rijksuniversiteit groningen

faculteit Wiskunde en Natuurwetenschappen

On the Units of Coordinate Rings of Algebraic Curves

Master Thesis Mathematics

July 2014

Student: Christiaan Koster

First Supervisor: Prof. dr. J. Top

Second Supervisor: Prof. dr. H. L. Trentelman

Abstract

In this thesis we have investigated the problem of finding the unit group of the coordinate ring of algebraic curves, and in particular of hyperelliptic curves. The existence of nontrivial units is linked to linear combinations of the points at infinity being torsion in the Jacobian of the curve. We have characterized the form of the unit group for hyperelliptic curves and have given many properties of it. Different methods were used to find examples of genus-2 hyperelliptic curves over $\mathbb{Q}$ with nontrivial unit group. Finally, we briefly looked at the situation for curves of genus larger than 2.

Contents

1 Introduction

An important part of algebraic geometry are algebraic curves. The most well known curves are probably elliptic curves. Elliptic curves are smooth curves of genus 1 and all smooth genus 1 curves are elliptic. There has been a lot of research done on the topic of elliptic curves and many things are known about them.

On curves of higher genus there hasn't been done as much research and there are still many unanswered questions. In this thesis a specific problem involving curves of genus larger than 1 is investigated, namely the problem of finding and characterizing the group of units of the coordinate ring of algebraic curves. In particular, we do this for hyperelliptic curves, which are curves of genus 2, over the field of rational numbers and over finite fields. We want to know what groups occur as unit groups and to find examples with different unit groups.

We will see that the unit group is related to the torsion order of a particular point on the Jacobian of the curve. For elliptic curves, there is the result of Mazur [15] about which groups occur for the group of points of finite order of an elliptic curve over the rational numbers, which also provides the answer for the Jacobian of elliptic curves as they are isomorphic as groups. Unfortunately, for curves of higher genus there are no such results and researchers are not even close to obtaining such results. Research on torsion points in the Jacobian of hyperelliptic curves over the rational numbers is recent and is still being done, for example [12] by Leprévost, [7] by Leprévost, Howe and Poonen and recently [6] by Howe.

Definitions and basic results from algebraic geometry that we will require in this thesis will be given in section 2. In section 3 a more thorough explanation of the subject of this thesis will be given, along with the definitions of Jacobians. Starting from section 4 the focus will be on hyperelliptic curves. The definitions and multiple characterizations of the unit group of the coordinate ring will be given. Then in section 5 we try to find example of hyperelliptic curves with interesting unit groups by using different techniques. After that, we briefly look at curves of genus larger than 2 and finally present our conclusions and options for further research in section 6.

2 Preliminaries

In this section we will define basic definitions and give standard results from algebraic geometry and in particular algebraic curves. Allt of the results come from Silverman's book [29], in particular chapters I and II. Throughout this section, we will assume that K is an arbitrary perfect field, i.e. a field such that every algebraic extension is separable. For example, $\mathbb{Q}$, $\mathbb{F}_q$ and $\mathbb{C}$ are perfect fields, where we use the standard notation for the field of rational numbers, finite field with q elements and the field of complex numbers respectively.

2.1 Affine Varieties

The affine n-space over K is denoted by $\mathbb{A}^n = \mathbb{A}^n(\overline{K})$. To any ideal $I \in \overline{K}[X] = \overline{K}[X_1, \cdots, X_n]$ we associate the set

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

Any such ideal I is finitely generated, and so the condition on V_I only needs to be checked on the generators of I. If $I = (f)$ for some f, then we use the notation $V_I = Z(f)$. The sets V_I are called affine algebraic sets and the ideal of V_I is given by

$$I(V_I) = \{f \in \overline{K}[X] : f(P) = 0 \text{ for all } lP \in V_I\}.$$

If the generators of the ideal of an algebraic set V can be generated by polynomials in $K[X]$, then V is defined over K, and this is denoted by V/K. An affine algebraic set V is called an affine variety if $I(V)$ is a prime ideal in $\overline{K}[X]$.

The coordinate ring of an affine variety V/K is $K[V] := K[X]/(I(V/K)$, where $I(V/K) = I(V) \cap K[X]$, and this ring is an integral domain. Its field of fractions is denoted by $K(V)$ and is called the function field of V/K. Similarly $\overline{K}[V]$ and $\overline{K}(V)$ are defined by replacing K by $\overline{K}$. For a variety V the dimension of V, denoted $\dim(V)$, is the transcendence degree of $\overline{K}(V)$ over $\overline{K}$. Let $P \in V$ and $f_1, \cdots, f_m \in \overline{K}[X]$ a set of generators of $I(V)$, then V is nonsingular (or smooth) at P if the $m \times n$ matrix

$$\left(\frac{\partial f_i}{\partial X_j}(P)\right)_{i \leq m, j \leq n}$$

has rank $n - \dim(V)$. If V is nonsingular at every point, then we say that V is nonsingular.

For each point $P \in V$, we define an ideal M_P of $\overline{K}[V]$ by

$$M_P = \{f \in \overline{K}[V] : f(P) = 0\}.$$

Then M_P is a maximal ideal and the local ring of V at P, denoted by $\overline{K}[V]_P$, is the localization of $\overline{K}[V]$ at M_P. In other words,

$$\overline{K}[V]_P = \{F \in \overline{K}(X) : F = f/g \text{ for some } f, g \in \overline{K}[V], g(P) \neq 0\}.$$

2.2 Projective Varieties

The projective n-space ove Kr is denoted by $\mathbb{P}^n = \mathbb{P}^n(\overline{K})$. A projective algebraic set is any set of the form V_I for a homogeneous ideal I. If V is a projective algebraic set, the ideal of V is

$$I(V) = \{f \in \overline{K}[V] : f \text{ is homogeneous and } f(P) = 0 \text{ for all } P \in V\}.$$

If $I(V)$ can be generated by homogeneous polynomials in $K[X]$, then V is defined over K and then the set of K-rational points of V is the set $V(K) = V \cap \mathbb{P}^n(K)$. Also, V is called a projective variety if $I(V)$ is a prime ideal in $\overline{K}[X]$.

Now, $\mathbb{P}^n$ contains many copies of $\mathbb{A}^n$. For example, for each $0 \leq i \leq n$, there is an inclusion $\phi_i : \mathbb{A}^n \to \mathbb{P}^n$ defined by

$$(y_1, \cdots, y_n) \mapsto (y_1 : y_2 : \cdots : y_{i-1} : 1 : y_i : \cdots : y_n).$$

We define

$$U_i = \{P = (x_0 : \cdots : x_n) \in \mathbb{P}^n : x_i \neq 0\},$$

then there is a natural bijection $\phi_i^{-1} : U_i \to \mathbb{A}^n$ defined by

$$(x_0 : \cdots : x_n) \mapsto (\frac{x_0}{x_i}, \frac{x_1}{x_i}, \cdots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \cdots, \frac{x_n}{x_i}).$$

For a fixed i, we will identify $\mathbb{A}^n$ with the set U_i in $\mathbb{P}^n$ via the map ϕ_i.

Now let V be a projective algebraic set with ideal $I(V) \subset \overline{K}[X]$, then $V \cap \mathbb{A}^n := \phi_i^{-1}(V \cap U_i)$ for some fixed i, is an affine algebriac set with ideal $I(V \cap \mathbb{A}^n) \subset \overline{K}[Y]$ given by

$$I(V \cap \mathbb{A}^n) = \{f(Y_1, \cdots, Y_{i-1}, 1, Y_{i+1}, \cdots, Y_n) : f(X_0, \cdots, X_n) \in I(V)\}.$$

This process is called dehomogenization with respect to X_i. This process can also be reversed. For any $f(Y) \in \overline{K}[Y]$ we define

$$f^*(X_0, \cdots, X_n) = X_i^d f(\frac{X_0}{X_i}, \frac{X_1}{X_i}, \cdots, \frac{X_{i-1}}{X_i}, \frac{X_{i+1}}{X_i}, \cdots, \frac{X_n}{X_i}),$$

where $d = \deg(f)$ is the smallest integer for which f^* is a polynomial. We say that f^* is the homogenization of f with respect to X_i.

Let $V \subset \mathbb{A}^n$ be an affine algebraic set with ideal $I(V)$, and consider V as a subset of $\mathbb{P}^n$ via $\phi_i(V)$. The projective closure of V, denoted by $\bar{V}$, is the projective algebraic set whose ideal $I(\bar{V})$ is generated by $\{f^*(X) : f \in I(V)\}$. If V is an affine variety, then $\bar{V}$ is a projective variety and $V = \bar{V} \cap \mathbb{A}^n$ and if V is defined over K, then $\bar{V}$ is as well.

Let V/K be a projective variety and choose $\mathbb{A}^n \subset \mathbb{P}^n$ such that $V \cap \mathbb{A}^n \neq \emptyset$. The dimension of V is the dimension of $V \cap \mathbb{A}^n$. The function field of V, denoted $K(V)$, is the function field of $V \cap \mathbb{A}^n$. Note that for different choices of $\mathbb{A}^n$, the different $K(V)$ are canonically isomorphic, so we may identify them.

Let $P \in V$ and choose $\mathbb{A}^n \subset \mathbb{P}^n$ with $P \in \mathbb{A}^n$, then V is nonsingular at P if $V \cap \mathbb{A}^n$ is nonsingular at P. The local ring of V at P is the local ring of $V \cap \mathbb{A}^n$ at P.

2.3 Rational Maps

Let V_1 and $V_2 \subset \mathbb{P}^n$ be projective varieties. A rational map from V_1 to V_2 is a map of the form

$$f : V_1 \to V_2, \qquad \phi = (f_0 : \cdots : f_n),$$

where the functions $f_0, \cdots, f_n \in \overline{K}(V_1)$ have the property that for every point $P \in V_1$ at which $f_0, \cdots, f_n$ are all defined, $\phi(P) = (f_0(P) : \cdots : f_n(P)) \in V_2$. It may be possible to

evaluate $\phi(P)$ at points P of V_1 where some f_i is not regular by replacting each f_i by gf_i for an appropriate $g \in \overline{K}(V_1)$.

A rational map ϕ is regular at $P \in V_1$ if there is a function $g \in \overline{K}(V_1)$ such that each gf_i is regular at P and such that there is some i for which $(gf_i)(P) \neq 0$. A rational map that is regular at every points is called a morphism. We say that V_1 and V_2 are isomorpihc, and write $V_1 \cong V_2$, if there are morphisms $\phi : V_1 \to V_2$ and $\psi : V_2 \to V_1$ such that $\psi \circ \phi$ and $\phi \circ \psi$ are the identity maps on V_1 and V_2 respectively.

We call a rational map $\phi : V_1 \to V_2$ a birational map if there is a rational map $\psi : V_2 \to V_1$ such that $\psi \circ \phi$ is the identity map on V_1. In that case we call V_1 and V_2 birationally equivalent.

2.4 Algebraic Curves

By a curve we will mean a projective variety of dimension 1. Let C be a curve and $P \in C$ a smooth point. Then $\overline{K}[C]_P$ is a discrete valuation ring. The valuation on $\overline{K}[C]_P$ is given by $\mathrm{ord}_P : \overline{K}[C]_P \to \{0, 1, 2, \cdots\} \cup \{\infty\}$ defined by $\mathrm{ord}_P(f) = \sup\{d \in \mathbb{Z} : f \in M_P^d\}$. Using $\mathrm{ord}_P(f/g) = \mathrm{ord}_P(f) - \mathrm{ord}_P(g)$ we extend ord_P to $\overline{K}(C)$. A uniformizer for C at P is any function $t \in \overline{K}(C)$ with $\mathrm{ord}_P(t) = 1$, i. e. a generator for the ideal M_P. If C is defined over K and if $t \in K(C)$ is a uniformizer at some nonsingular point $Q \in C(K)$, then $K(C)$ is a finite separable extension of $K(t)$.

Let $f \in \overline{K}(C)$, then f has a zero at P if $\mathrm{ord}_P(f) > 0$ and if $\mathrm{ord}_P(f) < 0$ then f has a pole at P. If $\mathrm{ord}_P(f) \geq 0$, then f is regular at P. If C is smooth and if $f \neq 0$, then there are only finitely many points of C at which f has a pole or zero. Further, if f has no poles, then $f \in \overline{K}$.

Let $V \subset \mathbb{P}^N$ be a variety, let $P \in C$ be a smooth point and let $\phi : C \to V$ be a rational map. Then ϕ is regular at P. In particular, if C is smooth, then ϕ is a morphism. If $\phi : C_1 \to C_2$ is a morphism of curves, then ϕ is either constant or surjective.

Suppose C_1 and C_2 are defined over K and suppose that $\psi : C_1 \to C_2$ is a nonconstant rational map defined over K. Then composition with ψ induces an injection of function fields fixing K,

$$\psi^* : K(C_2) \to K(C_1), \qquad \psi^* f = f \circ \psi.$$

Then $K(C_1)$ is a finite extension of $\psi^*(K(C_2))$. We say that ψ is a finite map and we define its degree to be $\deg \psi = [K(C_1) : \psi^*(K(C_2))]$. We say that ψ is separable or inseparable if the field extension $K(C_1)/\psi^* K(C_2)$ has the corresponding property. If ψ were a constant map, then we define the degree of ψ to be 0.

Let $P \in C_1$, then the ramification index of ψ at P, denoted by $e_\psi(P)$, is the quantity $e_\psi(P) = \mathrm{ord}_P(\psi^* t_{\psi(P)})$, where $t_{\psi(P)} \in K(C_2)$ is a uniformizer at $\psi(P)$. Note that $e_\psi(P) \geq 1$. We say that ψ is unramified at P if $e_\psi(P) = 1$. If C_1 and C_2 are now smooth, then for every $Q \in C_2$ we have that

$$\sum_{P \in \psi^{-1}(Q)} e_\psi(P) = \deg(\psi).$$

2.5 Divisors

The divisor group of a curve C, denoted by $\mathrm{Div}(C)$, is the free abelian group generated by the points of C. Thus a divisor $D \in \mathrm{Div}(C)$ is a formal sum $D = \sum_{P \in C} n_P(P)$, where $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many $P \in C$. The degree of D is defined by $\deg D = \sum_{P\ inC} n_p$. The divisors of degree 0 form a subgroup of $\mathrm{Div}(C)$ which we denote by $\mathrm{Div}^0(C)$.

Assume now that C is smooth and let $f \in \overline{K}(C)^*$. Then we can associate to f the divisor $\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f)(P)$. Then $\mathrm{div}(f) = 0$ if and only if $f \in \overline{K}^*$ and $\deg(\mathrm{div}(f)) = 0$.

A divisor $D \in \mathrm{Div}(C)$ is principal if it has the form $D =$div (f) for some $f \in \overline{K}(C)^*$. Two divisors are linearly equivalent, written $D_1 \sim D_2$, if $D_1 - D_2$ is principal. The divisor class group (or Picard group) of C, denoted $\mathrm{Pic}(C)$, is the quatient of $\mathrm{Div}(C)$ by its subgroup of principal divisors. We define the degree-0 part of the Picard group of C, denoted $\mathrm{Pic}^0(C)$, to be the quotient of $\mathrm{Div}^0(C)$ by the subgroup of principal divisors.

Let $\psi : C_1 \to C_2$ be a nonconstant map of smooth curves. We define maps of divisor groups as

$$\begin{aligned} \psi^* :\ \mathrm{Div}(C_2) &\to \mathrm{Div}(C_1), \\ (Q) &\mapsto \sum_{P \in \psi^{-1}(Q)} e_\psi(P)(P), \end{aligned} \qquad \begin{aligned} \psi_* :\ \mathrm{Div}(C_1) &\to \mathrm{Div}(C_2), \\ (P) &\mapsto (\psi P), \end{aligned}$$

and extend $\mathbb{Z}$-linearly to arbitrary divisors.

Let C be a curve. The space of differential forms on C, denoted by Ω_C, is the $\overline{K}$-vector space generated by symbols of the form dx for $x \in \overline{K}(C)$, subject to the usual relations:

$$\begin{aligned} &(i) \quad d(x+y) = dx + dy && \text{for all } x, y \in \overline{K}(C). \\ &(ii) \quad d(xy) = xdy + ydx && \text{for all } x, y \in \overline{K}(C). \\ &(iii) \quad da = 0 && \text{for all } a \in \overline{K}. \end{aligned}$$

The following is proposition 4.3 of chapter II in Silverman [29]

Proposition 2.1. *Let C be a curve, let $P \in C$, and let $t \in \overline{K}(C)$ be a uniformizer at P.*

a For every $\omega \in \Omega_C$ there exists a unique function $g \in \overline{K}(C)$, depending on ω and t, satisfying $\omega = gdt$. We denote g by ω/dt.

b Let $f \in \overline{K}(C)$ be regular at P. Then df/dt is also regular at P.

c Let $\omega \in \Omega_C$ with $\omega \neq 0$. The quantity $ord_P(\omega/dt)$ depends only on ω and P, independent of the choice of uniformizer t. We call this value the order of ω at P and denote it by $ord_P(\omega)$.

d Let $x, f \in \overline{K}(C)$ with $x(P) = 0$, and let $p =$ char K. Then

$$\begin{aligned} &ord_P(fdx) = ord_P(f) + ord_P(x) - 1 && \text{if } p = 0 \text{ or } p \nmid ord_P(x) \\ &ord_P(fdx) \geq ord_P(f) + ord_P(x) && \text{if } p > 0 \text{ and } p \mid ord_P(x). \end{aligned}$$

e Let $\omega \in \Omega_C$ with $\omega \neq 0$. Then $ord_P(\omega) = 0$ for all but finitely many $P \in C$.

Let $\omega \in \Omega_C$. The divisor associated to ω is

$$\mathrm{div}(\omega) = \sum_{P \in C} \mathrm{ord}_P(\omega)(P) \in \mathrm{Div}(C).$$

Then ω is regular if $\mathrm{ord}_P(\omega) \geq 0$ for all $P \in C$ and it is nonvanishing if $\mathrm{ord}_P(\omega) \leq 0$ for all $P \in C$. The canonical divisor class on C is the image in $\mathrm{Pic}(C)$ of $\mathrm{div}(\omega)$ for any nonzero $\omega \in \Omega_C$. Any divisor in this divisor class is called a canonical divisor.

A divisor $D = \sum n_P(P)$ is positive (or effective), denoted by $D \geq 0$, if $n_P \geq 0$ for every $P \in C$. Similarly, for any two divisors $D_1, D_2 \in \mathrm{Div}(C)$ we write $D_1 \geq D_2$ if $D_1 - D_2$ is positive. We associate to D the set of functions

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

The set $\mathcal{L}(D)$, which we call the Riemann-Roch space of D, is a finite-dimensional $\overline{K}$-vector space and we denote its dimension by $l(d) = \dim_{\overline{K}} \mathcal{L}(D)$. If $\deg D < 0$, then $\mathcal{L}(D) = \{0\}$ and $l(D) = 0$. If $D' \in \mathrm{Div}(C)$ is leanrly equivalent to D, then $\mathcal{L}(D) \cong \mathcal{L}(D')$.

