + \frac{2}{5}a_2^4 + 5 &= 0 \\ 2a_0a_2 + a_1^2 - \frac{2}{25}a_2^6 &= 0 \\ 2a_0a_1 + \frac{1}{125}a_2^8 - 5 &= 0. \end{aligned}$$

The three equations in a_0, a_1 and a_2 define a zero-dimensional algebraic set with no $\mathbb{Q}$-rational points. This completes the proof $\square$

In these three sections we determined the conditions on the parameter $\lambda \in \mathbb{Q}$ under which the jacobian of the hyperelliptic curve $C_\lambda : Y^2 = X^5 - 5X^3 + 5X + \lambda$ has a rational point of small order.

5. Summary and Outlook

In this thesis we look at jacobians of curves defined over number fields and considered their torsion subgroup. While for genus one curves, that is elliptic curves, the situation is settled over $\mathbb{Q}$ and small degree number fields, for curves of higher genus little is known. First we consider hyperelliptic curves and construct explicit examples with torsion divisors of large order.

For this goal, we look at the methods used for example by Flynn, Leprévost and Elkies. Using these approaches and variations or combinations of them, we are able to reconstruct known examples for hyperelliptic curves with a divisor of prescribed order. Furthermore, we find new examples with large torsion. The methods are based on different techniques which we describe in detail in this thesis. The most important approaches are the use of certain relations between different divisors and an application of Hensel's Lemma. For the use of relations between divisors we try to construct a curve such that two or three imposed relations hold. These relations are chosen in such a manner that they imply the existence of a torsion divisor of large order. Using this technique, we are able to construct a new example of a hyperelliptic curve of genus two with a 39-torsion point on its jacobian. The idea behind the use of Hensel's Lemma is to find a solution to certain norm equations in the coordinate ring of the curve. A solution to this norm equation gives us a rational function on the curve with poles only at infinity and a N-fold zero at exactly one point. This again guarantees that this divisor is of finite order dividing N. Usually we use for this approach a prime number N to ensure the order to be exactly N. Using both of these constructions, we are not only able to find single examples but even to construct whole infinite families either with constant genus or increasing genus. Furthermore, we find small degree number fields such that there exist curves defined over these number fields admitting a torsion point of prime order p, where p is a prime for which no example of a curve defined over $\mathbb{Q}$ is known by now. The largest prime number p, such that there is a hyperelliptic curve of genus two with a $\mathbb{Q}$-rational torsion divisor of order p is known, is $p = 29$.

We expect that for any prime number $p > 7$ we can construct a hyperelliptic curve of genus $\frac{p-7}{2}$ with a $\mathbb{Q}$-rational torsion point of order p on its jacobian using this method.

After considering hyperelliptic curves, we turn to a broader class of curves namely superelliptic curves. We are able to construct a series of superelliptic curves with

genus going to infinity having a torsion divisor linear in the genus. This series is the characteristic zero analogon to a family of curves over finite fields given by SCHEIDLER. Furthermore, it is possible to use HENSEL's Lemma to construct curves with a $\mathbb{Q}$-rational torsion divisor in this case, too.

For hyperelliptic and superelliptic curves, we see that there is a close relation between the computation of a non-trivial unit in the coordinate ring of a curve and the order of a divisor supported only at infinity. For hyperelliptic curves such a unit can be computed by using continued fractions. For function fields which are degree three extensions of the rational function field, we are able to show a connection between the periodicity of the VORONOI algorithm and the order of a certain divisor. For this we need to assume a certain splitting behavior of the place at infinity namely to a rational place of degree one and a rational place of degree two. Using this approach, we are able to give a series of curves with a divisor of order quadratic in the genus.

In the last section we consider a special family of hyperelliptic curves and determine the specializations such that there exists point of given order on the specialization.

FURTHER WORK: Since in this area of research still not much is known, there are a lot of questions yet to be answered. We have already seen in the introduction that there are a lot of open problems concerning the torsion subgroup of an abelian variety defined over a number field.

Problem. *Given a positive integers N, g and a field K, is it possible to find an abelian variety $A_{/K}$ of dimension g such that*

$$N | \# A_{tors}(K)?$$

In this thesis we construct curves of various genus with a rational point of prescribed order on the jacobian. Even in the dimension two case, it remains unclear whether a curve with a rational torsion point of order N for any possible N is known. Furthermore, we just consider the case where we have one torsion point on the jacobian. It remains an open question whether we are able to construct a curve with a rational point P of order N and a rational point Q of order N' on the jacobian. Another open question about this problem is whether it is possible to construct a three-dimensional family of curves with a rational point of order N on the jacobian. This would be a rather large step towards a better understanding of the moduli space of these objects. Historically this would follow the path which is taken in the dimension one case. The examples found for genus two curves induce the expectation that the largest prime order p of a rational point on the jacobian could be $p = 29$. Furthermore, it seems like the points of large order all lie on

the image of the curve under some embedding into the jacobian. It would be interesting to know whether this observation is at random or whether there is some reason behind it. For higher genus curves there are still only a few examples known for large torsion orders. We have tried to adapt the techniques of genus two curves to genus three curves, but we were not able to find any example for a large torsion point. A fruitful area of research is the development of techniques that apply for genus larger than two. Some of these questions perhaps can be tackled by similar techniques as presented in this thesis. These presented questions about the explicit construction of torsion points on jacobians of curves are a good starting point for further research.

The next two open problems seem a lot harder than the first one.

Problem. *Let $A_{/K}$ be an abelian variety of dimension g and $P \in A_{tors}(K)$. Does there exist a number $N_0(K, g)$ such that*

$$\mathrm{ord}(P) \leq N_0(K, g)?$$

This problem, known as the Boundedness Conjecture, and its uniform version are at the moment the most prominent conjectures concerning the rational torsion subgroup of abelian varieties. A possible starting point is to prove the existence of such a constant restricting to jacobians of hyperelliptic curves of genus two over the rational numbers. If we restrict to jacobians of hyperelliptic curves with complex multiplication, such a constant is already known. So restricting to hyperelliptic curves with real multiplication could be a possible next step.

Problem. *Find explicit formulae for the moduli space describing abelian varieties of dimension g with a torsion point or a torsion subgroup of certain order.*

This problem is as hard as the previous one. Only for small N as $N = 2, 3$ and $g = 2$ or for elliptic curves there are equations for the moduli space known. Questions concerning the moduli space of these objects can only be answered with a deep understanding of modular forms of higher dimension.

Summing up, we conclude that there is still a lot of interesting work to do in this area of research.

A. Magma Codes

A.1. 13-Torsion Following Leprévost

Lemma A.1. *With the following* Magma *code we computed the family of hyperelliptic curves admitting a* 13*-torsion point on its jacobian in Theorem 3.14.*

```
 //Setting up the rational function field
 K<p,t>:=RationalFunctionField(Rationals(),2);
 R<x>:=PolynomialRing(K);
 r:=0;
 //Setting q:=-p^2 makes the first coefficient of a vanish
 q:=-p^2;
 //Setting up the congruence modulo b
 b:=x^4-(p^2-2*q)*x^3+(q^2-2*(p*r-t))*x^2-(r^2-2*q*t)*x+t^2;
 R1:=x^3-(p^2-2*q)*x^2+(q^2-2*(p*r-t/2))*x-(r^2-q*t);
 S:=quo<R|b>;
 R1:=R1/(p*t);
 //Lifting the congruence
 R2:=R1-R!(S!((R!((R1^2-x)/b))/(2*R1)))*b;
 S2:=quo<R|b^2>;
 //Computing the defining polynomial
 a:=R!(S2!(R2^13));
 f:=R!((a^2-x^13)/b^2);
 //Computing the Igusa invariants
 IgusaClebschInvariants(f);
[
    (2p^8t^3 - 2p^4t^4 - 2t^5)/p^12,
    (1/4p^16t^6 - 23/4p^12t^7 + 25/2p^8t^8 + 23/4p^4t^9 +
        1/4t^10)/p^24,
    (1/8p^24t^9 - 173/64p^20t^10 + 75/16p^16t^11 - 559/32p^12t^12 -
        75/16p^8t^13 - 173/64p^4t^14 - 1/8t^15)/p^36,
    (-1/16p^8t^19 + 349/256p^4t^20 + 1/16t^21)/p^44
]
```

A.2. 19-Torsion Family

Lemma A.2. *The* Magma *code for determining that there exist no isomorphism of our family and the family of* Leprévost *is the following,*

```
//Constructing a rational function field in the indeterminates
//a for our family
//and a2 for the family of Leprévost
K<a,a2>:=RationalFunctionField(Rationals(),2);
R<x>:=PolynomialRing(K);
//Setting up our family
t:=-4-(a^4 + 6*a^2+4*a+1)/a^3;
b:=-a-(4+t);
c:=6-a*b;
d:=-a*c-4;
A:=1/2*((a-b-1)*x^2-(a+c)*x-d);
f:=A^2-t*x^4*(x-1);
C:=HyperellipticCurve(f);
//Finished setting up our family
//Compute absolute Igusa invariants
ICI_c:=IgusaClebschInvariants(C);
absII_c:=[
          ICI_c[2]/ICI_c[1]^2,
          ICI_c[3]/ICI_c[1]^3,
          ICI_c[4]/ICI_c[1]^5
         ];
//Setting up Leprevost family
A2:=-(a2^10+6*a2^9+29*a2^8+168*a2^7+482*a2^6-348*a2^5+482*a2^4
      +168*a2^3+29*a2^2+6*a2+1)*x^2
      +2*(a2+1)^2*(a2^8+4*a2^7+20*a2^6+92*a2^5
             +22*a2^4+92*a2^3+20*a2^2+4*a2+1)*x
      -(a2+1)^6*(a2^4+14*a2^2+1);
f2:=A2^2-1024*a2^4*(a2^2-1)^2*(a2^4+14*a2^2+1)^2*x^3*(x-1)^2;
C2:=HyperellipticCurve(f2);
//Finished setting up Leprevost family
//Compute absolute Igusa invariants for Leprévost family
```

```
ICI_c2:=IgusaClebschInvariants(C2);
absII_c2:=[
           ICI_c2[2]/ICI_c2[1]^2,
           ICI_c2[3]/ICI_c2[1]^3,
           ICI_c2[4]/ICI_c2[1]^5
          ];
//taking the difference of the absolute Igusa invariants
diff2:=[Numerator(absII_c[i]-absII_c2[i]): i in [1..3]];
//Setting up the scheme of parameters with
//equal absolute Igusa invariants
AA:=AffineSpace(Parent(diff2[1]));
X:=Scheme(AA,diff2);
```

A.3. 11-Torsion family

Lemma A.3. *With this* Magma *code we computed the family of hyperelliptic curves of genus two with a* 11*-torsion divisor on the image of the curve in its jacobian. The corresponding result in the thesis is Example 3.5.*

```
//Constructing the rational function field
K<lambda,mu,eta>:=RationalFunctionField(Rationals(),3);
S<X>:=PolynomialRing(K);
//Setting the u-coordinate of the torsion divisor
xi:=eta^2+2*lambda*mu*eta-lambda+2*lambda^2*eta+lambda^2*mu^2
+2*lambda^3*mu +lambda^4;
u:=X+xi;
//Lifting the quadratic congruence with Hensel's Lemma
R:=X^2+mu*X+eta;
b:=X^3+(2*mu+lambda)*X^2+(2*eta+mu^2+2*lambda*mu+lambda^2)*X
+2*mu*eta-1+2*lambda*eta+2*lambda^2*mu+lambda^3+lambda*mu^2;
S1:=quo<S|b>;
S2:=quo<S|b^2>;
lambda1:=X-lambda;
lambda2:=S!(S1!(-lambda1/(2*R)));
R2:=R+lambda2*b;
//Computing the defining polynomial with arbitrary u-coordinate
F:=S!((S!(S2!(R2)^11)^2-u^11)/b^2);
R:=RingOfIntegers(K);
```

```
//Computing the coefficients of F under the assumption that the
//u-coordinate of the torsion divisor is equal to x
S:=quo<R|R!xi>;
R<x>:=PolynomialRing(S);
R!F;
```

A.4. 17-torsion over a Number Field

Lemma A.4. *The* Magma *code for computing the defining equation for the* 17*-torsion example is the following.*

```
//Setting up the rational function field
K<p,q,t,u>:=RationalFunctionField(Rationals(),4);
R<x>:=PolynomialRing(K);
//Setting up the congruence modulo Q
r:=(-1/8*p^3 + 1/2*p*q + 2*u);
s:=(1/64*p^4 - 1/8*p^2*q + p*u + 1/4*q^2);
b:=x^6+p*x^5+q*x^4+r*x^3+s*x^2+t*x+u^2;
R1:=x^3+p/2*x^2+(q-1/4*p^2)/2*x+u;
S:=quo<R|b>;
//Lifting the congruence modulo Q to a congruence modulo Q^2
R2:=R1-R!(S!((R!((R1^2-(-1/4*p^2*u + q*u - t)*x)/b))/(2*R1)))*b;
S1:=quo<R|b^2>;
//Computing the defining polynomial
a:=R!((S1!R2)^17);
F:=R!((a^2-((-1/4*p^2*u + q*u - t)*x)^17)/b^2);
```