The next theorem states a fundamental result in the algebraic geometry of curves.

Theorem 2.1. *(Riemann-Roch) Let C by a smooth curve and let K_C be a canonical divisor on C. There is an integer $g \geq 0$, called the genus of C, such that for every divisor $D \in Div(C)$),*

$$l(D) - l(K_C - D) = \deg D - g + 1.$$

Corollary 2.1. *(a) $l(K_C) = g$*

(b) $\deg K_C = 2g - 2$.

(c) If $\deg D > 2g - 2$, then $l(D) = \deg D - g + 1$.

3 Units and Jacobians

In this section the main subject of the thesis will be explained, which is to find a certain unit group, as well as Jacobians of curves, which are an important tool in our study of units.

3.1 Units

Let K be a field, $\overline{K}$ a separable closure of K and let V be a variety defined over K. The ring of regular functions on V defined over $\overline{K}$ is denoted by $\mathcal{O}(V)$ and when the functions are restricted to the K-rational points of V we denote it by $\mathcal{O}(V_K)$. We are interested in the group of units of $\mathcal{O}(V_K)$, which is $\mathcal{O}(V_K)^*$, in the case that V is an algebraic curve. The units are invertible regular functions on V, so they cannot have any zeros and poles. If V is a projective variety in $\mathbb{P}^n$, then by theorem I.3.4 in [5] we have that $\mathcal{O}(V) \equiv \overline{K}$ and thus $\mathcal{O}(V)^* \equiv \overline{K}^*$. If we restrict the regular functions on V to only the regular functions on $V(K)$, then we still have that $\mathcal{O}(V_K) \equiv K$. This matches the intuitive notion that on a projective variety, if a function has no zeros and no poles, then it has to be a nonzero constant.

From now on we assume that V is an affine curve in $\mathbb{A}^2$ and we will also assume that V is smooth. Then by theorem I.3.2 in [5] we have that $\mathcal{O}(V) \equiv \overline{K}[V]$ where $\overline{K}[V]$ is the coordinate ring of V. In particular, $\mathcal{O}(V_K) \equiv K[V]$ which follows from [29] exercise I 1.12(a) which says that $K[V] = \{f \in \overline{K}[V] : f = f^\sigma \text{ for all } \sigma \in Gal(\overline{K}/K)\}$. Thus, we want to study $K[V]^*$. Note that at least $K^* \subseteq K[V]^*$. We will usually take $K = \mathbb{Q}$ or $K = \mathbb{F}_q$ for q a power of some prime.

Let $f \in K[x, y]$ be an absolutely irreducible polynomial such that $V = Z(f)$. By Corollaries I 6.11 and 6.11 in [5] there is a unique nonsingular projective curve $\tilde{V}$ such that V and $\tilde{V}$ are birationally equivalent. We call $\tilde{V}$ the projective completion of V and it holds that $K(V) \cong K(\tilde{V})$. Let $g \in K[V] \setminus \{0\}$, then there is a corresponding $\tilde{g} \in \overline{K}(\tilde{V})^*$. We know that $\operatorname{div}(\tilde{g}) = 0$ and as $K[V] = K[x, y]/(f)$, we also know that g has no poles in V. Thus, the poles of g must be at the points of $\tilde{V} \setminus V$. Now, if $g \in K[V]^*$, then there is an $h \in K[V]^*$ such that $g \cdot h = 1$. Thus, g also cannot have any zeros in V. However, if $g \notin K$, then g must have some zeros and poles. As they are not in V, they must be in $\tilde{V} \setminus V$.

Another way to see this is as follows. Suppose $g \in K[V]^*$ and let $\operatorname{div}(g) = \sum_{P \in V} \operatorname{ord}_P(g)(P) + \sum_{P \in \tilde{V} \setminus V} \operatorname{ord}_P(g)(P)$. Let $D(g) := \sum_{P \in V} \operatorname{ord}_P(g)(P)$, then as $g \in K[V]$ we know that $D(g)$ is an effective divisor. As $1/g$ is also in $K[V]$ we have that $D(\frac{1}{g})$ is also effective. But $D(g) = -D(\frac{1}{g})$, so we must have that $D(g) = 0$. This means that g only has zeros and poles at the points of $\tilde{V} \setminus V$. The points of $\tilde{V} \setminus V$ are the points at infinity of V. With this we have proven the following lemma.

Lemma 3.1. *A unit $g \in K[V]^*$ must have all its zeros and poles at the points of $\tilde{V} \setminus V$, i.e. at the points at infinity.*

As $K(V) \cong K(\tilde{V})$ it must hold that $\tilde{V} \setminus V$ is finite. This allows us to say something about the size of $K[V]^*$. Firstly, $K[V]^* = \{g \in K[V] : \operatorname{div}(g) = \sum_{P \in \tilde{V} \setminus V} n_P(P) \text{ for certain } n_P \in \mathbb{Z}\}$. Secondly, suppose that $P_1, \cdots, P_m$ are the points at infinity, then any K-linear combination of them gives rise to a possible unit of $K[V]$ as long as the degree of the corresponding divisor is zero. Because of this restriction, the P_i's generate a free abelian group of rank $m-1$ and not m.

If we have found $m-1$ units $g_1, \cdots, g_{m-1}$ that correspond to $m-1$ linearly independent combinations of the $P_1, \cdots, P_m$, then all units can be found. In this case $K[V]^* = K\cdot < g_1 > \cdot \ldots \cdot < g_m >$. In general, we have the following.

Lemma 3.2. *Let m be the number of points at infinity of V, then there is an integer $0 \leq r < m$ and units $g_1, \cdots, g_r \in K[V]^* \setminus K^*$ such that $div(g_1)$, $\cdots$, $div(g_r)$ are linearly independent. In particular, if $m = 1$, then $K[V]^* = K^*$.*

The maximum r for which the lemma holds is called the rank of $K[V]^*$. If it is zero, then $K[V]^* = K^*$, and if it is a positive integer r, then there are units $g_1, \cdots, g_r \in K[V]^* \setminus K^*$ such that $K[V]^* = K\cdot < g_1 > \cdot \ldots \cdot < g_r >$. We now give a few examples.

Example 3.1. *Let K be a field of characteristic not 2 or 3 and let E be an elliptic curve given by a Weierstrass equation $y^2 = x^3 + ax + b$. Then $\tilde{E} \subset \mathbb{P}^2$ is given by the equation $y^2z = x^3 + axz^2 + bz^3$ and $\tilde{E} \setminus E = \{(0:1:0)\}$. As there is only point at infinity we have that $K[E]^* = K^*$.*

Example 3.2. *Let K be a field of characteristic not 2 and let Y be the curve given by $x^2 - y^2 = 1$ over K. Then $\tilde{Y} \subset \mathbb{P}^2$ is given by $x^2 - y^2 = z^2$ and $\tilde{Y} \setminus Y = \{(1:\pm 1:0)\}$. As there are two points at infinity, the rank of $K[Y]^*$ is either 1 or 0. From the equation of Y we see that $(x+y)(x-y) = 1$ and thus $x \pm y$ are units. From $div(x-y) = (1:1:0) - (1:-1:0)$ we see that $K[Y]^* = K^*\cdot < x - y >$.*

Example 3.3. *Let K be a field of characteristic not 2 and let X be the curve given by $x^2 + y^2 = 1$ over K. Then $\tilde{X} \subset \mathbb{P}^2$ is given by $x^2 + y^2 = z^2$ and $\tilde{X} \setminus X = \{(1:\pm i:0)\}$ where i is a root of $x^2 + 1 \in K[x]$. If i is contained in K, then there are two points at infinity, and it can be shown that $K[X]^* = K^*\cdot < x + iy >$. If K does not contain i, then $(1:\pm i:0)$ do not lie over K and thus $K[X]^* = K^*$. However, over $K(i)$ it does again hold that $K(i)[X]^* = K(i)^*\cdot < x + iy >$.*

The fact that $K[V]^* \cong K^* \times \mathbb{Z}^r$ makes it analogous to the unit ring in the case of number rings, see [30] for lecture notes on number theory. Let R be a number ring in a number field L, then $R^* \equiv M \times \mathbb{Z}^r$ where M is the group of roots of unity in R. For more on analogous results between number fields and function fields, see [21] by F. Oort. There is also the following very useful theorem from there.

Theorem 3.1. *Let K be a finite field and let C be a curve over K with m points at infinity. Then $rank(K[C]^*) = m - 1$.*

3.2 Jacobians

We have just seen that the units are those functions on the curve with all their zeros and poles at the points at infinity. This can also be turned around: when is a divisor whose support is a subset of the points at infinity a principal divisor. This leads to the notion of the Jacobian of a projective algebraic curve C. From section 1, the principal divisors form a subgroup $\mathcal{P}$ of the degree 0 divisors $\mathrm{Div}^0(C)$, and the degree-0 part of the Picard group of C is $\mathrm{Pic}^0(C) = \mathrm{Div}^0(C)/\mathcal{P}$. The Jacobian of C, which we denote by $J(C)$, is defined as $\mathrm{Pic}^0(C)$ with the structure of an algebraic variety on it. For details, see [19] by Mumford where this is done over the field of complex numbers or [17] chapter 3. In fact, $J(C)$ is an abelian variety of dimension equal to the genus g of C.

Definition 3.1. *An abelian variety X over a field K is a projective algebraic variety that is also an algebraic group, i.e. it has a group law that can be defined by morphisms.*

Note that abelian varieties are always smooth, see [18] Chapter 11. So $J(C)$ is a smooth projective variety with a group law where the addition and inverse mappings are morphisms. We define the Jacobian of C over L for a field extension $K \subset L \subset \overline{K}$, denoted by $J(C)(L)$, as the subgroup of $J(C)$ fixed by $\mathrm{Gal}(\overline{K}/L)$. Then $J(C)(L)$ is again an abelian variety. We would like that $J(C)(L)$ is equal to $\mathrm{Div}^0(C_L)$ modulo the principal divisors defined over L. This doesn't hold in general, but it holds at least if $C(L) \neq \emptyset$. For the grouplaw on an abelian variety there is the following proposition from Chapter 1, corollary 1.4 in [17].

Proposition 3.1. *The group structure on an abelian variety is commutative.*

This is not always true for affine algebraic varieties that are algebraic groups. For example $\{(a_{ij}) \in \mathbb{A}^{n^2} : \det(a_{ij}) = 1\}$ is a smooth affine variety with a grouplaw that is defined by morphisms, but which is not commutative.

With the Jacobian defined it can be used to find units as follows: consider a divisor $D = \sum_{P \in \tilde{C} \setminus C} n_P(P)$ then the question is if D is congruent to the 0 divisor class in $J(C)$. A slightly different question is if D is of finite order in $J(C)$. We define $J(C)_{tors}$ as the torsion subgroup of $J(C)$, the subgroup of $J(C)$ consisting of all points of finite order. The question is then if $nD \in J(C)_{tors}$ for some nonzero integer n. For computations we will use the computer package Magma.

If K is a finite field, then there are only finitely many degree 0 divisors of C defined over K. Hence, $J(C)(K)$ is also finite and thus any divisor class in it is of finite order. The number of elements of $J(C)(K)$ is called the classnumber of C over K.

While we are interested mostly in the units for curves over $\mathbb{Q}$, we can use the reduction modulo primes to find units or to show that no units exist. We first have the following result.

Lemma 3.3. *Let $C/\mathbb{Q}$ be an algebraic curve and let p be a prime. If C has good reduction modulo p, then the Jacobian of C has good reduction modulo p as well.*

Also, the map $J(C)(\mathbb{Q}) \to \bar{J}(C)(\mathbb{F}_p)$ by 'taking mod p' is a homomorphism. For $p \geq 3$ even more holds.

Lemma 3.4. *Let p be an odd prime and suppose that $C/\mathbb{Q}$ has good reduction modulo p. Then, the 'mod p homomorphism' $J(C)(\mathbb{Q})_{tors} \to J(C)(\mathbb{F}_p)$ is injective.*

This follows from lemma 1 in [31]. Now suppose $[\sum_{P \in \tilde{C} \setminus C} n_P(P)] \in J(C)(\mathbb{Q})_{tors}$ of order d, then mod p the order must again be d for all $p \geq 3$ such that $C \mod p$ is again smooth. As $J(C)(\mathbb{F}_p)$ is finite, this order can always be computed. We will use this observation later on for examples.

Since we are interested in torsion on the Jacobian, it would be useful to know what kind of orders can occur. Unfortunately, this is not known yet. There are some conjectures about the torsion subgroup on abelian varieties over number fields, see [28].

Conjecture 3.1. *(Torsion Conjecture for Abelian Varieties). If A is an abelian variety defined over a number field K of degree m, then $|A(K)_{tors}|$ is bounded above by a constant depending only on d and K.*

Conjecture 3.2. *(Strong Torsion Conjecture for Abelian Varieties). If A is an abelian variety defined over a number field K of degree m, then $|A(K)_{tors}|$ is bounded above by a constant depending only on d and m.*

4 Hyperelliptic Curves

In this section the necessary definitions and properties for hyperelliptic curves are given which will be required when trying to find units in the coordinate rings. From now on, all fields K are assumed to be of characteristic not 2.

4.1 Definitions

We start with the definition of a hyperelliptic curve from [5] exercise IV 1.7.

Definition 4.1. *A curve C is called hyperelliptic of genus $g \geq 2$ if there exists a finite morphism $f : C \to \mathbb{P}^1$ of degree 2.*

Let $f \in K[x]$ be a separable polynomial of degree $2g+1$ or $2g+2$ for some integer $g \geq 2$ and let $C_0 \subset \mathbb{A}^2$ be the algebraic set given by the equation $y^2 = f(x)$. As f is separable, the ideal $(y^2 - f(x))$ is prime in $K[x, y]$ and thus C_0 is an affine variety. C_0 is 1-dimensional as it is given by one polynomial equation and so C_0 is an affine curve. As f is separable we have that C_0 is smooth. Let (x, y) be a point satisfying $y^2 = f(x)$, then the partial derivatives give $2y = 0$ and $f'(x) = 0$. As f is separable it does not have any double roots. So (x, y) is smooth. We use C_0 to define a hyperelliptic curve.

Define the map $\phi : C_0 \to \mathbb{P}^{g+2}$ by $\phi(x, y) = (1 : x : x^2 : \cdots : x^{g+1} : y)$ and let C be the projective closure of $\phi(C_0)$. Then C is smooth, $C \cap \{X_0 \neq 0\} \cong C_0$ and C is a hyperelliptic curve of genus g, see also Chapter II exercise 2.14 in [29]. For a proof see Appendix A. Hyperelliptic curves given by such equations are what we are interested in. Hence from now on, all hyperelliptic curves are assumed to be defined by an affine curve of the form $y^2 = f(x)$. When we use the notation $(x, y) \in C$ for a point on C we mean the corresponding point (x, y) on C_0. The construction can also be done if f is not separable, however, the resulting curve is only hyperelliptic if f is separable as a point $(x, y) \in C$ is then smooth if and only if f is separable.

Note that if f is not separable, the equation $y^2 = f(x)$ can still define a hyperelliptic curve. Write $f = f_1 f_2$ where $f_1 \in \overline{K}[x]$ is a square polynomial and $f_2 \in \overline{K}[x]$ is a product of linear polynomials times a unit, then the coordinate transformation $x \mapsto x$, $y \mapsto \frac{y}{\sqrt{f_1}}$ gives the equation $y^2 = f_2$ and now f_2 is separable.

Example 4.1. *Consider the curve $C_0 : y^2 = x^6 + 1$ over a field K. We embed C_0 in $\mathbb{P}^4$ using the map $\phi(x, y) = (1 : x : x^2 : x^3 : y)$. Let $(u : x : v : w : y)$ be the coordinates in $\mathbb{P}^4$, then we have $v = x^2$ and $w = x^3$ when $u = 1$. Let C be the projective closure of $\phi(C_0)$, then this gives the relations $uv = x^2, uw = xv$. We also need the relation $xw = v^2$. Then $C \subset \mathbb{P}^4$ is a curve given by the equation $y^2 = w^2 + u^2$, plus the quadratic relations $uv = x^2, uw = xv$ and $xw = v^2$. Then C is birationally equivalent to the projective closure of C_0, which is given by $y^2u^4 = x^6 + u^6$, by the morphism $\psi(u : x : v : w : y) = (u : x : y)$. Hence $C \cap \{u \neq 0\}$ is isomorphic to C_0.*

The points on C but not on C_0 are the points at infinity of C_0 and they are the points with $u = 0$. From the quadratic relations this gives the points $(0 : 0 : 0 : 1 : \pm 1)$. Now we show that C is smooth. We first take the open part $(u \neq 0)$. The equations are now $f_1 = y^2 - w^2 - 1$, $f_2 = v - x^2$, $f_3 = w - xv$ and $f_4 = xw - v^2$. Then the matrix of derivatives at a point $P = (x, v, w, y)$ is

$$\begin{pmatrix} 0 & 0 & -2w & 2y \\ -2x & 1 & 0 & 0 \\ -v & -x & 1 & 0 \\ w & -2v & x & 0 \end{pmatrix}$$

This matrix always has rank 3 *as either* $w \neq 0$ *and/or* $y \neq 0$*. If* $u = 0$*, then we have the points* $(0:0:0:1:\pm 1)$*. Taking the open part* $(w \neq 0)$ *the matrix of derivatives at these two points is*

$$\begin{pmatrix} 0 & 0 & 0 & \pm 2 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

This matrix has rank 3 as well in both cases. Hence C *is a smooth curve. See Appendix A for why* C *is hyperelliptic of genus* 2*.*

Like before, we are only interested in the affine part of C, which is exactly the part that is isomorphic to the curve of the form $y^2 = f(x)$. So from now when talking about C we mean the affine part of C in $\mathbb{A}^2$, while keeping the points at infinity in mind. The coordinate ring of C is then $K[C] = K[x,y]/(y^2 - f(x)) = K[x][\sqrt{f}]$, and it is an integral domain as $y^2 - f$ is irreducible. We will sometimes write y for $\sqrt{f}$ for elements of $K[C]$. We want to study $K[C]^*$.

4.2 The Unit Group

For $K[C]^*$ it is obvious that $K^* \subset K[C]^*$. We want to at least find out if and/or when the unit group is trivial, i.e. $K[C]^* = K^*$, and we want to describe examples. The rest of this section will be used to determine what $K[C]^*$ looks like while in the next section examples and specific methods for finding units will be given.