A.5. 7-Torsion via Pells Equation

Lemma A.5. *The absolute* Igusa *invariants of C_λ in Theorem 3.37 are given by*

$$\begin{aligned}
\alpha(C_\lambda) &= \big(\lambda^{24} + 32\lambda^{22} + 436\lambda^{20} + 3431\lambda^{18} + 17663\lambda^{16} + 63280\lambda^{14} + 162608\lambda^{12} \\
&\quad + 302517\lambda^{10} + \frac{807965}{2}\lambda^8 + \frac{752535}{2}\lambda^6 + \frac{3690073}{16}\lambda^4 + 82881\lambda^2 + 13092\Big) \cdot \\
&\quad \frac{1}{2^6(\lambda^{12} + 16\lambda^{10} + 90\lambda^8 + 265\lambda^6 + 432\lambda^4 + \frac{1403}{4}\lambda^2 + 102)^2}, \\
\beta(C_\lambda) &= \Big(\lambda^{36} + 48\lambda^{34} + 1038\lambda^{32} + \frac{27097}{2}\lambda^{30} + \frac{241237}{2}\lambda^{28} + \frac{6266553}{8}\lambda^{26} \\
&\quad + \frac{7732161}{2}\lambda^{24} + \frac{29762419}{2}\lambda^{22} + \frac{363095039}{8}\lambda^{20} + \frac{884972175}{8}\lambda^{18} \\
&\quad + \frac{863944095}{4}\lambda^{16} + \frac{2694007649}{8}\lambda^{14} + \frac{3323900783}{8}\lambda^{12} + \frac{6387815919}{16}\lambda^{10} \\
&\quad + \frac{4661354371}{16}\lambda^8 + \frac{9936719491}{64}\lambda^6 \\
&\quad + \frac{453675089}{8}\lambda^4 + 12631657\lambda^2 + 1289688\Big) \cdot \\
&\quad \frac{1}{2^9(\lambda^{12} + 16\lambda^{10} + 90\lambda^8 + 265\lambda^6 + 432\lambda^4 + \frac{1403}{4}\lambda^2 + 102)^3}, \\
\gamma(C_\lambda) &= \big(\lambda^2 + 2\big)^{14} \cdot \\
&\quad \frac{\big(\lambda^{14} + 21\lambda^{12} + 160\lambda^{10} + \frac{1301}{2}\lambda^8 + \frac{3167}{2}\lambda^6 + \frac{37337}{16}\lambda^4 + 1921\lambda^2 + 676\big)}{2^{14}(\lambda^{12} + 16\lambda^{10} + 90\lambda^8 + 265\lambda^6 + 432\lambda^4 + \frac{1403}{4}\lambda^2 + 102)^5}.
\end{aligned}$$

B. Formulae for the Kummer Surface

Let $P := (\kappa_1 : \ldots : \kappa_4) \in \mathcal{K}(\mathrm{Jac}(C))$ be a point on the KUMMER surface of the jacobian of the genus two hyperelliptic curve C. Then $\delta_2(P) = (a_1(P) : \ldots : a_4(P))$ is given by the coordinates

$$
\begin{aligned}
a_1(P) =& 4\kappa_1\kappa_4^3 + 4\kappa_4^2(\kappa_1^2 f_2 - \kappa_2\kappa_3 f_5 - 3\kappa_3^2 f_6) \\
&+ 4\kappa_4(-4\kappa_1^3 f_0 f_4 + \kappa_1^3 f_1 f_3 - 8\kappa_1^2\kappa_2 f_0 f_5 - 2\kappa_1^2\kappa_3 f_1 f_5 - 12\kappa_1\kappa_2^2 f_0 f_6 - \kappa_1\kappa_2^2 f_1 f_5 \\
&- 6\kappa_1\kappa_2\kappa_3 f_1 f_6 - 2\kappa_1\kappa_2\kappa_3 f_2 f_5 - 4\kappa_1\kappa_3^2 f_2 f_6 - \kappa_1\kappa_3^2 f_3 f_5 - 2\kappa_2^3 f_1 f_6 - 4\kappa_2^2\kappa_3 f_2 f_6 \\
&- 6\kappa_2\kappa_3^2 f_3 f_6 - 8\kappa_3^3 f_4 f_6 + 2\kappa_3^3 f_5^2) \\
&+ 4\kappa_3^4 f_4 f_5^2 + 4\kappa_1^4 f_1^2 f_4 + 4\kappa_1^4 f_0 f_3^2 - 16\kappa_3^4 f_2 f_6^2 + 4\kappa_2^4 f_0 f_5^2 - 16\kappa_3^4 f_4^2 f_6 \\
&- 16\kappa_2\kappa_3^3 f_3 f_4 f_6 - 16\kappa_1^4 f_0^2 f_6 - 16\kappa_1^4 f_0 f_2 f_4 - 4\kappa_1^2\kappa_2\kappa_3 f_1 f_3 f_5 + 4\kappa_2^3\kappa_3 f_1 f_5^2 \\
&+ 4\kappa_2\kappa_3^3 f_3 f_5^2 + 4\kappa_2^2\kappa_3^2 f_2 f_5^2 - 16\kappa_1^3\kappa_2 f_0 f_1 f_6 - 32\kappa_1^3\kappa_2 f_0 f_2 f_5 + 8\kappa_1^3\kappa_2 f_1^2 f_5 \\
&+ 32\kappa_1^3\kappa_3 f_0 f_2 f_6 - 16\kappa_1^3\kappa_3 f_0 f_3 f_5 - 16\kappa_1^3\kappa_3 f_1^2 f_6 - 64\kappa_1^2\kappa_2^2 f_0 f_2 f_6 - 8\kappa_1^2\kappa_2^2 f_0 f_3 f_5 \\
&+ 12\kappa_1^2\kappa_2^2 f_1^2 f_6 - 16\kappa_1^2\kappa_2\kappa_3 f_0 f_4 f_5 - 16\kappa_1^2\kappa_2\kappa_3 f_1 f_2 f_6 - 48\kappa_1^2\kappa_3^2 f_0 f_4 f_6 \\
&+ 16\kappa_1^2\kappa_3^2 f_0 f_5^2 + 24\kappa_1^2\kappa_3^2 f_1 f_3 f_6 - 8\kappa_1^2\kappa_3^2 f_1 f_4 f_5 - 16\kappa_1^2\kappa_3^2 f_2^2 f_6 - 32\kappa_1\kappa_2^3 f_0 f_3 f_6 \\
&- 16\kappa_1\kappa_2^2\kappa_3 f_0 f_5^2 - 24\kappa_1\kappa_2^2\kappa_3 f_1 f_3 f_6 - 16\kappa_1\kappa_2\kappa_3^2 f_0 f_5 f_6 \\
&- 8\kappa_1\kappa_2\kappa_3^2 f_1 f_5^2 - 16\kappa_1\kappa_2\kappa_3^2 f_2 f_3 f_6 + 32\kappa_1\kappa_3^3 f_0 f_6^2 - 16\kappa_1\kappa_3^3 f_1 f_5 f_6 - 8\kappa_1\kappa_3^3 f_3^2 f_6 \\
&- 16\kappa_2^4 f_0 f_4 f_6 - 16\kappa_2^3\kappa_3 f_0 f_5 f_6 - 16\kappa_2^3\kappa_3 f_1 f_4 f_6 \\
&- 48\kappa_2^2\kappa_3^2 f_0 f_6^2 - 8\kappa_2^2\kappa_3^2 f_1 f_5 f_6 - 16\kappa_2^2\kappa_3^2 f_2 f_4 f_6 - 32\kappa_2\kappa_3^3 f_1 f_6^2 + 8\kappa_3^4 f_3 f_5 f_6 \\
a_2(P) =& 4\kappa_2\kappa_4^3 + \kappa_4^2(4\kappa_1^2 f_1 + 8\kappa_1\kappa_2 f_2 - 8\kappa_1\kappa_3 f_3 + 5\kappa_2^2 f_3 + 8\kappa_2\kappa_3 f_4 + 4\kappa_3^2 f_5) \\
&+ 2\kappa_4(2\kappa_1^3 f_0 f_3 + 8\kappa_1^2\kappa_2 f_0 f_4 + \kappa_1^2\kappa_2 f_1 f_3 - 8\kappa_1^2\kappa_3 f_0 f_5 + 8\kappa_1^2\kappa_3 f_1 f_4 \\
&- 6\kappa_1^2\kappa_3 f_2 f_3 + 4\kappa_1\kappa_2^2 f_0 f_5 + 4\kappa_1\kappa_2^2 f_1 f_4 - 24\kappa_1\kappa_2\kappa_3 f_0 f_6 \\
&+ 8\kappa_1\kappa_2\kappa_3 f_1 f_5 + 8\kappa_1\kappa_2\kappa_3 f_2 f_4 - 5\kappa_1\kappa_2\kappa_3 f_3^2 \\
&- 8\kappa_1\kappa_3^2 f_1 f_6 + 8\kappa_1\kappa_3^2 f_2 f_5 - 6\kappa_1\kappa_3^2 f_3 f_4 + 2\kappa_2^3 f_1 f_5 + 4\kappa_2^2\kappa_3 f_1 f_6 + 4\kappa_2^2\kappa_3 f_2 f_5 \\
&+ 8\kappa_2\kappa_3^2 f_2 f_6 + \kappa_2\kappa_3^2 f_3 f_5 + 2\kappa_3^3 f_3 f_6) \\
&+ \kappa_1^4 f_1^2 f_3 + 5\kappa_1^2\kappa_3^2 f_3^3 + 16\kappa_3^4 f_1 f_6^2 + \kappa_3^4 f_3 f_5^2 + 16\kappa_1^4 f_0^2 f_5 - 8\kappa_1\kappa_2^2\kappa_3 f_1 f_3 f_5 \\
&+ 32\kappa_1^2\kappa_2\kappa_3 f_1^2 f_6 - 20\kappa_1\kappa_2\kappa_3^2 f_1 f_3 f_6 - 4\kappa_1^4 f_0 f_2 f_3 + 32\kappa_1^3\kappa_2 f_0^2 f_6 + 16\kappa_1^3\kappa_2 f_0 f_1 f_5
\end{aligned}
$$

$$
\begin{aligned}
&- 4\kappa_1^3\kappa_2 f_0 f_3^2 - 32\kappa_1^3\kappa_3 f_0 f_2 f_5 + 16\kappa_1^3\kappa_3 f_0 f_3 f_4 + 16\kappa_1^3\kappa_3 f_1^2 f_5 - 6\kappa_1^3\kappa_3 f_1 f_3^2 \\
&+ 32\kappa_1^2\kappa_2^2 f_0 f_1 f_6 - 4\kappa_1^2\kappa_2^2 f_0 f_3 f_4 + 4\kappa_1^2\kappa_2^2 f_1^2 f_5 - 64\kappa_1^2\kappa_2\kappa_3 f_0 f_2 f_6 \\
&- 20\kappa_1^2\kappa_2\kappa_3 f_0 f_3 f_5 \\
&+ 32\kappa_1^2\kappa_2\kappa_3 f_0 f_4^2 + 16\kappa_1^2\kappa_2\kappa_3 f_1 f_2 f_5 - 12\kappa_1^2\kappa_2\kappa_3 f_1 f_3 f_4 - 20\kappa_1^2\kappa_3^2 f_0 f_3 f_6 \\
&- 14\kappa_1^2\kappa_3^2 f_1 f_3 f_5 + 16\kappa_1^2\kappa_3^2 f_1 f_4^2 + 16\kappa_1^2\kappa_3^2 f_2^2 f_5 - 20\kappa_1^2\kappa_3^2 f_2 f_3 f_4 - 4\kappa_1\kappa_2^3 f_0 f_3 f_5 \\
&+ 8\kappa_1\kappa_2^3 f_1^2 f_6 - 56\kappa_1\kappa_2^2\kappa_3 f_0 f_3 f_6 + 32\kappa_1\kappa_2^2\kappa_3 f_0 f_4 f_5 + 32\kappa_1\kappa_2^2\kappa_3 f_1 f_2 f_6 \\
&- 64\kappa_1\kappa_2\kappa_3^2 f_0 f_4 f_6 + 32\kappa_1\kappa_2\kappa_3^2 f_0 f_5^2 + 16\kappa_1\kappa_2\kappa_3^2 f_1 f_4 f_5 + 32\kappa_1\kappa_2\kappa_3^2 f_2^2 f_6 \\
&- 12\kappa_1\kappa_2\kappa_3^2 f_2 f_3 f_5 - 32\kappa_1\kappa_3^3 f_1 f_4 f_6 + 16\kappa_1\kappa_3^3 f_1 f_5^2 + 16\kappa_1\kappa_3^3 f_2 f_3 f_6 - 6\kappa_1\kappa_3^3 f_3^2 f_5 \\
&- 4\kappa_2^4 f_0 f_3 f_6 + 8\kappa_2^3\kappa_3 f_0 f_5^2 - 4\kappa_2^3\kappa_3 f_1 f_3 f_6 + 32\kappa_2^2\kappa_3^2 f_0 f_5 f_6 + 4\kappa_2^2\kappa_3^2 f_1 f_5^2 \\
&- 4\kappa_2^2\kappa_3^2 f_2 f_3 f_6 + 32\kappa_2\kappa_3^3 f_0 f_6^2 + 16\kappa_2\kappa_3^3 f_1 f_5 f_6 - 4\kappa_2\kappa_3^3 f_3^2 f_6 - 4\kappa_3^4 f_3 f_4 f_6
\end{aligned}
$$