For $d \in \mathbb{Z}$ a nonsquare we know that in $\mathbb{Z}[\sqrt{d}]$ we can define a norm $N : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}$ defined as $N(a+b\sqrt{d}) = a^2 - db^2$ such that $a+b\sqrt{d}$ is a unit if and only if $N(a+b\sqrt{d}) = \pm 1$. The situation we have is similar to this, except now we have polynomials instead of integers. However, this does not change anything to the result. Thus, we define $N : K[C] \to K[x]$ by $N(a + b\sqrt{f}) = a^2 - fb^2$ where $a, b \in K[x]$. Then N satisfies $N(\alpha\beta) = N(\alpha) \cdot N(\beta)$ for all $\alpha, \beta \in K[C]$.

Lemma 4.1. *Let* C/K *be a hyperelliptic curve defined by* $y^2 = f(x)$*, then* $a + b\sqrt{f} \in K[C]$ *is a unit if and only if* $N(a + b\sqrt{f}) \in K[x]^* = K^*$*.*

The proof is the same as for the number ring $\mathbb{Z}[\sqrt{d}]$, but we present it here quickly.

Proof. Suppose that $N(a+b\sqrt{f}) = c \in K^*$, then $(a+b\sqrt{f})\cdot(a-b\sqrt{f}) = c$ and so $c^{-1}(a-b\sqrt{f})$ is the inverse of $a + b\sqrt{f}$. Now suppose that $\alpha \in K[C]^*$, then there is a β such that $\alpha\beta = 1$. Then $N(\alpha) \cdot N(\beta) = N(\alpha\beta) = N(1) = 1$ and $N(\alpha), N(\beta) \in K[x]$. This is only possible if in fact $N(\alpha), N(\beta) \in K^*$. □

Thus we have that $K[C]^* = \{a + b\sqrt{f} : a, b \in K[x], a^2 - fb^2 \in K^*\}$. There are two cases where we can immediately see that the unit group is trivial.

Proposition 4.1. *Let* C/K *be a hyperelliptic curve given by* $y^2 = f(x)$*, then* $K[C]^* = K^*$ *if* f *has odd degree or if the leading coefficient of* f *is not a square in* K*.*

Proof. Suppose that f has odd degree and let $a + by \in K[C]^*$. If $b \neq 0$, then fb^2 will have odd degree as well, while a^2 always has even degree. Hence $a^2 - fb^2$ will then always be a nonconstant polynomial. Hence, we require that $b = 0$. But then $a^2 - fb^2 = a^2 \in K^*$ gives that $a \in K^*$. Thus $K[C]^* = K^*$.

Now suppose that f has even degree and that the leading coefficient of f is not a square in K. Let $a + by \in K[C]^*$ again, then $a^2 - fb^2 = c$ for some $c \in K^*$. This means that a^2 and fb^2 must have the same degree if $b \neq 0$. Let a_0, b_0, f_0 be the nonzero leading coefficients of a, b, f respectively, then the leading coefficient of $a^2 - fb^2$ is $a_0^2 - f_0 b_0^2$. As $a^2 - fb^2 \in K^*$ it is required that $a_0^2 - f_0 b_0^2 = 0$, or equivalently that $a_0^2 = f_0 b_0^2$. However, we assumed that f_0 is not a square in K and thus this is only possible if $a_0 = b_0 = 0$. This gives a contradiction as a_0 and b_0 were nonzero. Hence, it is again required that $b = 0$ and thus $K[C]^* = K^*$. □

So assume that the degree of f is even, thus it is equal to $2g + 2$ for some g, and that the leading coefficient a is a square in K. By dividing both sides of the equation $y^2 = f(x)$ by a and using the change of variables $y \mapsto \frac{y}{\sqrt{a}}$ for some square root of a one can assume that f is monic. We now use the results from the previous section. We know that a unit $a + b\sqrt{f}$ must have all its zeros and poles at the points at infinity by lemma 3.1. In Appendix A it is shown that there are two points on the hyperelliptic curve C that are not on the affine part C_0. These can be identified with the points $(0 : \cdots : 0 : 1 : \pm a) \in C \subset \mathbb{P}^{g+2}$. So C has two points at infinity, which we will denote by ∞^+ and ∞^-. Thus, for the affine points we will still work with the curve $C_0 = Z(y^2 - f(x))$, but when we talk about the points at infinity we mean ∞^+ and ∞^-.

There is also another way to see what the points at infinity are. We use the coordinate transformation $\xi = 1/x$ and $\eta = \frac{y}{x^{g+1}}$. This gives the curve C_1 with equation $\eta^2 = f^*(\xi)$ where f^* is the reciprocal of f. If we now glue C_0 en C_1 together using this coordinate transformation we get the hyperelliptic curve C. Let a be the leading coefficient of f, then the points at infinity correspond to $(0, \pm\sqrt{a})$ in C_1. As we assumed that a is a square in K these points do lie over K. See also Chapter II exercise 2.14 in [29]

As there is more than one point at infinity, there can be nontrivial units. As there are two such points we know by lemma 3.2 that there is one nontrivial generator if the unit group is nontrivial.

Lemma 4.2. *Let C/K be a hyperelliptic curve and suppose that $K[C]^* \neq K^*$. Let $n > 0$ be the minimal n such that there is a $\varepsilon \in K[C]^*$ with $div(\varepsilon) = n\infty^+ - n\infty^-$. Then $K[C]^* = K^* \cdot < \varepsilon >$.*

Proof. As $K[C]^* \neq K^*$ there is a $\phi \in K[C]^* \setminus K^*$ such that $\mathrm{div}(\phi) = n(\infty^+ - \infty^-)$ with $n \neq 0$. Hence, such there is a minimal $n > 0$ such that there is a $\varepsilon \in K[C]^*$ with $\mathrm{div}(\varepsilon) = n\infty^+ - n\infty^-$. Clearly $K^* \cdot < \varepsilon > \subseteq K[C]^*$.

Now suppose there is $\phi \in K[C]^*$ with $\phi \notin K^* \cdot < \varepsilon >$. It must hold that $\mathrm{div}(\phi) = m(\infty^+ - \infty^-)$ for some $m \in \mathbb{Z}$, $m \neq 0$. Write $m = qn + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < n$. If $r = 0$, then $m = qn$ and so $\mathrm{div}(\frac{\phi}{\varepsilon^q}) = 0$. This means that $\frac{\phi}{\varepsilon^q}$ is a constant and thus $\phi \in K^* \cdot < \varepsilon >$. If $r \neq 0$, then $\mathrm{div}(\frac{\phi}{\varepsilon^q}) = r(\infty^+ - \infty^-)$. As $0 < r < n$ this gives a contradiction as we assumed that n was minimal. Thus $r = 0$ and $K[C]^* \subseteq K^* \cdot < \varepsilon >$. This proves the lemma. □

Thus, if the unit group is nontrivial, we get

$$\begin{aligned} K[C]^* &= \{a + b\sqrt{f} : a, b \in K[x], a^2 - fb^2 \in K^*\} \\ &= \{\phi \in K[C] : \mathrm{div}(\phi) = n(\infty^+) - n(\infty^-) \text{ for some } n \in \mathbb{Z}\} \\ &= K^* \cdot < \varepsilon > . \end{aligned}$$

The generator of $K[C]^*/K^*$ is called a fundamental unit and it is denoted by ε. Note that this means that $K[C]^*/K^*$ is an infinite cyclic group. We can write $\varepsilon = h_1 + yh_2$ for certain $h_1, h_2 \in K[x]$. Obviously ε is not unique, as it is invariant under multiplication by K^*. As such we can assume that either h_1 or h_2 is monic. When $K = \mathbb{Q}$, we can instead assume that $h_1 \in \mathbb{Z}[x]$ with positive leading coefficient and that the gcd of all coefficients is 1 instead of h_1 being monic. Also, as $\varepsilon^{-1} = c(h_1 - yh_2)$ for some nonzero constant c we can always assume that the leading coefficients of h_1 and h_2 are positive.

For the existence of nontrivial units there is also the following lemma.

Lemma 4.3. *Let C/K be a hyperelliptic curve given by $y^2 = f(x)$. If $K[C]^* \neq K^*$, then there is a nontrivial $\phi \in K[C]^*$ such that $N(\phi) = 1$.*

Proof. Let ε be a fundamental unit. If $N(\varepsilon)$ is a square in K, then $\frac{\varepsilon}{\sqrt{N(\varepsilon)}}$ has norm 1. If $N(\varepsilon)$ is not a square in K, then $\frac{\varepsilon^2}{N(\varepsilon)}$ has norm 1. □

Thus for the existence of nontrivial units, it is enough to look for functions whose norm is either a square or equal to 1.

There are some properties of ε that are easy to show. For the proofs of these results we will need to know what the Riemann-Roch space of $d(\infty^+ + \infty^-)$ is. We explain this first and then give the results. Let $D \in Div(C)$. Recall from section 2 that the Riemann-Roch space of D is $\mathcal{L}(D) = \{f \in \overline{K}(C)^* : div(f) \geq -D\} \cup \{0\}$ with dimension $l(D) = \dim_{\overline{K}}(\mathcal{L}(D))$ and that $\mathrm{div}(f) \geq -D$ means that $\mathrm{div}(f) + D$ is effective. Write $D_\infty = \infty^+ + \infty^-$, then we need to know what $\mathcal{L}(dD_\infty)$ is.

From the definition, it consists of all functions with a pole of order at most d at ∞^+ and/or ∞^-. Clearly, the functions x and y have only poles at the points at infinity, but we need to know the orders. Let C be given by $y^2 = f(x)$ where f has degree $2g + 2$. Then the function x has a zero at $(0, \pm\sqrt{a_0})$ where a_0 is the constant coefficient of f. If $a_0 \neq 0$, the order at each zero is 1, and otherwise the order is 2 at $(0, 0)$. As $\deg(\mathrm{div}(x)) = 0$ we must have $\mathrm{div}(x) = (0, \sqrt{a_0}) + (0, -\sqrt{a_0}) - \infty^+ - \infty^-$.

For the function y there is a zero at each root of f. As f is squarefree, the order at each root must be 1. Let $f = \prod_{i=1}^{2g+2}(x - \alpha_i)$ with $\alpha_i \in \overline{K}$, then $\mathrm{div}(y) = \sum_{i=1}^{2g+2}(0, \alpha_i) - (g + 1)\infty^+ - (g + 1)\infty^-$.

By corollary 2.1 it follows that if $d \geq g$, then $l(dD_\infty) = 2d - g + 1$. If $d > g$ a basis is given by $1, x, \cdots, x^d, y, \cdots, x^{d-g-1}y$ as each of these functions are in $\mathcal{L}(dD_\infty)$ and they are all linearly independent. If $d \leq g$, then $y \notin \mathcal{L}(dD_\infty)$ and thus a basis is given by $1, x, \cdots, x^d$.

Proposition 4.2. *Let C/K be a hyperelliptic curve of genus g of characteristic not 2 defined by $y^2 = f$ where $f \in K[x]$ is of degree $2g+2$. Suppose that $\varepsilon = h_1 + yh_2$ is a fundamental unit and let $d > g$ be the order of $\infty^+ - \infty^-$ in $J(C)$, then $deg(h_1) = d$ and $deg(h_2) = d - g - 1$.*

Proof. Assume that $\mathrm{div}(\varepsilon) = d\infty^+ - d\infty^-$. Let $D_\infty = \infty^+ + \infty^-$, then $\mathrm{div}(\varepsilon) = 2d\infty^+ - dD_\infty$. Hence $\varepsilon \in \mathcal{L}(dD_\infty)$ and $\varepsilon \notin \mathcal{L}(mD_\infty)$ for any $m < d$ as $\mathrm{div}(\varepsilon)$ has exact order d. Now $\mathcal{L}(dD_\infty)$

is generated by $1, x, \cdots, x^d, y, \cdots, x^{d-g-1}y$ and thus ε is a combination of these. As ε is not in $\mathcal{L}((d-1)D_\infty)$ it is not a combination of $1, x, \cdots, x^{d-1}, y, \cdots, y^{d-g-2}$. Hence $\deg(h_1) = d$ or $\deg(h_2) = d - g - 1$. As $h_1^2 - fh_2^2 \in K^*$ it follows that h_1^2 and fh_2^2 must have the same degree. It follows that both $\deg(h_1) = d$ and $\deg(h_2) = d - g - 1$. □

The proposition only gives information if $d > g$. The next lemma shows that $d \leq g$ is not possible.

Lemma 4.4. *Let C/K be a hyperelliptic curve of genus g given by $y^2 = f$ where f is of degree $2g + 2$, then for all integers $d < g + 1$ it holds that $\infty^+ - \infty^-$ cannot be a d-torsion point of $J(C)$.*

Proof. Suppose that ε is a fundamental unit of $K[C]^*$ with $\operatorname{div}(\varepsilon) = d(\infty^+ - \infty^-)$ for some $d \leq g$. Then $\varepsilon \in \mathcal{L}(dD_\infty)$. As $d \leq g$ we know that $\mathcal{L}(dD_\infty)$ is generated by $1, x, \cdots, x^d$ and thus ε is a combination of these. Hence $\varepsilon = h_1$ for some $h_1 \in K[x]$. But then $N(\varepsilon) = h_1^2 \notin K^*$ unless $h_1 \in K^*$. Hence $\operatorname{div}(\varepsilon) = d(\infty^+ - \infty^-)$ with $d \leq g$ is not possible and thus $\infty^+ - \infty^-$ cannot have order less than $g + 1$ in $J(C)$. □

Thus the order of $\infty^+ - \infty^-$ is at least $g + 1$. For every genus there are also hyperelliptic curves where $\infty^+ - \infty^-$ has order $g+1$. For example, suppose $f = h^2 - 1$ for some polynomial $h \in K[x]$ of degree $g + 1$, with $\gcd(h^2 - 1, h') = 1$ to ensure the separability, then $h + y$ is a unit as $(h + y)(h - y) = h^2 - f = 1$. From proposition 4.2 it follows that $\operatorname{div}(h + y) = (g + 1)(\infty^+ - \infty^-)$. Something similar holds in general.

Corollary 4.1. *Let C/K be a hyperelliptic curve of genus g given by $y^2 = f(x)$ where $f \in K[x]$ is separable and of degree $2g + 2$. Then $\infty^+ - \infty^-$ has order $g + 1$ in $J(C)$ if and only if $f = h^2 - c$ for some $h \in K[x]$ and $c \in K^*$.*

Proof. First suppose that $\infty^+ - \infty^-$ has order $g + 1$ in $J(C)$. Let ε be a fundamental unit, then as $\infty^+ - \infty^-$ has order $g + 1$ it follows from proposition 4.2 that $\varepsilon = P_{g+1} + P_0 y$ where $P_{g+1}, P_0 \in K[x]$ are of degree $g + 1, 0$ respectively. By dividing ε by P_0 we can assume that $\varepsilon = P_{g+1} + y$. Then $N(\varepsilon) = P_{g+1}^2 - f = c \in K^*$. Hence $f = P_{g+1}^2 - c$.

Now suppose that $f = h^2 - c$ for some $h \in K[x]$ and $c \in K^*$ with f still separable. Then $\phi = h + y$ is a unit as $N(\phi) = c$. As $\deg(\phi) = g + 1$ it follows that ϕ is a fundamental unit as $\infty^+ - \infty^-$ cannot have torsion order less than $g + 1$. Hence $\infty^+ - \infty^-$ has order $g + 1$. □

From now on we will write $\varepsilon = P_d + yP_{d-g-1}$ where $P_d, P_{d-g-1} \in K[x]$ are polynomials of degree $d, d - g - 1$ respectively.

To decide if a given function is a unit one can check if its norm is a nonzero constant or check its zeros and poles which should all be at the points at infinity.

Example 4.2. *Consider the curve C over $\mathbb{Q}$ given by $y^2 = f(x)$ where $f = x^6 + 2x^4 + x^3 + x^2 + x + 1$. The function $h = \frac{1}{2} + x + x^3 + y$ is a unit as $N(h) = (\frac{1}{2} + x + x^3)^2 - f = \frac{-3}{4}$. Now we check its zeros and poles.*

Let $(x, y) \in C$ be an affine point, then it is a zero of h if $y = -(\frac{1}{2} + x + x^3)$ and $y^2 = 1 + x + x^2 + x^3 + 2x^4 + x^6$. Squaring the first condition given $y^2 = (\frac{1}{2} + x + x^3)^2$ and hence we require $(\frac{1}{2} + x + x^3)^2 = 1 + x + x^2 + x^3 + 2x^4 + x^6$ or $1/4 = 1$, which shows that f has no zeros except a zero of multiplicity 6 at one of the points at infinity, which we can assume to be ∞^+.

For the poles we have that projectively $h = \frac{\frac{z^3}{2}+xz^2+x^3+yz^2}{z^3}$. *The poles of* h *are in the denominator and* z^3 *has a zero of multiplicity* 3 *at* ∞^+ *and* ∞^-. *Hence* $div(h) = 6\infty^+ - 3\infty^+ - 3\infty^- = 3\infty^+ - 3\infty^-$ *and thus* h *is indeed a unit.*

This example shows that while it is possible to check the zeros and poles of a function, it is much faster to just use the norm if one wants to check if a function is a unit.

Using the consequence of lemma 3.4 there is the following result.

Lemma 4.5. *Let* $C/\mathbb{Q}$ *be a hyperelliptic curve of genus* g *given by* $y^2 = f(x)$ *where* $f \in \mathbb{Z}[x]$ *has leading coefficient* a^2 *and degree* $2g+2$. *Let* p *be an odd prime with* $p \mid a$ *and* $\Delta(f)$ *is the discriminant of* f. *If* $p \nmid \Delta(f)$, *then* $\infty^+ - \infty^-$ *is not torsion in* $J(C)$.

Proof. As $p \mid a$ we have that $f \mod p$ has degree less than $2g+2$. Since $p \nmid \Delta(f)$ it follows that $f \mod p$ is separable and that $\deg(f \mod p) = \deg(f) - 1$. Hence C has good reduction at p. From lemma 3.4 it follows that if $\infty^+ - \infty^-$ would be torsion in $J(C)$, it must have the same order in $J(C)(\mathbb{F}_p)$. As $\deg(f \mod p)$ is odd we know that $\mathbb{F}_p[C]^* = \mathbb{F}_p^*$ and thus $\infty^+ - \infty^-$ is not torsion in $J(C)$. □

Proposition 4.3. *Let* $C/\mathbb{Q}$ *be a hyperelliptic curve of genus* g *given by* $y^2 = f(x)$ *where* $f \in \mathbb{Z}[x]$ *is separable and of degree* $2g+2$. *Suppose that* $\varepsilon = P_l + yP_{l-g-1}$ *is a fundamental unit of* $\mathbb{Q}[C]^*$ *for some integer* $l > g$, *of the particular form where* $P_l, P_{l-g-1} \in \mathbb{Z}[x]$ *and the greatest common divisor of all coefficients of* P_l *together with all coefficients of* P_{l-g-1} *is 1. Let* p *be an odd prime where* C *has good reduction, then* $\varepsilon \mod p$ *is a fundamental unit of* $\mathbb{F}_p[C]^*$.