$$
\begin{aligned}
a_3(P) =& 4\kappa_3\kappa_4^3 + 4\kappa_4^2(-3\kappa_1^2 f_0 - \kappa_1\kappa_2 f_1 + \kappa_3^2 f_4) \\
&+ 4\kappa_4(-8\kappa_1^3 f_0 f_2 + 2\kappa_1^3 f_1^2 - 6\kappa_1^2\kappa_2 f_0 f_3 - 4\kappa_1^2\kappa_3 f_0 f_4 - \kappa_1^2\kappa_3 f_1 f_3 - 4\kappa_1\kappa_2^2 f_0 f_4 \\
&- 6\kappa_1\kappa_2\kappa_3 f_0 f_5 - 2\kappa_1\kappa_2\kappa_3 f_1 f_4 - 2\kappa_1\kappa_3^2 f_1 f_5 - 2\kappa_2^3 f_0 f_5 - 12\kappa_2^2\kappa_3 f_0 f_6 - \kappa_2^2\kappa_3 f_1 f_5 \\
&- 8\kappa_2\kappa_3^2 f_1 f_6 - 4\kappa_3^3 f_2 f_6 + \kappa_3^3 f_3 f_5) \\
&+ 4\kappa_2^4 f_1^2 f_6 - 16\kappa_1^4 f_0^2 f_4 - 16\kappa_1^4 f_0 f_2^2 + 4\kappa_3^4 f_2 f_5^2 + 4\kappa_1^4 f_1^2 f_2 + 4\kappa_3^4 f_3^2 f_6 - 16\kappa_3^4 f_0 f_6^2 \\
&- 8\kappa_1^2\kappa_3^2 f_1 f_2 f_5 + 4\kappa_1^3\kappa_2 f_1^2 f_3 + 4\kappa_1^2\kappa_2^2 f_1^2 f_4 + 4\kappa_1\kappa_2^3 f_1^2 f_5 + 8\kappa_1^4 f_0 f_1 f_3 \\
&- 32\kappa_1^3\kappa_2 f_0^2 f_5 - 4\kappa_1\kappa_2\kappa_3^2 f_1 f_3 f_5 - 16\kappa_1^3\kappa_2 f_0 f_2 f_3 + 32\kappa_1^3\kappa_3 f_0^2 f_6 - 16\kappa_1^3\kappa_3 f_0 f_1 f_5 \\
&- 8\kappa_1^3\kappa_3 f_0 f_3^2 - 48\kappa_1^2\kappa_2^2 f_0^2 f_6 - 8\kappa_1^2\kappa_2^2 f_0 f_1 f_5 - 16\kappa_1^2\kappa_2^2 f_0 f_2 f_4 - 16\kappa_1^2\kappa_2\kappa_3 f_0 f_1 f_6 \\
&- 16\kappa_1^2\kappa_2\kappa_3 f_0 f_3 f_4 - 8\kappa_1^2\kappa_2\kappa_3 f_1^2 f_5 - 48\kappa_1^2\kappa_3^2 f_0 f_2 f_6 + 24\kappa_1^2\kappa_3^2 f_0 f_3 f_5 \\
&- 16\kappa_1^2\kappa_3^2 f_0 f_4^2 + 16\kappa_1^2\kappa_3^2 f_1^2 f_6 - 16\kappa_1\kappa_2^3 f_0 f_1 f_6 - 16\kappa_1\kappa_2^3 f_0 f_2 f_5 \\
&- 24\kappa_1\kappa_2^2\kappa_3 f_0 f_3 f_5 - 16\kappa_1\kappa_2^2\kappa_3 f_1^2 f_6 - 16\kappa_1\kappa_2\kappa_3^2 f_0 f_4 f_5 - 16\kappa_1\kappa_2\kappa_3^2 f_1 f_2 f_6 \\
&+ 32\kappa_1\kappa_3^3 f_0 f_4 f_6 - 16\kappa_1\kappa_3^3 f_0 f_5^2 - 16\kappa_1\kappa_3^3 f_1 f_3 f_6 - 16\kappa_2^4 f_0 f_2 f_6 - 32\kappa_2^3\kappa_3 f_0 f_3 f_6 \\
&- 64\kappa_2^2\kappa_3^2 f_0 f_4 f_6 + 12\kappa_2^2\kappa_3^2 f_0 f_5^2 - 8\kappa_2^2\kappa_3^2 f_1 f_3 f_6 - 16\kappa_2\kappa_3^3 f_0 f_5 f_6 \\
&- 32\kappa_2\kappa_3^3 f_1 f_4 f_6 + 8\kappa_2\kappa_3^3 f_1 f_5^2 - 16\kappa_3^4 f_2 f_4 f_6
\end{aligned}
$$

$$
\begin{aligned}
a_4(P) =& \kappa_4^4 + 2\kappa_4^2(4\kappa_1^2 f_0 f_4 - \kappa_1^2 f_1 f_3 + 4\kappa_1\kappa_2 f_0 f_5 + 8\kappa_1\kappa_3 f_0 f_6 + 4\kappa_2^2 f_0 f_6 \\
&+ 4\kappa_2\kappa_3 f_1 f_6 + 4\kappa_3^2 f_2 f_6 - \kappa_3^2 f_3 f_5) \\
&+ 4\kappa_4(-2\kappa_3^3 f_3^2 f_6 - 2\kappa_1^3 f_0 f_3^2 - 2\kappa_3^3 f_2 f_5^2 + 8\kappa_1^2\kappa_3 f_0 f_2 f_6 - 2\kappa_1^3 f_1^2 f_4 \\
&+ 16\kappa_1\kappa_2^2 f_0 f_2 f_6 \\
&- 4\kappa_1\kappa_2^2 f_1^2 f_6 + \kappa_1\kappa_2\kappa_3 f_1 f_3 f_5 + 8\kappa_1^3 f_0 f_2 f_4 + 12\kappa_1^2\kappa_2 f_0 f_2 f_5 - 3\kappa_1^2\kappa_2 f_1^2 f_5 \\
&+ 4\kappa_1^2\kappa_3 f_0 f_3 f_5 - 2\kappa_1^2\kappa_3 f_1^2 f_6 + 2\kappa_1\kappa_2^2 f_0 f_3 f_5 + 20\kappa_1\kappa_2\kappa_3 f_0 f_3 f_6 + 8\kappa_1\kappa_3^2 f_0 f_4 f_6 \\
&- 2\kappa_1\kappa_3^2 f_0 f_5^2 + 4\kappa_1\kappa_3^2 f_1 f_3 f_6 + 4\kappa_2^3 f_0 f_3 f_6 + 16\kappa_2^2\kappa_3 f_0 f_4 f_6 - 4\kappa_2^2\kappa_3 f_0 f_5^2 \\
&+ 2\kappa_2^2\kappa_3 f_1 f_3 f_6 + 12\kappa_2\kappa_3^2 f_1 f_4 f_6 - 3\kappa_2\kappa_3^2 f_1 f_5^2 + 8\kappa_3^3 f_2 f_4 f_6)
\end{aligned}
$$