Proof. Since $\varepsilon = P_l + yP_{l-g-1}$ is a fundamental unit of $\mathbb{Q}[C]^*$ it means that $\infty^+ - \infty^-$ has order l in $J(C)(\mathbb{Q})$. Let p be a prime where C has good reduction, then $\infty^+ - \infty^-$ must also have order l in $J(C)(\mathbb{F}_p)$. If $\varepsilon \mod p$ is a unit in $\mathbb{F}_p[C]$, then $\mathrm{div}(\varepsilon \mod p) = al(\infty^+ - \infty^-)$ for some integer a. As the degree of P_l and P_{l-g-1} cannot increase when taken modulo p, it must be that $a = \pm 1$ or $a = 0$. Hence if $\varepsilon \in \mathbb{F}_p[C]$ is a nontrivial unit, then it is automatically a fundamental unit.

For $\varepsilon \mod p$ to be a unit, we require that $N(\varepsilon) \in \mathbb{F}_p^*$. We know that $N(\varepsilon) = P_l^2 - fP_{l-g-1}^2 = c \in \mathbb{Q}^*$. Hence, we need to show that $c \mod p \in \mathbb{F}_p^*$. Suppose that $c \equiv 0 \mod p$. For f we write $\bar{f} = f \mod p \in \mathbb{F}_p[x]$, similar with P_l and P_{l-g-1}. Then in $\mathbb{F}_p[x]$ we have that $\bar{P}_l^2 = \bar{f}\bar{P}_{l-g-1}^2$. It is not possible that $\bar{P}_l = \bar{P}_{l-g-1} = 0$ as we assumed that the greatest common divisor of all the coefficients is equal to 1. Also $\bar{f} \neq 0$ as C has good reduction at p.

Hence, both sides of $\bar{P}_l^2 = \bar{f}\bar{P}_{l-g-1}^2$ are nonzero. Thus $\bar{f} = \frac{\bar{P}_l^2}{\bar{P}_{l-g-1}^2}$ which shows that $\bar{f}$ is a square. This gives a contradiction as C has good reduction at p which means that $\bar{f}$ must be separable. Hence $(c \mod p) \in \mathbb{F}_p^*$ and thus $N(\varepsilon \mod p) = \bar{P}_l^2 - \bar{f}\bar{P}_{l-g-1}^2 \in \mathbb{F}_p^*$. This means that $\varepsilon \mod p$ is a unit. Now to show that it is nontrivial.

Let $\phi := \delta\varepsilon^2$ where $\delta = \pm 1$, then $N(\phi) = c^2$. We show that $\phi \mod p$ is a nontrivial unit in $\mathbb{F}_p[C]$, and it then follows that $\varepsilon \mod p$ is nontrivial as well. Suppose that $\phi \equiv d \mod p$ for some $d \in \mathbb{Z}$ with $p \nmid d$, then $\phi = d + pP + pyQ$ for certain $P, Q \in \mathbb{Z}[x]$. Then $N(\phi) = c^2 \equiv d^2 \mod p$. Now choose δ such that $d \equiv c \mod p$.

From $N(\phi) = c^2$ we get $p^2 f Q^2 = (pP + d - c)(pP + d + c)$. Here $pP + d - c$ and $pP + d + c$ are coprime and as $d \equiv c \mod p$ we have that $p^2 \mid (pP + d - c)$. Write $pQ = pQ_1Q_2$ such that $Q_1 \mid (pP + d - c)$ and $Q_2 \mid (pP + d + c)$. Then $pP + d = c + p^2\lambda Q_1^2 = -c + \kappa Q_2^2$ for some

$\lambda, \kappa \in \mathbb{Q}[x]$. Now $-c + \kappa Q_2^2 \equiv d \equiv a \mod p$ and thus $\kappa Q_2^2 \equiv 2a \mod p$. But this means that $\kappa, Q_2 \mod p \in \mathbb{F}_p^*$. So $\kappa \equiv k \mod p$ for some $k \in \mathbb{Z}_{\neq 0}$. For f we have that $f = \lambda\kappa$ and as $f \in \mathbb{Z}[x]$ by assumption we get that $\frac{1}{p} \nmid \lambda$ as $p \nmid \kappa$. But then $f \equiv k\lambda \mod p$. This gives a contradiction as f has good reduction modulo p and thus $f \mod p$ still has degree $2g+2$. We conclude that $\phi \mod p$ is not in $\mathbb{F}_p^*$ and thus $\varepsilon \mod p$ is a nontrivial unit in $\mathbb{F}_p[C]$. $\square$

The proposition means that for a prime p of good reduction the map $\mathbb{Q}[C]^*/\mathbb{Q}^* \to \mathbb{F}_p[C]^*/\mathbb{F}_p$ defined by $\varepsilon^n \mapsto \varepsilon^n \mod p$ is injective.

For an example, consider the curve C given by $y^2 = x^6 - 2x^5 + 3x^4 + 3x^2 + 2x + 1$ over $\mathbb{Q}$. Then $\varepsilon = x^5 - 3x^4 + 5x^3 - 3x^2 + 2x + (x^2 - 2x + 2)y$ is a fundamental unit with $\mathrm{div}(\varepsilon) = 5\infty^+ - 5\infty^-$. Then, if C has good reduction modulo p for a prime p, it holds that $\varepsilon \mod p$ is a fundamental unit of $\mathbb{F}_p[C]$.

From proposition 4.2 it follows that if ε is known, then also the order $\infty^+ - \infty^-$ in $J(C)$ is known. The other way around is also possible. If one knows the order d of $\infty^+ - \infty^-$ in the Jacobian of a genus 2 curve C given by $y^2 = f(x)$, then, from [2] by I. Boyer, ε can be found using Padé approximations, which give an approximation of a function by a rational function of a given order. This works as follows. We want to find $P_d(x)$ and $P_{d-3}(x)$ of degrees d and $d-3$ respectively, such that $P_d(x)^2 - f(x)P_{d-3}(x)^2 = c$ where $c \in \mathbb{Q}^*$. This would then imply that

$$x^6 f(\frac{1}{x}) = \frac{(x^d P_d(\frac{1}{x}))^2 - cx^{2d}}{(x^{d-3}P_{d-3}(\frac{1}{x}))^2}.$$

By Taylor expansions we then get

$$\sqrt{x^6 f(\frac{1}{x})} = \frac{x^d P_d(x)}{x^{d-3}P_{d-3}(x)} - \frac{c}{2}x^d + o(x^{2d}).$$

The Padé approximation of $\sqrt{x^6 f(\frac{1}{x})}$ of order $(d, d-3)$ then gives $x^d P_d(\frac{1}{x})$ and $x^{d-3}P_{d-3}(\frac{1}{x})$. From this it is easy to get $P_d(x)$ and $P_{d-3}(x)$ back. This also works for larger genus. Another way to find ε is to compute a basis for $\mathcal{L}(d(\infty^+ - \infty^-))$. This means that finding ε is equivalent to finding the order of $\infty^+ - \infty^-$ in $J(C)$. In the next section we will give examples and methods of finding ε for genus 2.

In the genus 1 case, where f has degree 4, over $\mathbb{Q}$, the work has already been done. In [24] Z. Scherr, using results from [32] by Webb and Yokota, gives a complete characterization of the solutions to the Pell equation $P_l^2 - fP_{l-2}^2 = 1$.

4.3 Units in Field Extensions

Here we briefly investigate how units behave in field extensions. Let L/K be a field extension and let C/K be a hyperelliptic curve of genus g given by $y^2 = f(x)$ where $f \in K[x]$ has degree $2g+2$. Firstly, if $\phi \in K[C]$ is not a unit, then it is also not a unit in $L[C]$. This follows immediately from $N(\phi) \notin K^*$, and thus $N(\phi) \notin L^*$.

For the existence of units over K we know that the leading coefficient of f has to be a square in K. In that case we can say something about the units over L.

Lemma 4.6. *Suppose that $h_1' + h_2'y \in L[C]$ is a unit, then $h_1' = bh_1$, $h_2' = bh_2$ where $h_1, h_2 \in K[x]$ and $b \in L^*$.*

For a proof see lemma 6 in [26] by Schmidt. From this, we get the following consequence about the unit groups.

Corollary 4.2. *If the leading coefficient of f is a square in K^*, then for any field extension L/K it holds that $L[C]^* \neq L^*$ if and only if $K[C]^* \neq K^*$. In addition, if $K[C]^* = K^* \cdot < \varepsilon >$, then $L[C]^* = L^* \cdot < \varepsilon >$. Conversely, if $L[C]^* = L^* \cdot < \eta >$, then $K[C]^* = K^* \cdot < b\eta >$ for some $b \in L^*$.*

Proof. If $\phi \in K[C]^*$ is nontrivial, then $N(\phi) \in K^*$. Hence, $N(\phi) \in L^*$ as well and thus $\phi \in L[C]^*$. Now suppose that $\mu \in L[C]^*$ is nontrivial, so $N(\mu) \in L^*$. From lemma 4.6 it follows that there is a $b_1 \in L^*$ such that $b_1\mu \in K[C]$. Then $N(b_1\mu) \in K[x] \cap L^* = K^*$ and thus $b\mu \in K[C]^*$. This proves the first part.

For the second part, let $\varepsilon \in K[C]$ be a fundamental unit of $K[C]^*$ and let $\eta \in L[C]$ be a fundamental unit of $L[C]^*$. Clearly, $L^* \cdot < \varepsilon > \subseteq L[C]^*$. By lemma 4.2 there is a $b \in L^*$ such that $b\eta \in K[C]^*$, which shows that $\eta \in L^* \cdot < \varepsilon >$ and thus $L[C]^* = L^* \cdot < \varepsilon >$. Conversely, we have that $K^* \cdot < b\eta > \subseteq K[C]^*$. Since ε and η are both fundamental units of $L[C]^*$ it follows that $\operatorname{div}(b\eta) = \operatorname{div}(\varepsilon)$. Hence $\varepsilon \in K^* \cdot < b\eta >$ and so $K[C]^* = K^* \cdot < b\eta >$. □

This means that if the leading coefficient of f is a square in K^*, then one only needs to look at the units over K to know the units over any field extension. If the leading coefficient is not a square in K, then $K[C]^* = K^*$. If it is a square in L/K, then there can be nontrivial units over L.

For example, consider the curve $C/\mathbb{Q}$ given by $y^2 = 2x^6 + 8x^5 + 16x^4 + 20x^3 + 14x^2 + 6x$. Now $\mathbb{Q}[C]^* = \mathbb{Q}^*$ as 2 is not a square in $\mathbb{Q}$. It is a square in $\mathbb{Q}(\sqrt{2})$ and there we find that $\varepsilon = 2x^4 + 6x^3 + 8x^2 + 6x + 1 + \sqrt{2}(x+1)y$ is a fundamental unit with $N(\varepsilon) = 1$. Note that $N(\varepsilon) \in \mathbb{Q}^*$, so in general $N(\varepsilon) \in L^* \setminus K^*$ is not true.

Finally, we have the following lemma by Schinzel [25].

Lemma 4.7. *Suppose that $f(x) \in K[x]$ is irreducible over any quadratic extension of K. Then $K[C]^* = K^*$.*

We give the proof as presented in [26] lemma 8.

Proof. Suppose that $\varepsilon = P_l + P_{l-g-1}y$ is a fundamental unit of $K[C]$ and we assume that the leading coefficient of P_l is 1. Then $N(\varepsilon) = c \in K^*$, which gives $fP_{l-g-1}^2 = P_l^2 - c = (P_l - b)(P_l + b)$ with $b^2 = c$. By assumption f is irreducible over $K(b)$ and so $f \mid (P_l - b)$ or $f \mid (P_l + b)$. Suppose that $f \mid (P_l - b)$, then $P_l - b = fQ$ with $Q \in K(b)[x]$. Then $P_{l-g-1}^2 = Q(P_l + b)$, and since $P_l - b, P_l + b$ are coprime, with leading coefficient 1, we have $Q = U^2$, $P_l + b = V^2$ with $U, V \in K(b)[x]$. Here $V^2 - fU^2 = (P_l - b) - (P_l + b) = 2b$, so that $V + Uy \in K(b)[C]$ is a nontrivial unit. By lemma 4.2 there is an $\alpha \in K(b)^*$ such that $\alpha(V + Uy) \in K[x]$. The relation $\deg(\alpha V) = \deg(V) = \frac{1}{2}\deg(P_l)$ now contradicts the fact that ε is a fundamental unit as the degree of P_l is minimal. □

So whenever f has this property, there are no nontrivial units over K and over any field extension of K.

5 Units on Hyperelliptic Curves of Genus 2

Now that some of the properties of units in the coordinate ring of hyperelliptic curves are known, one can try to find examples. In this section we do just that for the simplest hyperelliptic curves, those of genus 2. Most of the examples will be over $\mathbb{Q}$, but some will be over $\mathbb{F}_p$ for some prime p. First we have the following theorem.

Theorem 5.1. *Every genus 2 curve over a field K is isomorphic to a hyperelliptic curve of genus 2.*

For a proof see [5] page 341. The theorem tells us that after considering genus 2 hyperelliptic curves, there are no other types of genus 2 curves to consider.

So let us consider a genus 2 hyperelliptic curve C, which is given by an equation of the form $y^2 = f(x)$ where $\deg(f) = 5$ or 6 and f is separable. As we want to study $K[C]^* = \Big(K[x][y]/(y^2 - f(x))\Big)^*$ we can assume that f is of degree 6 and that the leading coefficient of f is a square in K, as by proposition 4.1 we otherwise have that $K[C]^* = K^*$. Also, if $K[C]^*$ is nontrivial, i.e. if $K[C]^* \neq K^*$, then there is a fundamental unit ε such that $K[C]^* = K^* \cdot < \varepsilon >$. We know that $K[C]^*$ is nontrivial if and only if $\infty^+ - \infty^-$ is torsion in $J(C)$. In addition, if $\infty^+ - \infty^-$ is torsion of order d, then by proposition 4.2 it holds that $\varepsilon = P_d + yP_{d-3}$ where $P_d, P_{d-3} \in K[x]$ are polynomials of degree $d, d-3$ respectively. If the order is known, then ε can be found be computing a basis for $L(d(\infty^+ - \infty^-))$. Finally, by lemma 4.4 we know that $\infty^+ - \infty^-$ cannot have torsion order 1 or 2.

Some research has been done on the size of the Jacobian of C over $\mathbb{Q}$. First, there are the conjectures 3.1 and 3.2 for the particular case of a Jacobian of a hyperelliptic curve. These are only conjectures, and thus researchers have tried to find hyperelliptic curves with a point of large order in the Jacobian. For these curves $\infty^+ - \infty^-$ does not need to have finite order, and if it does have finite order, the order need not be large. As such, we cannot always use such examples in the literature, but they do give information on what orders of $\infty^+ - \infty^-$ are possible or what orders we can expect to find.

Researchers have found examples of genus-2 curves over $\mathbb{Q}$ whose Jacobian have torsion points of order n for $1 \leq n \leq 30$, $32 \leq n \leq 36$ and $n \in \{39, 40, 45, 48, 60, 63\}$, see [3, 4, 7, 9–13, 20, 22, 23]. This fact is presented in [6] by E. Howe and in that paper he presents more examples for some known orders, but also an example of a genus-2 curve over $\mathbb{Q}$ whose Jacobian has a rational torsion point of order 70, which is the largest order discovered so far. For many of these n there are in fact infinite families of genus-2 curves with the given property. Currently, Max Kronberg is also doing research on the subject for his PhD thesis at the University of Olderburg.

Some of the examples in the literature are also examples for nontrvial units. For example in [4] there is the 1-parameter family of curves over $\mathbb{Q}$ given by $y^2 = x^6 + 2x^5 + (2t+3)x^4 + 2x^3 + (t^2+1)x^2 + 2t(1-t)x + t^2$ such that $\infty^+ - \infty^-$ has order 11 in the Jacobian. And in [12] there is the example over $\mathbb{Q}$ given by $y^2 = x^6 - 4x^5 + 10x^4 - 10x^3 + 5x^2 - 2x + 1$ where $\infty^+ - \infty^-$ has order 21 in the Jacobian.

In this section we will try to find many different l that occur as order of $\infty^+ - \infty^-$ over hyperelliptic curves and also families of hyperelliptic curves where $\infty^+ - \infty^-$ has the same

order. To do this we try different techniques. From the results in the literature we hope to find examples for many integers in the list of known integers that do occur as torsion order. However, it is highly unlikely that we will find an example for an l that is not in that list.

5.1 Examples with Magma

Using the computer package Magma the order d of $\infty^+ - \infty^-$ and a basis for $\mathcal{L}(d(\infty^+ - \infty^-))$ for a fixed curve over $\mathbb{Q}$ or over $\mathbb{F}_q$ for some prime power q can be found. The following Magma code will do this and works for any genus.

```
K:=Rationals();
//K can also be a finite field
P<x>:=PolynomialRing(K);
f:=x^6+1;
//f any separable polynomial of even degree and square leading coefficient
C:=HyperellipticCurve(f);
inf1:=C![1,1,0];
inf2:=C![1,-1,0];
//inf1 and inf2 are how Magma sees the points at infinity
d:=Order(inf1-inf2);
if d ne 0 then
D1:=Divisor(inf1);
D2:=Divisor(inf2);
D:=d*(D1-D2);
F<x,y>:=FunctionField(C);
d;
Basis(D)[1];
end if;
```

First the curve gets computed and the points at infinity are defined. The difference of these points in Magma is automatically seen as the difference of the corresponding points in the Jacobian, and the order d of it is computed. If d is finite, then the divisors of ∞^+ and ∞^- are defined and the output is the order d and a basis for the Riemann-Roch space of $d(\infty^+ - \infty^-)$, which is a fundamental unit. Note that computing the order in this way is much faster than first defining the divisors and then computing the order of their difference in the Jacobian. If the order d is not finite, which in Magma is given as 0, there is no output given. This is expected to always work, however in older versions of Magma it does not. Sometimes, the calculation of the order of $\infty^+ - \infty^-$ somehow goes wrong. What happens is that the computation in Magma gives a nonzero order, while the order is actually not finite. For example, this happens for the curve given by $y^2 = x^6 + 37x^4 + x^2 + 1$. The above Magma code gives $d = 12$ for this curve, but the Riemann-Roch space of $12(\infty^+ - \infty^-)$ is actually zero dimensional, so $12(\infty^+ - \infty^-)$ is not torsion. This got fixed in Magma version 2.20-6.