$$+ 16\kappa_3^4 f_2^2 f_6^2 + \kappa_3^4 f_3^2 f_5^2 - 2\kappa_1^4 f_1^3 f_5 + 16\kappa_2^4 f_0^2 f_6^2 + \kappa_1^4 f_1^2 f_3^2 + 16\kappa_1^4 f_0^2 f_4^2$$
$$- 4\kappa_1^4 f_0 f_1^2 f_6 + 16\kappa_1^4 f_0 f_2^2 f_4 + 16\kappa_1^2\kappa_2\kappa_3 f_0 f_1 f_5^2 - 16\kappa_3^4 f_1 f_3 f_6^2 - 8\kappa_1\kappa_2\kappa_3^2 f_0 f_3 f_5^2$$
$$- 2\kappa_3^4 f_1 f_5^3 + 16\kappa_3^4 f_0 f_4 f_6^2 + 16\kappa_1^4 f_0^2 f_2 f_6 + \kappa_2^4 f_1^2 f_5^2 - 16\kappa_1^4 f_0^2 f_3 f_5 + 8\kappa_1^4 f_0 f_1 f_2 f_5$$
$$- 8\kappa_1^4 f_0 f_1 f_3 f_4 - 4\kappa_1^4 f_0 f_2 f_3^2 - 4\kappa_1^4 f_1^2 f_2 f_4 - 32\kappa_1^3\kappa_2 f_0^2 f_3 f_6 + 32\kappa_1^3\kappa_2 f_0^2 f_4 f_5$$
$$+ 32\kappa_1^3\kappa_2 f_0 f_1 f_2 f_6 - 16\kappa_1^3\kappa_2 f_0 f_1 f_3 f_5 + 32\kappa_1^3\kappa_2 f_0 f_2^2 f_5 - 8\kappa_1^3\kappa_2 f_1^3 f_6$$
$$- 8\kappa_1^3\kappa_2 f_1^2 f_2 f_5 - 64\kappa_1^3\kappa_3 f_0^2 f_4 f_6 + 32\kappa_1^3\kappa_3 f_0^2 f_5^2 + 16\kappa_1^3\kappa_3 f_0 f_1 f_3 f_6$$
$$+ 16\kappa_1^3\kappa_3 f_0 f_2 f_3 f_5 - 4\kappa_1^3\kappa_3 f_1^2 f_3 f_5 + 32\kappa_1^2\kappa_2^2 f_0^2 f_4 f_6 + 16\kappa_1^2\kappa_2^2 f_0^2 f_5^2$$
$$- 24\kappa_1^2\kappa_2^2 f_0 f_1 f_3 f_6 + 64\kappa_1^2\kappa_2^2 f_0 f_2^2 f_6 + 8\kappa_1^2\kappa_2^2 f_0 f_2 f_3 f_5 - 16\kappa_1^2\kappa_2^2 f_1^2 f_2 f_6$$
$$- 2\kappa_1^2\kappa_2^2 f_1^2 f_3 f_5 + 64\kappa_1^2\kappa_2\kappa_3 f_0^2 f_5 f_6 - 32\kappa_1^2\kappa_2\kappa_3 f_0 f_1 f_4 f_6$$
$$+ 64\kappa_1^2\kappa_2\kappa_3 f_0 f_2 f_3 f_6 + 8\kappa_1^2\kappa_2\kappa_3 f_0 f_3^2 f_5 - 8\kappa_1^2\kappa_2\kappa_3 f_1^2 f_3 f_6$$
$$+ 64\kappa_1^2\kappa_3^2 f_0^2 f_6^2 + 96\kappa_1^2\kappa_3^2 f_0 f_2 f_4 f_6 - 32\kappa_1^2\kappa_3^2 f_0 f_2 f_5^2$$
$$- 16\kappa_1^2\kappa_3^2 f_0 f_3^2 f_6 + 8\kappa_1^2\kappa_3^2 f_0 f_3 f_4 f_5 - 32\kappa_1^2\kappa_3^2 f_1^2 f_4 f_6$$
$$+ 12\kappa_1^2\kappa_3^2 f_1^2 f_5^2 + 8\kappa_1^2\kappa_3^2 f_1 f_2 f_3 f_6 + 32\kappa_1\kappa_2^3 f_0^2 f_5 f_6$$
$$+ 32\kappa_1\kappa_2^3 f_0 f_2 f_3 f_6 - 8\kappa_1\kappa_2^3 f_1^2 f_3 f_6 + 64\kappa_1\kappa_2^2\kappa_3 f_0^2 f_6^2$$
$$+ 32\kappa_1\kappa_2^2\kappa_3 f_0 f_1 f_5 f_6 + 48\kappa_1\kappa_2^2\kappa_3 f_0 f_3^2 f_6 + 64\kappa_1\kappa_2\kappa_3^2 f_0 f_1 f_6^2$$
$$- 32\kappa_1\kappa_2\kappa_3^2 f_0 f_2 f_5 f_6 + 64\kappa_1\kappa_2\kappa_3^2 f_0 f_3 f_4 f_6 + 16\kappa_1\kappa_2\kappa_3^2 f_1^2 f_5 f_6 + 8\kappa_1\kappa_2\kappa_3^2 f_1 f_3^2 f_6$$
$$- 64\kappa_1\kappa_3^3 f_0 f_2 f_6^2 + 16\kappa_1\kappa_3^3 f_0 f_3 f_5 f_6 + 32\kappa_1\kappa_3^3 f_1^2 f_6^2 + 16\kappa_1\kappa_3^3 f_1 f_3 f_4 f_6$$
$$- 4\kappa_1\kappa_3^3 f_1 f_3 f_5^2 + 16\kappa_2^4 f_0 f_2 f_4 f_6 - 4\kappa_2^4 f_0 f_2 f_5^2 - 4\kappa_2^4 f_1^2 f_4 f_6 + 32\kappa_2^3\kappa_3 f_0 f_1 f_6^2$$
$$+ 32\kappa_2^3\kappa_3 f_0 f_3 f_4 f_6 - 8\kappa_2^3\kappa_3 f_0 f_3 f_5^2 + 32\kappa_2^2\kappa_3^2 f_0 f_2 f_6^2 - 24\kappa_2^2\kappa_3^2 f_0 f_3 f_5 f_6$$
$$+ 64\kappa_2^2\kappa_3^2 f_0 f_4^2 f_6 - 16\kappa_2^2\kappa_3^2 f_0 f_4 f_5^2 + 16\kappa_2^2\kappa_3^2 f_1^2 f_6^2 + 8\kappa_2^2\kappa_3^2 f_1 f_3 f_4 f_6 - 2\kappa_2^2\kappa_3^2 f_1 f_3 f_5^2$$
$$- 32\kappa_2\kappa_3^3 f_0 f_3 f_6^2 + 32\kappa_2\kappa_3^3 f_0 f_4 f_5 f_6 - 8\kappa_2\kappa_3^3 f_0 f_5^3 + 32\kappa_2\kappa_3^3 f_1 f_2 f_6^2$$
$$- 16\kappa_2\kappa_3^3 f_1 f_3 f_5 f_6 + 32\kappa_2\kappa_3^3 f_1 f_4^2 f_6 - 8\kappa_2\kappa_3^3 f_1 f_4 f_5^2 - 4\kappa_3^4 f_0 f_5^2 f_6 + 8\kappa_3^4 f_1 f_4 f_5 f_6$$
$$- 8\kappa_3^4 f_2 f_3 f_5 f_6 + 16\kappa_3^4 f_2 f_4^2 f_6 - 4\kappa_3^4 f_2 f_4 f_5^2 - 4\kappa_3^4 f_3^2 f_4 f_6.$$

Bibliography

[Ada95] Brigitte Adam. Voronoĭ-algorithm expansion of two families with period length going to infinity. *Math. Comp.*, 64(212):1687–1704, 1995.

[AR80] William W. Adams and Michael J. Razar. Multiples of points on elliptic curves and continued fractions. *Proc. London Math. Soc. (3)*, 41(3):481–498, 1980.

[Art24] E. Artin. Quadratische Körper im Gebiete der höheren Kongruenzen. II. *Math. Z.*, 19(1):207–246, 1924.

[BB66] Walter L. Jr. Baily and Armand Borel. Compactification of Arithmetic Quotients of Bounded Symmetric Domains. *Annals of Mathematics*, 84(3): pp. 442–528, 1966.

[BGM96] Jr. George A. Baker and Peter Graves-Morris. *Padé approximants*, volume 59 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1996.

[BL04] Christina Birkenhake and Herbert Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2004.

[BS10] Nils Bruin and Michael Stoll. The Mordell-Weil sieve: proving non-existence of rational points on curves. *LMS Journal of Computation and Mathematics*, 13:272–306, 2010. ISSN 1461-1570.

[Buc85] Johannes Buchmann. A generalization of Voronoĭ's unit algorithm. I. *J. Number Theory*, 20(2):177–191, 1985.

[Can87] David G. Cantor. Computing in the Jacobian of a Hyperelliptic Curve. *Mathematics of Computation*, 48(177):95–101, January 1987.

[Can94] David G. Cantor. On the analogue of the division polynomials for hyperelliptic curves. *J. Reine Angew. Math.*, 447:91–145, 1994.

[CF96] John W.S. Cassels and E. Victor Flynn. *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*. Cambridge Studies in Religious Traditions. Cambridge University Press, 1996.

[CFA+05] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. Discrete Mathematics and Its Applications. Taylor & Francis, 2005.

[Cha41] Claude Chabauty. Sur les points rationnels des variétés algébriques dont l'irrégularité est supérieure à la dimension. *C. R. Acad. Sci. Paris*, 212: 1022–1024, 1941.