We don't know the extend of this problem in older versions, i.e. if it is possible for Magma to give a nonzero order while the actual order is a different integer or if Magma says the order is infinite while it is actually finite. If K is a finite field, then the problem should not exist as the Jacobian is then always finite and thus $\infty^+ - \infty^-$ is always torsion.

To prevent this problem in the output, one can add an additional if-statement to check if the Riemann-Roch space of $d(\infty^+ - \infty^-)$ is not 0-dimensional. Changing the last 4 lines of

the above Magma code to the following does this. However, this will not fully fix the problem if it is possible that Magma says the order is infinite while it is actually finite.

```
R:=RiemannRochSpace(D);
if Dimension(R) ne 0 then
F<x,y>:=FunctionField(C);
d;
Basis(D)[1];
end if;
end if;
```

As said, we dont know if there are any other problems in computing the order of $\infty^+ - \infty^-$ in Magma, which is why we also created different Magma codes to find out if a hyperelliptic curve has nontrivial units. These can be found in Appendix B.1 and B.2. Both methods use the consequence of lemma 3.4, which is that if $\infty^+ - \infty^-$ has finite order d in the Jacobian over $\mathbb{Q}$, then for each odd prime p of good reduction it must hold that $\infty^+ - \infty^-$ also has order d in $J(C)(\mathbb{F}_p)$.

Note that thanks to this consequence it is relatively simple to find a bound on the possible orders of $\infty^+ - \infty^-$. All that is needed is to find a prime p of good reduction and bound the number of elements of the Jacobian of the curve over $\mathbb{F}_p$. If $\infty^+ - \infty^-$ is torsion over $\mathbb{Q}$, then the order must be less than this bound. If such a bound is found, then by trying every possible order it is possible to decide if $\infty^+ - \infty^-$ is torsion or not.

The following example shows how the consequence of lemma 3.4 can be used.

Example 5.1. *For example the hyperelliptic curve C over $\mathbb{Q}$ given by $y^2 = x^6 + x^5 + x^4 + 1$ has good reduction modulo p for $p = 3, 5$. For $p = 3$, the reduced curve has the function $\varepsilon_1 = x^3 - x^2 + y$ as a fundamental unit with $div(\varepsilon_1) = 3\infty^+ - 3\infty^-$. For $p = 5$, the reduced curve has the function $\varepsilon_2 = 4x^9 + 4x^8 + 4x^7 + 3x^6 + x^5 + 4x^4 + 3x^3 + 3x^2 + 2 + (4x^6 + 2x^5 + 4x^4 + x^3 + x^2 + 1)y$ as a fundamental unit with $div(\varepsilon_2) = 9\infty^+ - 9\infty^-$. As the order of the divisor class of $\infty^+ - \infty^-$ in $J(C_{\mathbb{F}_3})$ and in $J(C_{\mathbb{F}_5})$ are different, it follows that $\mathbb{Q}[C]^* = \mathbb{Q}^*$.*

The Magma code in Appendix B.1 works by finding two primes of good reduction, computing the order of $\infty^+ - \infty^-$ in the Jacobian over the curve modulo these primes and comparing if they are the same. If they are the same order d, the dimension of $\mathcal{L}(d(\infty^+ - \infty^-))$ is checked. If it is nonzero, the output is the order d and a basis for $\mathcal{L}(d(\infty^+ - \infty^-))$. If the dimension is zero or if different orders are found modulo the primes then no output is given.

The code in Appendix B.2 works by finding a prime p of good reduction and computing the classnumber h of the curve over $\mathbb{F}_p$, which is the number of elements of the Jacobian. As the order of $\infty^+ - \infty^-$ must be a divisor of h, a for loop is used to check the dimension of $\mathcal{L}(d(\infty^+ - \infty^-))$ for each divisor d of h. As soon this dimension is nonzero the for loop is stopped and the output is the order d and a basis for $\mathcal{L}(d(\infty^+ - \infty^-))$. If for each d the dimension of $\mathcal{L}(d(\infty^+ - \infty^-))$ is zero, then no output is given.

Using these two methods on the curve given by $y^2 = x^6 + 37x^4 + x^2 + 1$ we find that $\infty^+ - \infty^-$ is not torsion. Upon inspection we find that modulo $3, 5, 7$ we have that $\infty^+ - \infty^-$ has order 3, but modulo 11 it has order 12. Both of these two methods should always work, however they are slower than computing the order of $\infty^+ - \infty^-$ directly as in the Magma code above.

To see what kind of orders occur for small coefficients, we can try it by brute forcing. For the Magma code see Appendix B.3. The code is based on direcly computing the order of $\infty^+ - \infty^-$ as it is the fastest method. The full versions of Magma that were available were all older than v2.20-6 and thus still had the above described problems. As the free version does not allow calculations long enough for the Magma code we use here, the above check of checking the dimension of the Riemann-Roch space of $d(\infty^+ - \infty^-)$ for a given order d is included in the code. So all the curves given by this brute force method do at least have nontrivial units, but it is not guaranteed that no curves were missed. In the following table we give a hyperelliptic curve for each of the orders found by the brute force method.

$f \in \mathbb{Q}[x]$	d		$f \in \mathbb{Q}[x]$	d
$x^6 - 6x^5 + 5x^4 + 10x^3 + 10x^2 + 4x - 10$	3		$x^6 - 4x^5 + 2x^4 + 9x^2 - 4x + 4$	13
$x^6 - 6x^5 + 3x^4 + 10x^3 + 7x^2 - 2x - 10$	4		$x^6 + 6x^4 - 4x^3 + 9x^2 - 4x + 4$	14
$x^6 - 6x^5 + 3x^4 - 8x^3 - 1x^2 - 10x - 7$	5		$x^6 - 4x^5 - 10x^3 - 4x + 1$	15
$x^6 - 6x^5 + 7x^4 + x^2 + 6x$	6		$x^6 - 4x^5 + 6x^4 - 2x^3 + x^2 - 2x + 1$	19
$x^6 - 6x^5 + 9x^4 - 4x^3 - 4x^2 + 4$	7		$x^6 - 6x^5 + 9x^4 - 2x^3 - 2x^2 + 1$	21
$x^6 - 4x^5 + 2x^4 + 4x^3 - x^2 + 2x + 2$	8		$4x^6 - 8x^5 + 8x^4 + 4x^3 - 7x^2 - 4x + 4$	23
$x^6 - 6x^5 + 9x^4 - 2x^3 - 6x^2 + 1$	9		$x^6 - 2x^5 - 9x^4 - 10x^3 - 3x^2 + 4x + 4$	24
$x^6 - 4x^5 + 6x^4 + 4x^3 + x^2 + 8x$	10		$x^6 - 4x^5 + 4x^4 + 6x^3 - 4x^2 + 1$	27
$x^6 - 6x^5 + 5x^4 + 8x^3 + 8x^2 + 8x + 4$	11		$x^6 - 2x^5 - 3x^4 - 8x^3 + 8x + 4$	29
$x^6 - 6x^5 + 7x^4 + 4x^3 + 7x^2 - 6x + 1$	12		$x^6 - 4x^5 + 4x^4 + 10x^3 + 4x^2 + 1$	39

Doing this brute force method with either of the other two methods we have given takes a significantly longer amount of time.

From the table we see that many integers that occur as order of a rational torsion point in the Jacobian of a genus-2 curve over $\mathbb{Q}$ also occur as order of $\infty^+ - \infty^-$ for such curves. We smallest integer of which there is no example in the table is 16. Checking the examples found in the literature we have been able to find some more examples that are interesting for us.

From [12] by Leprevost there is the curve given by $f := 36x^6 - 156x^5 + 241x^4 - 192x^3 + 102x^2 - 36x + 9$ and here $\infty^+ - \infty^-$ has order 25.

From [6] by Howe there is a curve with a rational torsion point of order 70. If we transform the curve such that it is of the form $y^2 = f(x)$ we get the curve $y^2 = 4x^6 - 12x^5 - 155x^4 + 690x^3 + 817x^2 - 7320x + 12816$ and here $\infty^+ - \infty^-$ has order 35.

The same thing can be done for the curves where the orders $33, 34$ and 36 occur, also found in [6]. This gives the curve given by $y^2 = 9x^6 + 54x^5 + 87x^4 + 30x^3 + 37x^2 - 28x + 4$ where $\infty^+ - \infty^-$ has order 33, the curve given by $y^2 = 36x^6 + 60x^5 + 25x^4 - 48x^3 - 56x^2 + 16$ where $\infty^+ - \infty^-$ has order 17 and the curve given by $y^2 = 36x^6 - 36x^5 - 3x^4 + 42x^3 - 27x^2 + 4x + 4$ where $\infty^+ - \infty^-$ has order 18. No example has been found yet for order 16.

If we use the brute force method with the modification that every hyperelliptic curve with nontrivial units that it finds is given as output, then there seems to be a pattern in when it is possible for nontrivial units to exist. This leads us to the following conjecture.

Conjecture 5.1. *Let $C/\mathbb{Q}$ be a hyperelliptic curve of genus g given by the equation $y^2 = f(x) = a^2x^{2g+2} + \sum_{i=0}^{2g+1} a_i x^i$ with $a, a_i \in \mathbb{Z}$ for each i such that f is separable. Then if $2a \nmid a_{2g+1}$ it holds that $\mathbb{Q}[C]^* = \mathbb{Q}^*$. In addition, if $2a \mid a_{2g+1}$ and $\frac{a_{2g+1}}{2a} \neq a_{2g} \mod 2$, then $\mathbb{Q}[C]^* = \mathbb{Q}^*$ as well.*

If this conjecture is proven to be true, then for the existence of nontrivial units it would be required that $f \in \mathbb{Z}[x]$ is of the form $f = a^2x^{2g+2} + 2abx^{2g+2} + (b+2c)x^{2g} + \cdots$. For elliptic curves a slight change is needed.

Conjecture 5.2. *Let $E/\mathbb{Q}$ be genus 1 curve given by $y^2 = f(x) = a^2x^4 + bx^3 + cx^2 + dx + e$ with $a, b, c, d, e \in \mathbb{Z}$ and $a \neq 0$ such that f is separable. If $2a \nmid b$ or if $2a \mid b$ and $\frac{b}{2a} \neq c \mod 2$, then $\infty^+ - \infty^-$ either has order 2 in $J(C)$ or the order is infinite. If in addition f is not of the form $h^2 - c$ for some $h \in \mathbb{Q}[x]$ and $c \in \mathbb{Q}^*$, then $\mathbb{Q}[C]^* = \mathbb{Q}^*$.*

We have not been able to prove the conjectures, but for elliptic curves we can prove a part of it. For that we will need the Nagell-Lutz theorem, see also Chapter VIII corollary 7.2 in [29].

Theorem 5.2. *Let $C/\mathbb{Q}$ be an elliptic curve with equation $y^2 = x^3 + ax^2 + bx + c$ with $a, b, c \in \mathbb{Z}$ and let Δ be the discriminant of E. Suppose that $P = (x_0, y_0) \in E(\mathbb{Q})$ is a nonzero torsion point.*
(a) $x_0, y_0 \in \mathbb{Z}$.
(b) Either $[2]P = \mathcal{O}$ or else $y_0^2 \mid \Delta$.

Lemma 5.1. *Let $C/\mathbb{Q}$ be genus 1 curve given by $y^2 = f(x) = a^2x^4 + bx^3 + cx^2 + dx + e$ with $a, b, c, d, e \in \mathbb{Z}$ and $a \neq 0$ such that f is separable. If $2 \nmid b$, then $\infty^+ - \infty^-$ is either not torsion or it has order 2 in $J(C)$.*

Proof. As the genus of C is 1 and the points at infinity are rational, since the leading coefficient of f is a square, it follows that C is elliptic and thus it is isomorphic over $\mathbb{Q}$ to an elliptic curve of the form $y^2 + h_1(x)y = h_2(x)$ where $h_1, h_2 \in \mathbb{Q}[x]$ are of degree $1, 3$ respectively and where h_2 is monic. Using Magma we find that C is isomorphic to the elliptic curve E given by

$$y^2 + \frac{b}{a^2}xy + \frac{2a^4d - a^2bc + \frac{b^3}{4}}{a^6}y = x^3 + \frac{-2a^2c + \frac{b^2}{2}}{a^4}x^2 + \frac{-4a^6e + a^4c^2 - \frac{a^2b^2c}{2} + \frac{b^4}{16}}{a^8}x. \quad (1)$$

The isomorphism $\phi : C \to E$ is given by (on the affine parts)

$$(x, y) \mapsto (2x^2 + \frac{b}{a^2}x - \frac{2}{a}y + \frac{a^2c - \frac{b^2}{4}}{a^4}, 4x^3 + \frac{2b}{a^2}x^2 - \frac{4}{a}xy + \frac{2a^2c - \frac{b^2}{2}}{a^4}x).$$

We want to know when $\infty^+ - \infty^-$ is torsion in $J(C)$. As C is elliptic we have that $J(C) \cong C \cong E \cong J(E)$. Hence, the question is when $\phi(\infty^+ - \infty^-)$ is torsion on E. Under ϕ we find that $\phi(\infty+) = (0, \frac{-2a^4d + a^2bc - \frac{b^3}{4}}{a^6})$ and $\phi(\infty^-) = \mathcal{O} \in E$. Thus, we investigate the point $P = (0, \frac{-2a^4d + a^2bc - \frac{b^3}{4}}{a^6})$. Before the Nagell-Lutz theorem can be used we need an elliptic curve given by integer coefficients and that is in the form $y^2 = h(x)$. Looking at equation 1 we see that the coefficients are not always integers. To resolve this we use the coordinate transformation $x \mapsto 4a^4x$, $y \mapsto 8a^6y$. This gives the equation

$$y^2 + 2bxy + (16a^4d - 8a^2bc + 2b^3)y = x^3 + (-8a^2c + 2b^2)x^2 + (-64a^6e + 16a^4c^2 - 8a^2b^2c + b^4)x.$$

To get this into the required form $y^2 = h(x)$ we use the coordinate transformation $\eta = y + bx + 8a^4d - 4a^2bc + b^3$. This gives that C is isomorphic to the elliptic curve $\tilde{E}$ given by

$$\eta^2 = x^3 + (-8a^2c + 3b^2)x^2 + (-64a^6e + 16a^4c + 16a^4bd - 16a^2b^2c + 3b^4)x + (8a^4d - 4a^2bc + b^3)^2$$

. Now ∞^+ corresponds to the point $\tilde{P} = (0, -8a^4d + 4a^2bc - b^3)$. Now we can use the Nagell-Lutz theorem. If $\tilde{P}$ is torsion on $\tilde{E}$ with $\mathrm{ord}(\tilde{P}) \neq 2$, then $[2]\tilde{P}$ should be a nontrivial torsion point as well and by the Nagell-Lutz theorem, its coefficients should be integers. We get

$$x([2]\tilde{P}) = \frac{k - \frac{3}{2}a^6b^4e - \frac{3}{8}a^4b^5d + \frac{1}{8}a^2b^6c - \frac{3}{256}b^8}{l + \frac{1}{4}a^4b^3d + \frac{1}{4}a^4b^2c^2 - \frac{1}{8}a^2b^4c + \frac{1}{64}b^6}$$

where $k, l \in \mathbb{Z}$ for all a, b, c, d, e. If now b is odd, then the numerator of $[2]\tilde{P}$ always has the fraction $\frac{-3}{256}b^8$ in it, while the denominator always has the fraction $\frac{1}{64}b^6$ in it. However, in the division the part $\frac{-3}{256}b^8$ can never get cancelled and so $x([2]\tilde{P}) \notin \mathbb{Z}$. Thus if b is odd the point $\tilde{P}$ can not have torsion order > 2. If it has order 2, then $\infty^+ - \infty^-$ also has order 2 in $J(C)$ and if it is not torsion, then $\infty^+ - \infty^-$ is not torsion either. □

Lemma 5.2. *Let $C/\mathbb{Q}$ be genus 1 curve given by $y^2 = f(x) = a^2x^4 + 2abx^3 + cx^2 + dx + e$ with $a, b, c, d, e \in \mathbb{Z}$ and $a \neq 0$ such that f is separable. If $c \neq b \mod 2$, then $\infty^+ - \infty^-$ is either not torsion or it has order 2 in $J(C)$.*

Proof. Like in the proof of lemma 5.1 we have that C is isomorphic to the elliptic curve E given by equation 1 but with b replaced by $2ab$. Now the coordinate transformation $x \mapsto a^2x$, $y \mapsto a^3y$ is enough to get the coefficients to be integers. As $c \neq b \mod 2$ we can assume that c is of the form $b^2 + 2u + 1$ where $u \in \mathbb{Z}$. This now gives the equation

$$y^2 + 2bxy + (2ad - 4bu - 2b)y = x^3 + (-4u - 2)x^2 + (-4a^2e + (1 + 2u)^2)x.$$

Now let $\eta = y + bx + ad - 2bu - b$, then we get the elliptic curve $\tilde{E}$ given by

$$\eta^2 = x^3 + (-4u + b - 2)x^2 + (-4a^2e + (1 + 2c)^2 + 2b(ad - 2bu - b))x + (ad - 2bu - b)^2.$$

Now C is isomorphic with $\tilde{E}$ and ∞^- corresponds to $\tilde{P} = (0, ad - 2bu - b)$. We are now in the position to use the Nagell-Lutz theorem. If $\tilde{P}$ is torsion with order > 2, then $[2]\tilde{P}$ must be a nontrivial torsion point as well. Computing $[2]\tilde{P}$ we get

$$x([2]\tilde{P}) = \frac{k + \frac{1}{4}}{l}$$

where $k, l \in \mathbb{Z}$. This means that $x([2]\tilde{P}) \notin \mathbb{Z}$ for all values of a, b, u, d, e. Hence, if $c \neq b \mod 2$, then $\tilde{P}$ either has order 2 or is not torsion and thus $\infty^+ - \infty^-$ also either has order 2 or is not torsion in $J(C)$. □

The part of conjecture 5.2 that we have not been able to prove yet is the condition that $a \mid b$. One can attempt to use the Nagell-Lutz theorem again, however the same argument does not work. If C is isomorphic to an elliptic curve E where we can use the Nagell-Lutz theorem, and if ∞^- corresponds with the point P, then for specific forms of the parameters we get $x([2]P) = \frac{k}{l}$ where both $k, l \in \mathbb{Z}$. Here it is difficult to tell if it is possible that $l \mid k$ or not. If it is possible, then the point could still not be torsion and another method would have to be used to prove it.

5.2 Continued Fractions

Another method of deciding if nontrivial units exist and finding them is by continued fractions. Continued fractions are used to solve Pell equations, which are equations of the form $P^2 - fQ^2 \in K^*$ where P, f, Q are integers or polynomials over some field K. In the integer case when f is positive and non-square there are infinitely many solutions in $\mathbb{Z}$. The polynomial case over $\mathbb{Q}$ is what we are interested in. We give a brief explanation of continued fractions and the properties that are related to finding units. For a more detailed explanation see [26]. Continued fractions were used in [24] by Z. Scherr, using results from [32], to give a complete characterization of solutions to the Pell equation over $\mathbb{Q}$ where f is of degree 4, so this gives the solution to units in elliptic curves.

Let K be a field, then the field of formal Laurent series in x over K is $K((\frac{1}{x}))$. Elements of $K((\frac{1}{x}))$ are of the form $\sum_{n \leq M} a_i x^n$ for some $M \in \mathbb{Z}$ where $a_i \in K$ for each i. Clearly we have $K[x] \subset K((\frac{1}{x}))$ as rings.

Lemma 5.3. *Let K be a field with char$(K) \neq 2$ and let $f \in K[x]$ be a monic polynomial of even degree, then there is a $g \in K((\frac{1}{x}))$ such that $g^2 = f$.*

This means that $K((\frac{1}{x}))$ contains all the square roots of monic polynomials of even degree and we denote one such square root of f as $\sqrt{f}$. We now give the continued fraction expansion of an element $g(x) = \sum_{n \leq M} a_i x^n \in K((\frac{1}{x}))$. We define $[g(x)] = \sum_{n=0}^{M} a_i x^n$ for the polynomial part of g. Set $a_0(x) = [g(x)]$ and $\alpha_0(x) = \frac{1}{g(x) - a_0(x)}$. Then for $i \geq 1$ we recursively define $a_i(x) = [\alpha_{i-1}(x)]$ and $\alpha_i(x) = \frac{1}{\alpha_{i-1}(x) - a_i(x)}$. This gives the continued fraction expansion $g(x) = [a_0(x); a_1(x), a_2(x), \cdots]$ where

$$[a_0(x); a_1(x), a_2(x), \cdots] := a_0(x) + \cfrac{1}{a_1(x) + \cfrac{1}{a_2(x) + \cfrac{1}{\ddots}}}.$$

The continued fraction expansion is called periodic if there is an $m \in \mathbb{Z}_{>0}$ such that $a_{km+i} = a_i$ for each $1 \leq i < m$ and for each $k \in \mathbb{Z}_{\geq 0}$. The integer m is then called the period of the continued fraction. The truncations of the continued fraction are denoted by $\frac{p_i(x)}{q_i(x)} = [a_0(x); a_1(x), \cdots, a_i(x)]$ and these are called the convergents of $g(x)$. The link between continued fractions and units in the coordinate ring of hyperelliptic curves is given by the following proposition, for a proof see Adams and Razar [1].

Proposition 5.1. *Let C be a hyperelliptic curve over a field K with char$(K) \neq 2$ defined by $y^2 = f(x)$ where f is monic and of even degree, then $K[C]^* \neq K^*$ if and only if the continued fraction expansion of $\sqrt{f(x)}$ is periodic.*

This links the existence of units to the periodicity of the continued fraction expansion of $\sqrt{f}$. For finding units there is the following, see Schmidt [26] for a proof.

Proposition 5.2. *Let C be a hyperelliptic curve over a field K with char$(K) \neq 2$ defined by $y^2 = f(x)$ where f is monic and of even degree. Suppose that $p(x) + yq(x) \in K[C]^*$ with $q \neq 0$, then $\frac{p(x)}{q(x)}$ is a convergent of $\sqrt{f(x)}$.*

For the fundamental unit $\varepsilon = P(x) + yQ(x)$ it must hold that $\frac{P(x)}{Q(x)} = [a_0(x); a_1(x), \cdots, a_i(x)]$ for some $i < m$ where m is the period of the continued fraction.

We give an example to illustrate the use of continued fractions. Consider the hyperelliptic curve C over $\mathbb{Q}$ given by $y^2 = x^6 + 2x^5 + x^4 + x + 1$. The function $h = x^5 + x^4 + \frac{1}{2} + x^2 y$ is a unit as $N(h) = (x^5 + x^4 + \frac{1}{2})^2 - (x^6 + 2x^5 + x^4 + x + 1) \cdot x^4 = \frac{1}{4}$. We now try to find this unit using continued fractions. The Laurent series and continued fraction expansions of $\sqrt{x^6 + 2x^5 + x^4 + x + 1}$ are

$$\begin{aligned}\sqrt{x^6 + 2x^5 + x^4 + x + 1} &= x^3 + x^2 + \frac{1}{2x^2} - \frac{1}{8x^7} + \cdots \\ &= x^3 + x^2 + \frac{1}{2x^2 + \frac{1}{2x^3 + 2x^2 + \frac{1}{2x^2 + \cdots}}}.\end{aligned}$$

We first try the function $y + x^3 + x^2$ corresponding to the resultant $[a_0(x)] = x^3 + x^2$. As $y + x^3 + x^2 = -\frac{1}{2x^2} + \cdots$ we see that $y + x^3 + x^2$ has a zero of multiplicity 2 at one of the points at infinity, say ∞^+, and a pole of multiplicity 3 at ∞^-. This follows from $\operatorname{div}(x) = (0,1) + (0,-1) - \infty^+ - \infty^-$. For the other zero we have to solve $(x^3 + x^2)^2 = x^6 + 2x^5 + x^4 + x + 1$. This gives $x + 1 = 0$. Hence $\operatorname{div}(y + x^3 + x^2) = (-1, 0) + 2\infty^+ - 3\infty^-$ and thus this is not a unit.

The next resultant is $[a_0(x); a_1(x)] = x^3 + x^2 + \frac{1}{2x^2} = \frac{x^5 + x^4 + \frac{1}{2}}{x^2}$. So the function we get is $x^5 + x^4 + \frac{1}{2} + yx^2$ and this is the same unit we had earlier.

5.3 Maps to Elliptic Curves

Some hyperelliptic curves admit a mapping to an elliptic curve. This map can be used to find torsion in the Jacobian. We explain how this goes and give an example. Let C be a hyperelliptic of genus 2 over a field K and let $\phi : C \to E$ be a non-constant map from C to an elliptic curve $(E, \mathcal{O})$. Then we can define maps of the corresponding divisor groups as follows:

$$\begin{aligned}\phi^* : \operatorname{Div}(E) &\to \operatorname{Div}(C) \\ (Q) &\mapsto \sum_{P \in \phi^{-1}(Q)} e_\phi(P)(P),\end{aligned} \qquad \begin{aligned}\phi_* : \operatorname{Div}(C) &\to \operatorname{Div}(E) \\ (P) &\mapsto \phi(P),\end{aligned}$$

and extend $\mathbb{Z}$-linearly to arbitrary divisors. By proposition 3.6 in chapter II in [29] these maps send principal divisors to principal divisors. Additionally, we can restrict ϕ_* to $\operatorname{Div}^0(C)$ and the image is then in $\operatorname{Div}^0(E)$ as $\deg(\phi_*(D)) = \deg(D)$. This then allows us to define $\phi_* : \operatorname{Pic}^0(C) \to \operatorname{Pic}^0(E)$. As $(E, \mathcal{O})$ is elliptic, we have that $\operatorname{Pic}^0(E) \cong E$ by $\sum n_i Q_i \mapsto \sum [n_i] Q_i$ with inverse $(x, y) \mapsto (x, y) - (\mathcal{O})$, see Chapter III proposition 3.4 in [29] for a proof.

Hence, we define $\phi_* : \operatorname{Pic}^0(C) \to E$ by $\phi_*(\sum n_i Q_i) = \sum [n_i](\phi(Q_i))$ and this ϕ_* sends torsion points of $\operatorname{Pic}^0(C)$ to torsion points of E. We require that $\infty^+ - \infty^-$ is torsion in $J(C) \cong \operatorname{Pic}^0(C)$ for finding units. The method we try here is by investigating when $\phi_*(\infty^+ - \infty^-)$ is torsion in E and when it is torsion we check it for $\infty^+ - \infty^-$.

For the torsion subgroup of elliptic curves over $\mathbb{Q}$ there is the following theorem by Mazur, see also [14] or [15].

Theorem 5.3. *Let E be an elliptic curve over $\mathbb{Q}$, then the torsion subgroup of E is isomorphic to $\mathbb{Z}/N\mathbb{Z}$ for $N \in \{1, \cdots, 10, 12\}$ or to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$ for $N \in \{1, 2, 3, 4\}$.*

For the torsion in the elliptic curves we will use division polynomials, see [29] page 105. As K is a field of characteristic not 2, consider an elliptic curve given by the Weierstrass equation $y^2 = x^3+a_2x^2+a_4x+a_6$ with $a_i \in K$ for all i. The division polynomials $\psi_m \in \mathbb{Z}[a_2, a_4, a_6, x, y]$ are recursively defined as

$$\begin{aligned}
\psi_1 =& 1\\
\psi_2 =& 2y\\
\psi_3 =& 3x^4 + 4a_2x^3 + 6a_4x^2 + 12a_6x + 4a_2a_6 - a_4^2\\
\psi_4 =& 2y(2x^6 + 4a_2x^5 + 10a_4x^4 + 40a_6x^3 + (40a_2a_6 - 10a_4^2)x^2\\
&+ (16a_2^2a_6 - 4a_2a_4^2 - 8a_4a_6)x + 8a_2a_4a_6 - 2a_4^3 - 16a_6^2)\\
&\vdots\\
\psi_{2m+1} =& \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \qquad \text{for } m \geq 2\\
\psi_{2m} =& \frac{\psi_m}{2y}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \qquad \text{for } m \geq 3
\end{aligned}$$

When these are considered as functions on E, the zeros of ψ_m are exactly the nontrivial m-torsion points of E, i.e. $\operatorname{div}(\psi_m) = \sum_{P\in E[m]}(P) - m^2(\mathcal{O})$. If we use that $y^2 = x^3 + a_2x^2 + a_4x + a_6$ on E, then for the division polynomials we get that $\psi_m \in \mathbb{Z}[a_2, a_4, a_6, x]$ when m is odd and that $2y\psi_m \in \mathbb{Z}[a_2, a_4, a_6, x]$ when m is even. This is how we will use them. The zeros are then the x-coordinates of the nontrivial torsion points. For examples we will use Magma to work with the division polynomials, and in Magma they are given as ψ_{2m+1} and $\psi_2\psi_{2m}$ as polynomials in $\mathbb{Z}[a_2, a_4, a_6, x]$. This is why we need the ψ_m's as polynomials in x and no y.

The maps between C and E are usually given on affine parts only, for simplicity. As such, we want the points at infinity in an affine plane. Hence, if C is given by $y^2 = f$, then we check the torsion of $(0, a) - (0, -a)$ using ϕ_* where a^2 is the leading coefficient of f. If we know the torsion here, then by the coordinate transformation $x \mapsto \frac{1}{x^6}$, $y \mapsto \frac{y}{x^3}$ we know the torsion of $\infty^+ - \infty^-$ for the curve $y^2 = \tilde{f}$ where $\tilde{f}$ is the reciprocal of f. Hence, we will check if the image of the divisor class of $(0, a) - (0, -a)$ is a zero of some ψ_n.

As an example, let C_t be the hyperelliptic curve over $\mathbb{Q}$ given by $y^2 = x^6+tx^4+1$ where t is a parameter. We give two maps maps to elliptic curves which will come from automorphisms on C_t. One automorphism σ_1 of C_t is given by $\sigma_1(x, y) = (-x, y)$. The invariant functions of C_t under σ_1 are the elements of $\mathbb{Q}(y, x^2)$. Let $\xi = x^2$, then these two generators are related by the elliptic curve $y^2 = \xi^3 + t\xi^2 + 1$, which we call E_1. A map ϕ_1 from C_t to E_1 is given by $\phi_1(x, y) := (x^2, y)$.

We do the same thing for another automorphism σ_2, namely $\sigma_2(x, y) = (-x, -y)$. The invariant functions are the elements of $\mathbb{Q}(x^2, xy)$. Let $\xi = x^2$ and $\eta = xy$, then we have the relation $\eta^2 = \xi^4 + t\xi^3 + \xi$. Dividing both sides by ξ^4 we get an elliptic curve given by $\left(\frac{\eta}{\xi^2}\right)^2 = \left(\frac{1}{\xi}\right)^3 + t\frac{1}{\xi} + 1$, and we call this curve E_2. A map ϕ_2 from C_t to E_2 is given by $(x, y) \mapsto (\frac{1}{x^2}, \frac{xy}{x^4})$.

From this we now get maps $\phi_{i*} : \operatorname{Pic}^0(C) \to E_i$ given by $\phi_{i*}(\sum n_j(P_j)) = \sum[n_j](\phi_i(P_j))$ for $i = 1, 2$. For C_t we are interested in the order of the divisor class of $(0, 1) - (0, -1)$ in the Jacobian. We use ϕ_{1*} and ϕ_{2*} for this.

We get

$$\phi_{1*}((0,1)-(0,-1)) = \phi_1(0,1) - \phi_1(0,-1) = (0,1) - (0,-1) = [2](0,1)$$
$$\phi_{2*}((0,1)-(0,-1)) = \phi_2(0,1) - \phi_2(0,-1) = \mathcal{O} - \mathcal{O} = \mathcal{O}$$

So $\phi_{2*}((0,1)-(0,-1))$ is always torsion and thus does not give any information. Hence, we can only use ϕ_{1*} and we need to find out for which values of t it holds that $[2](0,1)$ is torsion on E_1. If $(0,1)$ does not have order 2, then this is equivalent to finding when $(0,1)$ is torsion. To compute for which values of t this holds we use the division polynomials of E_1 and substitute $x = 0$ into them. For this we use the following Magma code:

```
K<t>:=FunctionField(Rationals());
E:=EllipticCurve([0,t,0,0,1]);
F<z,y>:=FunctionField(E);
for i:=2 to 12 do
psi<x>:=DivisionPolynomial(E,i);
ConstantCoefficient(psi);
end for;
```

Normally, the DivisionPolynomial command in Magma gives as output 3 polynomials, namely ψ_m, ψ_m, 1 if m is odd and $2y\psi_{2m}, \frac{\psi_{2m}}{2y}, (2y)^2$ if m is even, but when defined as a polynomial only the fist polynomial is used. The zeros of this polynomial give the x-coordinates of the torsion points. Substituting $x = 0$ into them means we just want the constant coefficient of it, so we can check for which t one of these is zero.

Let ψ_n denote the n-th division polynomial as given by Magma, then $\psi_3(0) = 4t$. So for $t = 0$ we know that $(0,1)$ is 3-torsion point of E_1. Checking on C_0 we find that $(0,1)-(0,-1)$ has order 3 in $J(C_0)$.

Next, we have $\psi_6(0) = -1024t^4 - 8192t$. The rational solutions to this are $t = 0$ and $t = -2$. Now $(0,1)$ is never a 2-torsion point as $\psi_2(0) = 4$, this tells us that $(0,1)$ is a 6-torsion point of E_1 for $t = -2$. Checking this on C_{-2} we find that $(0,1) - (0,-1)$ also has order 6 in $J(C_{-2})$.

Checking $\psi_n(0)$ for the other $n \leq 12$ we don't find any other rational solutions. Thus, only for $t = 0$ and for $t = -2$ do we have that $(0,1) - (0,-1)$ is torsion in $J(C_t)$, and so the coordinate ring of the hyperelliptic curve given by $y^2 = x^6 + tx^2 + 1$ only contains nontrivial units for $t = 0, -2$. The generators can then easily be found.

In general, if $\phi_1 : C \to E_1$ is a map from a genus 2 hyperelliptic curve C to an elliptic curve E_1, then there is always another map ϕ_2 from C to a different elliptic curve $E2$. The map $(\phi_{1*}, \phi_{2*}) : J(C) \to E_1 \times E_2$ defined as $(\sum n_i(P_i)) \mapsto (\sum[n_i](\phi_1(P_i)), \sum[n_i](\phi_2(P_i)))$ is then an isogeny, see [27]. When this occurs we say that C has split jacobian. As the map is now an isogeny, it means that when the image of a point is torsion, the point it self must be torsion as well.

Similar as to how we defined (ϕ_{1*}, ϕ_{2*}), we can define $(\phi_1^*, \phi_2^*) : E_1 \times E_2 \to J(C)$ by $(P,Q) \mapsto \phi_1^*(P) - \phi_1^*(\mathcal{O}_1) + \phi_2^*(Q) - \phi_2^*(\mathcal{O}_2)$. From the composition of the two maps we get an isogeny $\tau : J(C) \to J(C)$ defined as $(P) - (Q) \mapsto \phi_1^*(\phi_1(P)) - \phi_1^*(\phi_1(Q)) + \phi_2^*(\phi_2(P)) - \phi_2^*(\phi_2(Q))$ and extending $\mathbb{Z}$-linearly. If one knows what the kernel of τ is, then this can be used to bound the order of points in $J(C)$ for which the image under (ϕ_{1*}, ϕ_{2*}) is torsion.

We check this for the example above. We need to know what

$$\phi_i^*(\phi_i(P)) = \sum_{Q \in \phi_i^{-1}(\phi_i(P))} e_{\phi_i}(Q)(Q)$$

is for $i = 1, 2$. As both E_i come from the relations between the invariant functions of the automorphism σ_i on C, we get that $\phi_i^*(\phi_i(P)) = (P) + \sigma_i(P)$. For τ we then get

$$\tau((P) - Q))) = (P) + \sigma_1(P) - (Q) - \sigma_1(Q) + (P) + \sigma_2(P) - (Q) - \sigma_2(Q).$$

Hence $\tau = 2 + \sigma + 1 + \sigma_2$. However, in our example we had $\sigma_1(x, y) = (-x, y)$ and $\sigma_2(x, y) = (-x, -y)$ and thus $\sigma_2 = -\sigma_1$ on $J(C)$ as the hyperelliptic involution is the identity on $J(C)$. So actually, τ is multiplication by 2 and thus the kernel consists of the 2-torsion points of $J(C)$. This means that if $(\phi_{1*}, \phi_{2*})((0, 1) - (0, -1))$ is torsion with order d, then $(0, 1) - (0, -1)$ would have order d or $2d$.

5.4 Creating the Curve from Units

We now try another method of finding units. Instead of starting with the equation of the curve, we start with the function we want as a fundamental unit and try to construct the equation of the curve where the chosen function is a fundamental unit. This works as follows: Let C/K be a hyperelliptic curve of genus g given by the equation $y^2 = f(x)$ where f has degree $2g + 2$. Suppose we want the divisor $\infty^+ - \infty^-$ to have order l in $J(C)$ for some integer l. Then from proposition 4.2 the unit we start with is of the form $\varepsilon = P_l + yP_{l-g-1}$ where P_i is a degree i polynomial over K and by lemma 4.4 we can assume that $l \geq g + 1$. As ε is a unit it satisfies $P_l^2 - fP_{l-g-1}^2 = c$ for some constant $c \in K^*$. From this we see that $f = \frac{P_l^2 - c}{P_{l-g-1}^2}$. Also, we can assume that P_{l-g-1} is monic as fundamental units are invariant under multiplication by K^*.