[CL12] Craig Costello and Kristin Lauter. Group law computations on jacobians of hyperelliptic curves. In Ali Miri and Serge Vaudenay, editors, *Selected Areas in Cryptography*, volume 7118 of *Lecture Notes in Computer Science*, pages 92–117. Springer Berlin Heidelberg, 2012. ISBN 978-3-642-28495-3. URL `http://dx.doi.org/10.1007/978-3-642-28496-0_6`.

[Col85] Robert F. Coleman. Effective Chabauty. *Duke Math. J.*, 52(3):765–770, 1985.

[DO14] Eduardo Ruiz Duarte and Octavio Páez Osuna. Explicit endomorphism of the jacobian of a hyperelliptic function field of genus 2 using base field operations. *IACR Cryptology ePrint Archive*, 2014:359, 2014. URL `http://dblp.uni-trier.de/db/journals/iacr/iacr2014.html#DuarteO14`.

[EH00] David Eisenbud and Joe Harris. *The geometry of schemes Graduate Texts in Mathematics, 197*. Springer Verlag, New York, 2000.

[Elk14] Noam D. Elkies. Simple genus-2 Jacobians with rational points of high order, July 2014. URL `http://www.math.harvard.edu/~elkies/g2_tors.html`.

[Fal83] Gerd Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[Fly90] E. Victor Flynn. Large rational torsion on abelian varieties. *J. Number Theory*, 36(3):257–265, 1990.

[Fly91] E. Victor Flynn. Sequences of rational torsions on abelian varieties. *Invent. Math.*, 106(2):433–442, 1991.

[Fly93] E. Victor Flynn. The group law on the jacobian of a curve of genus 2. *Journal für die reine und angewandte Mathematik*, 439:45–69, 1993.

[Gor02] Eyal Z. Goren. *Lectures on Hilbert modular varieties and modular forms*, volume 14 of *CRM Monograph Series*. American Mathematical Society, Providence, RI, 2002. With the assistance of Marc-Hubert Nicole.

[Gra90] David Grant. Formal groups in genus two. *J. Reine Angew. Math.*, 411: 96–121, 1990.

[Gra13] David Grant. On an analogue of the Lutz-Nagell theorem for hyperelliptic curves. *J. Number Theory*, 133(3):963–969, 2013.

[Gro60] Alexander Grothendieck. Éléments de géométrie algébrique. I. Le langage des schémas. *Inst. Hautes Études Sci. Publ. Math.*, (4):228, 1960.

[Ham66] William F. Hammond. The Modular Groups of Hilbert and Siegel. *American Journal of Mathematics*, 88(2):pp. 497–516, 1966.

[Har77] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.

[Has00] Ki-ichiro Hashimoto. On Brumer's family of RM-curves of genus two. *Tohoku Math. J. (2)*, 52(4):475–488, 2000.

[Hen18] Kurt Hensel. Eine neue theorie der algebraischen zahlen. *Mathematische Zeitschrift*, 2(3):433–452, 1918.

[HK89] Franz Halter-Koch. Reell-quadratische Zahlkörper mit großer Grundeinheit. *Abh. Math. Sem. Univ. Hamburg*, 59:171–181, 1989.

[HLP00] Everett W. Howe, Franck Leprévost, and Bjorn Poonen. Large torsion subgroups of split Jacobians of curves of genus two or three. *Forum Math.*, 12(3):315–364, 2000.

[HM98] Joe Harris and Ian Morrison. *Moduli of Curves*. Graduate Texts in Mathematics. Springer Verlag, 1998.

[How14] Everett W. Howe. Genus-2 Jacobians with torsion points of large order, July 2014. URL `http://arxiv.org/abs/1407.2654v2;http://arxiv.org/pdf/1407.2654v2`.

[HW01] J. William Hoffman and Steven H. Weintraub. The Siegel modular variety of degree two and level three. *Trans. Amer. Math. Soc.*, 353(8):3267–3305 (electronic), 2001.

[Igu60] Jun-ichi Igusa. Arithmetic variety of moduli for genus two. *Ann. of Math. (2)*, 72:612–649, 1960.

[Kan05] Naoki Kanayama. Division polynomials and multiplication formulae of Jacobian varieties of dimension 2. *Math. Proc. Cambridge Philos. Soc.*, 139(3):399–409, 2005.

[Kos14] Christiaan Koster. On the units of coordinate rings of algebraic curves, 2014. URL `http://scripties.fwn.eldoc.ub.rug.nl/FILES/scripties/Wiskunde/Masters/2014/Koster.C.J./Christiaan_Koster_WM_2014.pdf`.

[Kub76] Daniel S. Kubert. Universal bounds on the torsion of elliptic curves. *Proceedings of the London Mathematical Society*, 3(2):193, 1976.

[Küh95] Josef Kühner. On a family of generalized continued fraction expansions with period length going to infinity. *J. Number Theory*, 53(1):1–12, 1995.

[Lan82] Serge Lang. *Introduction to Algebraic and Abelian Functions*, volume 89 of *Graduate Texts in Mathematics*. Springer New York, 1982.

[Lan05] Tanja Lange. Formulae for arithmetic on genus 2 hyperelliptic curves. *Applicable Algebra in Engineering, Communication and Computing*, 15 (5):295–328, 2005. ISSN 0938-1279. URL `http://dx.doi.org/10.1007/s00200-004-0154-8`.

[Lep91a] Franck Leprévost. Famille de courbes de genre 2 munies d'une classe de diviseurs rationnels d'ordre 13. *C. R. Acad. Sci. Paris Sér. I Math.*, 313 (7):451–454, 1991.

[Lep91b] Franck Leprévost. Familles de courbes de genre 2 munies d'une classe de diviseurs rationnels d'ordre 15, 17, 19 ou 21. *C. R. Acad. Sci., Paris, Sér. I*, 313(11):771–774, 1991.

[Lep93] Franck Leprévost. Points rationnels de torsion de jacobiennes de certaines courbes de genre 2. *C. R. Acad. Sci. Paris Sér. I Math.*, 316(8):819–821, 1993.

[Lep95] Franck Leprevost. Jacobiennes de certaines courbes de genre 2: torsion et simplicité. *J. Théor. Nombres Bordeaux*, 7(1):283–306, 1995. Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993).

[LPS04] Franck Leprévost, Michael Pohst, and Andreas M. Schöpp. Rational torsion of $J_0(N)$ for hyperelliptic modular curves and families of Jacobians of genus 2 and genus 3 curves with a rational point of order 5, 7 or 10. *Abh. Math. Sem. Univ. Hamburg*, 74:193–203, 2004.

[LSY03] Yoonjin Lee, Renate Scheidler, and Christopher Yarrish. Computation of the fundamental units and the regulator of a cyclic cubic function field. *Experiment. Math.*, 12(2):211–225, 2003.

[Maz77] B. Mazur. Modular curves and the eisenstein ideal. *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, 47(1):33–186, 1977. ISSN 0073-8301.

[Mes91] Jean-Francois Mestre. Familles de courbes hyperelliptiques à multiplications réelles. In *Arithmetic algebraic geometry (Texel, 1989)*, volume 89 of *Progr. Math.*, pages 193–208. Birkhäuser Boston, Boston, MA, 1991.

[Mil08] James S. Milne. Abelian Varieties (v2.00), 2008. URL `http://www.jmilne.org/math/`.

[Mil11] James S. Milne. Algebraic Geometry (v5.21), 2011. URL `http://www.jmilne.org/math/`.