Now as $P_l^2 - fP_{l-g-1}^2 = c$, it is required that $P_l^2 \equiv c \mod (P_{l-g-1}^2)$. Hence $c \in K^*$ is a square in $K[x]/(P_{l-g-1}^2)$. We want to know what information this gives about c in K. If $l = g + 1$, so $P_{l-g-1} = 1$, then c can be arbitrary and every c is possible: By corollary 4.1 we have $f = P_{g+1}^2 - c$. The only requirement here is that f does have to be separable. We have $f' = 2P_{g+1}P'_{g+1}$ and it is clear that f and P_{g+1} have no common zeros as $c \neq 0$. Let $\alpha_1, \cdots, \alpha_g$ be the roots of P'_{g+1} in $\mathbb{C}$, then f has a double root if $c = -P_{g+1}(\alpha_i)^2$ for some i such that $P_{g+1}(\alpha_i)^2 \in \mathbb{Q}^*$. Thus, for fixed P_{g+1} there are only finitely many c not possible.

Over $\mathbb{Q}$ we can only show the following for other l:

Lemma 5.4. *Let $P \in \mathbb{Q}[x]$ be a monic polynomial and let $c \in \mathbb{Q}^*$. Assume that P has an irreducible factor of odd degree and that c is a square in $\mathbb{Q}[x]/(P^2)$. Then c is a square in $\mathbb{Q}$.*

Proof. As c is a square in $\mathbb{Q}[x]/(P^2)$ there are $Q, R \in \mathbb{Q}[x]$ such that $Q^2 - c = RP^2$. Write $P = \prod_{i=1}^m \pi_i^{e_i}$ for the prime factorization of P with $\pi_i \neq \pi_j$ whenever $i \neq j$, then the radical of P is $\mathrm{rad}(P) = \prod_{i=1}^m \pi_i$ and we have assumed that there is a j such that $\deg(\pi_j)$ is odd. Then we have the ringhomomorphism $\phi : \mathbb{Q}[x]/(P^2) \to \mathbb{Q}[x]/rad(P)$ given by $\phi(a + (P^2)) = a + rad(P)$. As each π_i is irreducible we know that $\mathbb{Q}[x]/(\pi_i)$ is a finite field extension $K_i/\mathbb{Q}$. Using the Chinese remainder theorem we then get $\mathbb{Q}[x]/rad(P) \cong \mathbb{Q}[x]/(\pi_1) \times \cdots \times \mathbb{Q}[x]/(\pi_m) \cong K_1 \times \cdots \times K_m$.

If we now look at c, then $\phi(c) \equiv c + rad(P)$ which corresponds to $(c, \cdots, c)$ in $K_1 \times \cdots \times K_m$ since it is a constant. As $Q^2 - c \equiv 0 \mod (P^2)$ it also holds that $Q^2 - c \equiv 0 \mod rad(P)$. Hence c is also a square in $\mathbb{Q}[x]/rad(P)$ and thus $(c, \cdots, c)$ is a square in $K_1 \times \cdots \times K_m$. As $c \in \mathbb{Q}^*$ it is a unit in $\mathbb{Q}[x]/(P_{l-g-1}^2)$ and hence $(c, \cdots, c)$ is actually a square in $K_1^* \times \cdots \times K_m^*$. But then each K_i must contain a copy of $\mathbb{Q}(\sqrt{c})$. If c is a square in $\mathbb{Q}$ this does not give any restriction as then $\mathbb{Q}(\sqrt{c}) = \mathbb{Q}$. So suppose that c is not a square in $\mathbb{Q}$, then for the degree of each K_i over $\mathbb{Q}$ we have $[K_i : \mathbb{Q}] = [K_i : \mathbb{Q}(\sqrt{c})] \cdot [\mathbb{Q}(\sqrt{c}) : \mathbb{Q}] = 2[K_i : \mathbb{Q}(\sqrt{c})]$. In particular, this degree is even. Hence, each π_i must have even degree. As it was assumed that $\deg(\pi_j)$ is odd we get a contradiction. We conclude that c is a square in $\mathbb{Q}$. $\square$

In particular, this lemma holds if P is of odd degree. For the fundamental unit $\varepsilon = P_l + yP_{l-g-1}$ this tells us that when $\mathrm{rad}(P_{l-g-1})$ has an irreducible factor of odd degree, c is a square in $\mathbb{Q}^*$.

With this method of starting from ε it is required that $\frac{P_l^2 - c}{P_{l-g-1}^2}$ is a polynomial. So we actually start with P_{l-g-1} and we need to find P_l and c such that this holds. When c is a square in K, we can divide both sides of $P_l^2 - fP_{l-g-1}^2 = c$ by c to get $\left(\frac{P_l}{\sqrt{c}}\right)^2 - \frac{f}{c}P_{l-g-1}^2 = 1$. Thus we can assume that $c = 1$ in this case.

Now $\frac{P_l^2 - 1}{P_{l-g-1}^2} = \frac{(P_l+1)(P_l-1)}{P_{l-g-1}^2}$. As $P_l + 1$ and $P_l - 1$ are coprime we can write $P_{l-g-1} = Q_1 Q_2$ for coprime polynomials $Q_1, Q_2 \in K[x]$ such that $Q_1^2 \mid (P_l+1)$ and $Q_2^2 \mid (P_l-1)$, or equivalently $P_l \equiv -1 \mod (Q_1^2)$ and $P_l \equiv 1 \mod (Q_2^2)$. Note that $\deg(P_l) \geq \deg(Q_i^2)$ is required to hold for $i = 1, 2$.

Let $d_i = \deg(Q_i)$, then we can assume $d_1 \geq d_2$ as otherwise we can swap Q_1 and Q_2 which will only cause a minus sign in P_l. The possible values for the d_i are $(d_1, d_2) = (\lfloor \frac{l}{2} \rfloor, \lfloor \frac{l+1}{2} \rfloor - g - 1), \cdots, (\lfloor \frac{l-g}{2} \rfloor, \lfloor \frac{l-g-1}{2} \rfloor)$ where $\lfloor \rfloor$ is the floor function. For example, for $l = 11$ and $g = 2$ this gives $(d_1, d_2) = (5, 3), (4, 4)$, when $l = 12$ instead it is $(6, 3)$ and $(5, 4)$.

The method we use to try and find P_l is to fix l and g and take some P_{l-g-1} with parameters. Write $P_{l-g-1} = Q_1 Q_2$ such that P_l is of the form $P_l = -1 + \lambda Q_1^2$ for some $\lambda \in K[x]$ and try to solve $P_l \equiv 1 \mod (Q_2^2)$. When an irreducible factor π of P_{l-g-1} is of odd degree, all the corresponding fundamental units must satisfy the above. When $l - g - 1$ is odd this always holds. However, if $l - g - 1$ is even there could be some examples where it does not hold. In that case we need another way of finding P_l and c.

From $P_l^2 \equiv c \mod (P_{l-g-1}^2)$ we see that $P_l^2 \equiv c \mod (P_{l-g-1})$ as well. As $P_l \equiv \sum_{i=0}^{l-g-2} a_i x^i \mod (P_{l-g-1})$ for certain $a_i \in K$ we can compute $P_l^2 \equiv (\sum_{i=0}^{l-g-2} a_i x^i)^2 \mod (P_{l-g-1})$ and solve when this is a nonzero constant. This gives c in terms of the coefficients of P_l and/or P_{l-g-1}. Next, write $P_l = \sum_{i=0}^{l-g-2} a_i x^i + \lambda P_{l-g-1}$ where $\lambda \in K[x]$ is of degree $g + 1$ and solve $P_l^2 \equiv c \mod (P_{l-g-1}^2)$. This method can work for any P_{l-g-1}, however it is a lot less efficient as the first method as now there are two equations that need to be solved.

Note that for the existence of nontrivial units we can assume that c is a square by lemma 4.3. However, to find a hyperelliptic curve where the fundamental unit $\varepsilon = P_l + yP_{l-g-1}$ has nonsquare norm, we would have to start with P_{2l-g-1}, which adds difficulty as well, as there are more equations to solve. If we find a suitable P_{2l}, then the unit $P_{2l} + yP_{2l-g-1}$ could either be a fundamental unit or it could be the square of a fundamental unit. So, if we the order l we want is not a prime, then the unit we find is not necessarily a fundamental unit. All in all, it is most likely better to solve the cases with c not a square directly, in stead of

starting with P_{2l-g-1}.

We will now give some examples of these methods for genus 2 over $\mathbb{Q}$. This will first be done for 7-torsion as it shows well how these methods work. So we start with a unit of the form $\varepsilon = P_7 + yP_4$ where $P_7, P_4 \in \mathbb{Q}[x]$ are of degree $7, 4$ respectively and P_4 is monic. We want to find an $f \in \mathbb{Q}[x]$ that is separable and of degree 6 such that $P_7^2 - fP_4^2 = c$. Then $f = \frac{P_7^2 - c}{P_4^2}$ and we want $P_7^2 \equiv c \mod P_4^2$. We first try the first method where c is (assumed to be) a square, so we can take $c = 1$. Write $P_4 = Q_1Q_2$ such that we want $P_7 \equiv -1 \mod (Q_1^2)$ and $P_7 \equiv 1 \mod (Q_2^2)$. Then we only need to try Q_1 cubic, Q_2 linear and Q_1, Q_2 both quadratic.

We first take $P_4 = x(x^3 + ax^2 + bx + c)$ (the linear term can be assumed to be equal to x by a translation). Then $P_7 = -1 + \lambda(x^3 + ax^2 + bx + c)^2$ where $\lambda \in \mathbb{Q}[x]$ is a linear polynomial. Write $\lambda = \alpha x + \beta$, then $P_7 \equiv -1 + (\alpha c^2 + 2\beta bc)x + \beta c^2 \equiv 1 \mod x^2$. Solving $-1 + (\alpha c^2 + 2\beta bc)x + \beta c^2 = 1$ for α and β we get $\lambda = \frac{-4b}{c^3}x + \frac{2}{c^2}$. Then

$$\begin{aligned} f = \frac{4}{c^6}&(-c + 2bx)(2bx^5 + (4ab - c)x^4 + (2a^2b + 4b^2 - 2ac)x^3 + (4ab^2 - a^2c + 2bc)x^2 \\ &+ (2b^3 + 2abc - 2c^2)x + 3b^2c - 2ac^2) \end{aligned}$$

and $\varepsilon = P_7 + yP_4 = -1 + (\frac{-4b}{c^3}x + \frac{2}{c^2})(x^3 + ax^2 + bx + c)^2 + y(x^3 + ax^2 + bx + c)$ is a unit for the curve given by $y^2 = f$. We aren't done yet as the constraints on the parameters a, b, c still need to be determined. It is at least required that $b \neq 0$, as otherwise f would not have degree 6, and $c \neq 0$, as otherwise λ is not well-defined. We also require that the factors in P_4 are coprime, but this should always hold automatically. Finally, we require that f is separable. For general values of a, b, c we have that $\gcd(f, f') = 1$, so that f is almost always separable. The square factor in f can also be removed by the coordinate transformation $x \mapsto x$, $y \mapsto \frac{c^3 y}{2}$. So, we have found a 3-parameter family of genus 2 hyperelliptic curves $C_{a,b,c}$ with a nontrivial unit all with 7-torsion divisor where the constraints on the parameters a, b, c are that $b, c \neq 0$.

We want to check if this is truly a 3-parameter family or if fewer parameters actually generate the same family of hyperelliptic curves. To do this we can use Igusa-Clebsch invariants. The Igusa-Clebsch invariants can be defined for a curve of genus 2 over any field with characteristic unequal to 2. They are four numbers (I_2, I_4, I_6, I_{10}) (or sometimes denoted by (A', B', C', D')) that live in a weighted projective space. The Igusa-Clebsch invariants of a polynomial are defined in terms of certain nice symmetric polynomials in its roots. Over the complex numbers the elements $i_1 := \frac{I_2^5}{I_{10}}$, $i_2 := \frac{I_2^3 I_4}{I_{10}}$ and $i_3 := \frac{I_2^2 I_6}{I_{10}}$ are the invariants of the curve. They perform the same role as the j-invariant does for elliptic curves. When two genus 2 hyperelliptic curves over $\mathbb{C}$ have the same i_1, i_2, i_3 then they are isomorphic. For details see [16] and [8]. We can use Magma to compute the Igusa-Clebsch invariants for the curves we have.

For our 3-parameter family we can try to use the invariants to check if for two different sets of parameters the curves are isomorphic (over $\mathbb{C}$ at least). Let i_1, i_2, i_3 be the 3 invariants of $C_{a,b,c}$, then we can define the rational map $\psi : \mathbb{A}^3 - \to \mathbb{A}^3$ given by $\psi(a, b, c) = (i_1, i_2, i_3)$. Now if the image of ψ is $\mathbb{A}^3$, then we know that we really have a 3-parameter family. The Igusa invariants are too large to compute the image directly, but using Magma we can compute the dimension of the image of ψ restricted to the plane $(a = 0)$. See Appendix B.4 for the Magma

code. It turns out that this dimension is 1. As a 2-dimensional variety of $\mathbb{A}^3$ is mapped to a 1-dimensional curve under ψ we conclude that $\mathrm{Im}(\psi) \neq \mathbb{A}^3$. We do not know yet whether the image of ψ is then 1- or 2-dimensional. However, if we take lines $a = 0$ and b or c some fixed constant we find that these lines get mapped to the same curve under ψ, at least for $b = 1, 2$, and $c = 1, 2$. Thus we conjecture that it is actually 1-dimensional.

Now we try the other possibility for P_4. We take $P_4 = (x^2+a)(x^2+bx+c)$ (by a translation the x-term can be removed in one of the factors), $P_7 \equiv -1 \mod (x^2 + bx + c)^2$ and $P_7 \equiv 1 \mod (x^2+a)^2$. Then $P_7 = -1+\lambda(x^2+bx+c)^2$ where λ is a cubic polynomial. Solving $P_7 \equiv 1 \mod (x^2 + a)^2$ for the coefficients in λ and removing any square factors we get for f

$$\begin{aligned}
f =\Big(& - a^4 - 3a^3b^2 - 3a^2b^4 - ab^6 + 6a^3c + 12a^2b^2c + 6ab^4c \\
& - 12a^2c^2 - 21ab^2c^2 - 5b^4c^2 + 10ac^3 + 12b^2c^3 - 3c^4 \\
& + (6a^2bc - 6ab^3c - 4b^5c - 12abc^2 + 4b^3c^2 + 6bc^3)x \\
& + (2a^3 + 9a^2b^2 + 3ab^4 - 6a^2c - 24ab^2c - 8b^4c + 6ac^2 + 15b^2c^2 - 2c^3)x^2 \\
& + (6a^2b + 2ab^3 - 12abc - 4b^3c + 6bc^2)x^3\Big) \\
& \cdot \Big(3a^4 - 3a^3b^2 - 2a^2b^4 - 10a^3c + 12a^2c^2 + 3ab^2c^2 - 6ac^3 + c^4 \\
& + (8a^3b + 4a^2b^3 - 18a^2bc - 6ab^3c + 12abc^2 - 2bc^3)x \\
& + (2a^3 - 3a^2b^2 - ab^4 - 6a^2c + 6ac^2 + 3b^2c^2 - 2c^3)x^2 \\
& + (6a^2b + 2ab^3 - 12abc - 4b^3c + 6bc^2)x^3\Big)
\end{aligned}$$

We don't know if this is actually a 3-parameter family or not. We at least require that $b \neq 0$ and $c \neq 0$. When using the Igusa-Clebsch invariants it is already too difficult for Magma to compute the image of $(a, b, c) \mapsto (i_1, i_2, i_3)$ restricted to the plane $(a = 0)$.

These were all the possibilities for the first method. Hence, we now try the second method of creating f. We only need to consider P_4 irreducible or P_4 a product of two quadratic polynomials. As such, we just start with P_4 arbitrary and after solving the first equation only take those solutions that are interesting. Thus, let $P_4 = x^4 + b_2x^2 + b_1x + b_0$ and write $P_7 \equiv a_3x^3 + a_2x^2 + a_1x + a_0 \mod (P_4)$. Solving $P_7^2 \equiv c \mod (P_4^2)$ where $c \in \mathbb{Q}^*$ for the a_i, b_j gives six different solutions, but not all of them will work. One of these solutions is $a_2 = a_0 = b_2 = 0$ and $b_0 = (b_2 - \frac{a_1}{a_3})^2$. This gives $P_4 = x^4 + b_2x^2 + (b_2 - \frac{a_1}{a_3})^2$, $P_7 = a_3x^3 + a_1x + \lambda P_4$ and $c = \frac{(a_3b_2-2a_1)(a_3b_2-a_1)^2}{a_3}$. Note that P_4 is irreducible and that c is nonsquare for many values of a_3, a_1, b_2. Thus this does give a different solution then the first method. Solving $P_7^2 \equiv c \mod (P_4^2)$ for the coefficients in λ gives

$$\lambda = \frac{a_3^3(2a_3b_2 - 3a_1)}{2(a_3b_2 - 2a_1)(a_3b_2 - a_1)^2}x^3 + \frac{b_2^2a_3^4 - b_2a_3^3a_1 - a_3^2a_1^2}{2(a_3b_2 - 2a_1)(a_3b_2 - a_1)^2}x.$$

Then $f = \frac{P_7^2 - c}{P_4^2}$ gives (after removing square factors)

$$\begin{aligned} f = &- 4b_2^5a_3^5 + 32a_3^4b_2^4a_1 - 100a_3^3b_2^3a_1^2 + 152a_3^2b_2^2a_1^3 - 112a_3b_2a_1^4 + 32a_1^5 \\ &+ (9b_2^4a_3^5 - 46b_2^3a_3^4a_1 + 87b_2^2a_3^3a_1^2 - 74b_2a_3^2a_1^3 + 25a_3a_1^4)x^2 \\ &+ (4b_2^3a_3^5 - 10b_2^2a_3^4a_1 + 2b_2a_3^3a_1^2 + 6a_3^2a_1^3)x^4 \\ &+ (4b_2^2a_3^5 - 12b_2a_3^4a_1 + 9a_3^3a_1^2)x^6 \end{aligned}$$

So we have found a 3-parameter family with c non-square and P_4 irreducible for general a_3, a_1, b_2. If we check the invariants, then with $b_2 = 0$ we have

$$(i_1, i_2, i_3) = (\frac{3671988787450000}{148980627}, \frac{3671988787450000}{148980627}, \frac{26212909963525}{148980627})$$

and we see that all three are constant. Thus, over $\mathbb{C}$, with $b_2 = 0$ the remaining parameters can be removed. If next $a_1 = 0$ then we get $(i_1, i_2, i_3) = (\frac{345025251}{676}, \frac{434166723}{10816}, \frac{419309811}{43264})$, which are again constants, but also different from the invariants with $b_2 = 0$. This shows that the family of curves we have is at least a 1-parameter family, however, we don't know how many parameters are exactly needed to generate the family.