[MP07] William Mccallum and Bjorn Poonen. The method of Chabauty and Coleman. Technical report, 2007. URL `www-math.mit.edu/~poonen/papers/chabauty.pdf`.

[Mül10] Jan Steffen Müller. Explicit Kummer surface formulas for arbitrary characteristic. *LMS J. Comput. Math.*, 13:47–64, 2010.

[Mum84] David Mumford. *Tata lectures on theta, 2 : Jacobian theta functions and differential equations*. Progress in mathematics. Birkhauser, Boston, Basel, Stuttgart, 1984. ISBN 0-8176-3110-0.

[Mum99] David Mumford. *The Red Book of Varieties and Schemes: Includes the Michigan Lectures (1974) on Curves and Their Jacobians*. Lecture Notes in Mathematics. Springer Verlag, 1999.

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[Oga94] Hiroyuki Ogawa. Curves of genus 2 with a rational torsion divisor of order 23. *Proceedings of the Japan Academy, Series A, Mathematical Sciences*, 70(9):295–298, 1994.

[Ôni02] Yoshihiro Ônishi. Determinant expressions for abelian functions in genus two. *Glasg. Math. J.*, 44(3):353–364, 2002.

[Oor88] Frans Oort. Endomorphism algebras of abelian varieties. In *Algebraic geometry and commutative algebra*, pages 469–502. Kinokuniya, Tokyo, 1988.

[Pat07] Roger D. Patterson. Creepers: Real quadratic orders with large class number, March 2007. URL `http://arxiv.org/pdf/math/0703519v1`.

[Poo06] Bjorn Poonen. Lectures on rational points on curves, 2006. URL `http://math.mit.edu/~poonen/papers/curves.pdf`.

[PvdPW07a] Roger D. Patterson, Alfred J. van der Poorten, and Hugh C. Williams. Characterization of a generalized shanks sequence. *Pacific J. Math*, 230 (1):185–215, 2007.

[PvdPW07b] Roger D. Patterson, Alfred J. van der Poorten, and Hugh C. Williams. Characterization of a generalized Shanks sequence. *Pacific J. Math.*, 230 (1):185–215, 2007.

[PvdPW08] Roger D. Patterson, Alfred J. van der Poorten, and Hugh C. Williams. Sequences of Jacobian varieties with torsion divisors of quadratic order. *Funct. Approx. Comment. Math.*, 39(part 2):345–360, 2008.

[Ray83] Michel Raynaud. Courbes sur une variété abélienne et points de torsion. *Inventiones mathematicae*, 71:207–234, 1983.

[Rei85] Clifford Reiter. Effective lower bounds on large fundamental units of real quadratic fields. *Osaka J. Math.*, 22(4):755–765, 1985.

[Run99] Bernhard Runge. Endomorphism rings of abelian surfaces and projective models of their moduli spaces. *Tohoku Math. J. (2)*, 51(3):283–303, 1999.

[Sch95] René Schoof. Counting points on elliptic curves over finite fields. *Journal de Théorie des Nombres de Bordeaux*, 7(1):219–254, 1995.

[Sch00] Renate Scheidler. Purely cubic complex function fields with small units. *Acta Arith.*, 95(4):289–304, 2000.

[Sch04] Renate Scheidler. Algorithmic aspects of cubic function fields. In *Algorithmic number theory*, volume 3076 of *Lecture Notes in Comput. Sci.*, pages 395–410. Springer, Berlin, 2004.

[Shi98] Goro Shimura. *Abelian varieties with complex multiplication and modular functions*, volume 46 of *Princeton Mathematical Series*. Princeton University Press, Princeton, NJ, 1998.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[SS00] Renate Scheidler and Andreas Stein. Voronoi's algorithm in purely cubic congruence function fields of unit rank 1. *Math. Comp.*, 69(231):1245–1266, 2000.

[Ste99] A. Stein. Introduction to continued fraction expansions in real quadratic function fields. *Research report (University of Waterloo. Faculty of Mathematics)*, 1999.

[Sti09] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer Verlag, Berlin, second edition, 2009.

[Sto01] Michael Stoll. Implementing 2-descent for Jacobians of hyperelliptic curves. *Acta Arith.*, 98(3):245–277, 2001.

[Sto13] Michael Stoll. Uniform Bounds for the Number of Rational Points on Hyperelliptic Curves of Small Mordell-Weil Rank, 2013. URL `http://arxiv.org/abs/1307.1773`.

[Tan11] Adrian Tang. *Infrastructure of Function Fields of Unit Rank One*. ProQuest LLC, Ann Arbor, MI, 2011. 288 pp. Thesis (Ph.D.)–University of Calgary (Canada).

[Tat66] John Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966.

[TTV91] Walter Tautz, Jaap Top, and Alain Verberkmoes. Explicit hyperelliptic curves with real multiplication and permutation polynomials. *Canad. J. Math.*, 43(5):1055–1064, 1991.

[vdG88] Gerard van der Geer. *Hilbert modular surfaces*, volume 16 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1988.

[vdP04a] Alfred J. van der Poorten. Genus 2 curves, continued fractions, and Somos sequences, December 2004. URL `http://arxiv.org/abs/math/0412372v1`.

[vdP04b] Alfred J. van der Poorten. *Periodic continued fractions and elliptic curves*, volume 41 of *Fields Inst. Commun.*, pages 353–365. Amer. Math. Soc., Providence, RI, 2004.

[vdP05] Alfred J. van der Poorten. Elliptic Curves and Continued Fractions, 2005. URL `http://arxiv.org/pdf/math/0403225v3.pdf`.

[Wei29] André Weil. L'arithmétique sur les courbes algébriques. *Acta Mathematica*, 52(1):281–315, 1929.

[Yam71] Yoshihiko Yamamoto. Real quadratic number fields with large fundamental units. *Osaka J. Math.*, 8:261–270, 1971.

Selbstständigkeitserklärung

Hiermit versichere ich, Max Christian Kronberg, dass ich diese Dissertation selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Sie wurde weder in ihrer Gesamtheit noch in Teilen einer anderen wissenschaftlichen Hochschule zur Begutachtung in einem Promotionsverfahren vorgelegt.

Außerdem erkläre ich, dass ich die allgemeinen Prinzipien wissenschaftlicher Arbeit und Veröffentlichung, wie sie in den Leitlinien guter wissenschaftlicher Praxis der Carl von Ossietzky Universität Oldenburg festgelegt sind, befolgt habe.

Oldenburg, 18.Mai 2015

Lebenslauf

Persönliche Daten

Name:	Max Christian Kronberg
Geburtsdatum:	09. Januar 1986
Geburtsort:	Neumünster

Bildungsgang

1992 – 1996	Grundschule Hohenwestedt
1996 – 2005	Gymnasium Herderschule Rendsburg **Abschluss: Abitur**
2006 – 2008	Carl von Ossietzky Universität Oldenburg 2-Fächer-Bachelorstudiengang Mathematik/Chemie
2008 – 2009	Carl von Ossietzky Universität Oldenburg Fach-Bachelorstudiengang Mathematik **Abschluss: Bachelor of Science**
2009 – 2011	Carl von Ossietzky Universität Oldenburg Fach-Masterstudiengang Mathematik **Abschluss: Master of Science**
seit 10/2011	Carl von Ossietzky Universität Oldenburg Promotionsstudium Mathematik