Next we try the methods for 5-torsion. The unit has the form $\varepsilon = P_5 + yP_2$ with P_2 monic. For the first method we only need to consider $P_2 = x^2 + a$ with $P_5 \equiv -1 \mod (P_2^2)$ and $P_2 = x(x+a)$ with $P_5 \equiv -1 \mod (x+a)^2$ and $P_5 \equiv 1 \mod (x^2)$. So, first take $P_2 = x^2+a$ and then $P_5 = -1 + (u_1x + u_0)P_2^2$. As here $P_5 \equiv -1 \mod (P_2^2)$ there is nothing else to solve. Then $f = \frac{P_5^2 - 1}{P_2^2} = (u_1x + u_0)\left(-2 + a^2u_0 + a^2u_1x + 2au_0x^2 + 2au_1x^3 + u_0x^4 + u_1x^5\right)$ with $u_1 \neq 0$. Now to determine if we can reduce the number of parameters.

This is done again with the Igusa invariants. Consider the rational map $(a, u_1, u_0) \mapsto (i_1, i_2, i_3)$ where i_1, i_2, i_3 are the invariants of the curve. The plane $(u_0 = 0)$ maps to the curve in $\mathbb{A}^3$ given by

$$y^2 - \frac{960}{241}yz + \frac{327680000}{2169}y + \frac{819200000}{2169}z = 0$$

and $x = -320y$. This is 1-dimensional and thus at least one parameter can be removed. Also, the plane $(a = 0)$ maps to the curve given by

$$y^2 - \frac{34562816}{5756125}yz - \frac{17289445376}{46049}y + \frac{10371072}{1151225}z^2 + \frac{53435432960}{46049}z$$

and $x = \frac{400000}{49}y - \frac{1228800}{49}z$. As we have two irreducible affine varieties that map to different irreducible curves we find that the image must be at least 2-dimensional.

Now let $P_2 = x(x + a)$ and $P_5 = -1 + \lambda(x + a)^2$ where $\lambda \in \mathbb{Q}[x]$ is a cubic polynomial. Solving $P_5 \equiv 1 \mod (x^2)$ gives $\lambda = u_3x^3 + u_2x^2 - \frac{4}{a^3}x + \frac{2}{a^2}$ where u_3, u_2 are arbitrary with $u_3 \neq 0$. Then $f = \frac{P_5^2 - 1}{P_2^2}$ gives

$$\begin{aligned} f = &\frac{1}{a^6}(2a - 4x + a^3u_2x^2 + a^3u_3x^3) \\ &\cdot (-6a + a^5u_2 - 4x + 2a^4u_2x + a^5u_3x + a^3u_3x^2 + 2a^4u_3x^2 + a^3u_3x^3) \end{aligned}$$

For the invariants the only thing we can say is that image of the plane ($u_2 = 0$) under the map $(a, u_2, u_3) \mapsto (i_1, i_2, i_3)$ is 1-dimensional. As we require both $a \neq 0$ and $u_3 \neq 0$ we can't take the planes where they are zero.

Next we try the second method. We take $P_2 = x^2 + b$ and suppose $P_5 \equiv a_1 x + a_0 \mod (P_2)$. Then $P_5^2 \equiv -a_1^2 b + 2a_1 a_0 x + a_0^2 \mod (P_2)$, so we require that $2a_1 a_0 = 0$. If $a_1 = 0$, then $c = a_0^2$ and this leads to the first example of the first method. If $a_0 = 0$, then $c = -a_1^2 b$ and this is not a square in $\mathbb{Q}$ for general b. It does mean we require $a_1 \neq 0$ and $b \neq 0$. So $P_5 = a_1 x + \lambda P_2$ where λ is cubic again and we solve $P_5^2 \equiv -a_1^2 b \mod (P_2^2)$. This gives $\lambda = u_3 x^3 + u_2 x^2 + (\frac{a_1}{2b} + u_3 b)x + b u_2$ and then

$$\begin{aligned} f = \frac{1}{4b^2}\Big(&4a_1^2 b + 4b^4 u_2^2 + (12a_1 b^2 u_2 + 8b^4 u_2 u_3)x \\ &+ (a_1^2 + 8b^3 u_2^2 + 12a_1 b^2 u_3 + 4b^4 u_3^2)x^2 + (4a_1 b u_2 + 16b^3 u_2 u_3)x^3 \\ &+ (4b^2 u_2^2 + 4a_1 b u_3 + 8b^3 u_3^2)x^4 + 8b^2 u_2 u_3 x^5 + 4b^2 u_3^2 x^6\Big) \end{aligned}$$

For how many parameters are required we can only check the image of $(a_1, b, u_2, u_3) \mapsto (i_1, i_2, i_3)$ for the hyperplane ($u_2 = 0$). This gives a 1-dimensional image. As we require $b, u_3, a_1 \neq 0$ we can't check this for other hyperplanes where one of the coordinates is zero. With this we do have found all possible examples of 5-torsion for $\infty^+ - \infty^-$.

For 3-torsion there isn't much to be done. The fundamental unit would have the form $P_3 + yP_0$, where P_3 is a cubic polynomial and P_0 is a nonzero constant. But this gives $P_3^2 - fP_0^2 = c$ or $f = \frac{P_3^2 - c}{P_0^2}$ where c is a nonzero constant. In other words, f is a square of a cubic polynomial up to a nonzero constant. We would like to parametrize all genus 2 curves with such 3-torsion in the Jacobian. Over an algebraically closed field we can use a coordinate transformation of the form $x \mapsto \frac{\alpha x + \beta}{\gamma x + \delta}$ with $\alpha\delta - \beta\gamma \neq 0$ such that the equation of the curve C becomes $y^2 = x(x-1)(x+1)(x-a)(x-b)(x-c) = (x^3 - x)(x-a)(x-b)(x-c)$. In this curve we look at the divisor class $D = [\infty^+ - \infty^-]$ in the Jacobian. We use Magma to see when $2D = -D$.

Magma uses the Mumford representation for points on the Jacobian. This works as follows (from the Magma handbook page on "Points on the Jacobian"): Let C be a hyperelliptic curve of genus g, then a triple $< a(x), b(x), d >$ specifies the divisor D of degree d on C defined by $A(x, z) = 0$, $y = B(x, z)$ where $A(x, z)$ is the degree d homogenization of $a(x)$ and $B(x, z)$ is the degree $(g + 1)$ homogenization of $b(x)$. The point on the Jacobian of C corresponding to $< a(x), b(x), d >$ is then $D - \frac{d}{2} D_\infty$ where $D_\infty = \infty^+ + \infty^-$ if there are two points at infinity and $D_\infty = 2\infty$ when there is only one. In the first case d is required to be even. All points on the Jacobian can be expressed in this way for the curves we consider. See B.5 for the Magma code used.

In Magma we have that $-D$ is represented by $< 1, -x^3 - \frac{a}{2}x^2, 2 >$. The first coordinate of $2D$ is

$$\frac{\frac{1}{4}\left(a^3 - 4a(1+b) + 8c\right)^2 - \left(a^2 - 4(1+b)\right)\left(a^3 - 4a(-1+b) + 8c\right)x}{(5a^4 + 16(1+b)^2 - 8a^2(1+3b) + 32ac)} + x^2.$$

This is a quadratic polynomial, but for 3-torsion it needs to be equal to 1. The only possibility is then that the denominator above is equal to zero. There is only a single c in the denominator

and solving for it gives

$$c = \frac{-16 + 8a^2 - 5a^4 - 32b + 24a^2b - 16b^2}{32a}.$$

We substitute this c into the equation of C. Then $-D$ still has the same representation, but the first coordinate of $2D$ is now

$$\frac{\frac{1}{16}\left(a^4 - 8a^2(-1+b) + 16(1+b)^2\right)^2}{a\left(a^6 - 64(1+b)^3 - 4a^4(7+3b) + 16a^2\left(7+10b+3b^2\right)\right)} + x.$$

This is a linear polynomial so we again need to solve when the denominator is equal to zero. As we want $a \neq 0$ this gives $b = -1 + \frac{a^2}{4}, -1 - a + \frac{a^2}{4}$ or $-1 + a + \frac{a^2}{4}$. Substituting $b = -1 + \frac{a^2}{4}$ into the equation of C gives the equation

$$y^2 = \frac{ax}{2} + \left(1 - \frac{a^2}{4}\right)x^2 - \frac{3ax^3}{2} + \left(-2 + \frac{a^2}{4}\right)x^4 + ax^5 + x^6 = \frac{1}{4}(x^3 - x)(a + 2x)(-2 + ax + 2x^2).$$

This gives the unit $1 + \frac{4x}{a} - 2x^2 - \frac{4x^3}{a} - \frac{4y}{a}$. With $b = -1 + a + \frac{a^2}{4}$ we get

$$\begin{aligned} y^2 &= \left(a - \frac{a^2}{2}\right)x + \left(1 - a - \frac{a^2}{4}\right)x^2 + \left(-2a + \frac{a^2}{2}\right)x^3 + \left(-2 + a + \frac{a^2}{4}\right)x^4 + ax^5 + x^6 \\ &= \frac{1}{4}(x^3 - x)(-2 + a + 2x)\left(2a + 2x + ax + 2x^2\right) \end{aligned}$$

and the unit $1 + \frac{(2-a)x}{a} - x^2 - \frac{2x^3}{a} - \frac{2y}{a}$. Finally, for $b = -1 - a + \frac{a^2}{4}$ we get

$$y^2 = \frac{1}{4}(x^3 - x)(2 + a + 2x)\left(-2a - 2x + ax + 2x^2\right)$$

and the unit $1 + \frac{(2+a)x}{a} - x^2 - \frac{2x^3}{a} - \frac{2y}{a}$. We denote these three curves by $C_{1,a_1}, C_{2,a_2}, C_{3,a_3}$ respectively. Checking the Igusa invariants of these curves, we find that the Igusa invariants of C_{3,a_3} are obtained from the Igusa invariants of C_{2,a_2} by $a_2 \mapsto -a_3$. So C_{3,a_3} is not of any interest. The Igusa invariants of C_{1,a_1} and C_{2,a_2} are only equal for particular values of a_1, a_2. For example, $C_{1,-3}$ and $C_{2,12}$ have the same Igusa invariants and are thus isomorphic (at least over some field extension). The only other rational pairs (a_1, a_2) for which this hold are $(\pm\frac{16}{3}, \frac{1}{3}), (\pm 4, -2), (\pm 1, -4)$, and $(3, 12)$, which we determined using Mathematica.

For higher torsion it will be more difficult to find curves with both methods. If we want p-torsion for an odd prime p, then with the first method we have $P_{p-3} = Q_1Q_2$ with $\deg(Q_1) = \frac{p-1}{2}$ or $\frac{p-3}{2}$. Taking $P_l = -1 + \lambda Q_1^2$ with λ linear or cubic, we have to solve $P_l^2 \equiv 1 \mod (Q_2^2)$. The higher we take p the more equations need to be solved and the more parameters in P_{p-3} are possible. This causes the difficulties with higher torsion as it is not possible to solve all the equations in general. What we can try is to take some coefficients in P_{p-3} fixed to make the equations easier to solve. However, fixing too many coefficients might cause no solutions to exist.

For the second method it is even worse as there are more parameters in P_p as well and we have to solve equations twice, first $P_p^2 \equiv c \mod (P_{p-3})$ and then $P_p^2 \equiv c \mod (P_{p-3}^2)$. We didn't have these problems yet for $p = 7$, but for $p = 11$ they are already present.

We try the first method for 11-torsion and take Q_1, Q_2 such that we have the least number of equations to solve. This means taking $P_8 = (\sum_{i=0}^{5} a_i x^i)(\sum_{j=0}^{3} b_j x^j)$ where $a_5 = b_3 = 1$. Let $P_{11} = -1+\lambda(\sum_{i=0}^{5} a_i x^i)$ with $\lambda = u_1 x + u_0$, then we have to solve $P_{11}^2 \equiv 1 \mod (\sum_{j=0}^{3} b_j x^j)^2$. In general we could not solve this. In fact, we have only managed to solve it when taking $(\sum_{j=0}^{3} b_j x^j) = x^3$. This gives $a_3 = \frac{36a_4^2}{35}$, $a_2 = \frac{972a_4^3}{875}$, $d_1 = \frac{5832a_4^4}{4375}$, $a_0 = \frac{52488a_4^5}{21875}$, $u_1 = -\frac{2392578125}{6198727824a_4^{11}}$ and $u_0 = \frac{478515625}{1377495072a_4^{10}}$. Substituting these values back in P_{11} and P_8 we get

$$f_{a_4} = \frac{P_{11}^2 - 1}{P_8^2} = \big(7476806640625(-9a_4 + 10x)(1347192a_4^5 + 641520a_4^4 x + 467775a_4^3 x^2 + 385000a_4^2 x^3 + 336875a_4 x^4 + 306250x^5)\big)/(153696906544127099904a_4^{22})$$

Now, if we check the Igusa invariants of this curve, we find that they are constant. Thus all these curves are at least isomorphic to eachother over some field extension of $\mathbb{Q}$. However, we can see that they are in fact isomorphic to each other over $\mathbb{Q}$. This is because f_{a_4} as polynomial in a_4 and x is homogeneous. Let C be the curve given by $y^2 = f_1$ and for any nonzero value of a_4 let D be the curve given by $y^2 = f_{a_4}$, then $(x, y) \mapsto (a_4 x, a_4 x)$ is an isomorphism from C to D. So the parameter can be removed in f_{a_4}. Taking $a_4 = 1$ and removing the square constant factors in f we get the hyperelliptic curve given by

$$y^2 = (-9 + 10x)\left(1347192 + 641520x + 467775x^2 + 385000x^3 + 336875x^4 + 306250x^5\right).$$

This curve has 11-torsion. We haven't managed to find an example with the second method.

While this method is not effective to find examples for higher torsion orders, it can be used to characterize all hyperelliptic curves over $\mathbb{Q}$ given by $y^2 = f(x)$ where f has degree 6 such that $\infty^+ - \infty^-$ has small torsion order. At least up to torsion order 7 it can be done.

6 Units on Curves with Genus at least 3

In this section we briefly explore the possiblities for the unit group in the coordinate ring of curves of genus at least 3 by looking at some examples.

6.1 Hyperelliptic Curves

For hyperelliptic curves of genus at least 3 many of the same methods that were used for genus 2 can still be used. In particular over $\mathbb{Q}$, the method of starting from a fundamental unit $P_l + yP_{l-g-1}$. From lemma 4.4 we already know that for higher genus the lower l-torsions cannot happen (when $l < g+1$), at the same time it is easier to find examples for different orders in higher genus.

Let C be a hyperelliptic curve of genus g over $\mathbb{Q}$ given by $y^2 = f(x)$. For 5-torsion in the genus 2 case the fundamental unit is of the form $P_5 + yP_2$ where $P_5^2 - fP_2^2 \in \mathbb{Q}^*$. If $P_5^2 - fP_2^2$ was actually a square in $\mathbb{Q}$ we could assume it was one. In that case $P_5 \equiv \pm 1 \mod (P_2^2)$. We could take P_2 arbitrary and $P_5 = -1 + \lambda P_2^2$ for a linear polynomial λ and all requirements would be satisfied. This also works for higher genus.

Lemma 6.1. *Let $l, g \in \mathbb{Z}_{>1}$ with $g+1 \leq l \leq 2(g+1)$, then there is a hyperelliptic curve C of genus g over $\mathbb{Q}$ such that $\infty^+ - \infty^-$ has order l in $J(C)$.*

Proof. Given l, g let $P_{l-g-1} \in \mathbb{Q}[x]$ be of degree $l-g-1$ (as $g+1 \leq l$ it exists) and let $P_l = -1 + \lambda P_{l-g-1}^2$ where $\lambda \in \mathbb{Q}[x]$ is of degree $2(g+1) - l$ and $\lambda \neq 0$. Then $f = \frac{P_l^2 - 1}{P_{l-g-1}^2} = \lambda^2 P_{l-g-1}^2 - 2\lambda \in \mathbb{Q}[x]$ is of degree $2g+2$. Now f defines a hyperelliptic curve of genus g if it is separable.

We have $f' = 2\lambda'(\lambda P_{l-g-1}^2 - 1) + 2\lambda^2 P_{l-g-1} P'_{l-g-1}$. Let $x \in \bar{Q}$ such that $f(x) = \lambda(x)(\lambda(x) P_{l-g-1}(x)^2 - 2) = 0$. If $\lambda(x) = 0$, then $f'(x) = -2\lambda'(x)$. So if λ is separable, then $f'(x) \neq 0$ if $\lambda(x) = 0$.

If $\lambda(x) P_{l-g-1}(x)^2 = 2$, then $f'(x) = 2\lambda'(x) + 2\lambda(x)^2 P_{l-g-1}(x) P'_{l-g-1}(x)$. Choosing λ, P_{l-g-1} such that this is then nonzero, we get that f is separable. For example, $\lambda = x^{2(g+1)-l} + \alpha$, $P_{l-g-1} = x^{l-g-1}$ for almost all $\alpha \in \mathbb{Z}_{\neq 0}$ with α not an $(2(g+1) - l)$-th power will work. Then f defines a hyperelliptic curve of genus g and $\varepsilon = P_l + yP_{l-g-1}$ is a fundamental unit with $\operatorname{div}(\varepsilon) = l(\infty^+ - \infty^-)$. $\square$

It is possible that $\infty^+ - \infty^-$ has order $l > 2(g+1)$ in $J(C)$, however for higher l it will be more difficult to find a hyperelliptic curve where $\infty^+ - \infty^-$ has order l. For l just slightly bigger than $2(g+1)$ it is likely that examples can be found by starting from the fundamental unit. Suppose that $l - 2a \leq 2(g+1)$ for a small positive integer a, take $P_{l-g-1} = x^a P_{l-g-1-a}$ where $P_{l-g-1-a} \in \mathbb{Z}[x]$ is monic and has degree $l-g-1-a$ and let $P_l = -1 + \lambda P_{l-g-1-a}^2$ where $\lambda \in \mathbb{Q}[x]$ has degree $l - 2(l-g-1-a) = 2(g+1+a) - l$. Solving $P_l^2 \equiv 1 \mod (x^{2a})$ for the coefficients in λ or $P_{l-g-1-a}$ wil give examples if solutions to this equality exist by taking $f = \frac{P_l^2 - 1}{P_{l-g-1}^2}$. This is what we did for 11-torsion in the genus 2 case. We now give an example of this for 11-torsion in genus 3 as well.

For genus 2 we tried $P_8 = x^3(x^5 + d_4x^4 + d_3x^3 + d_2x^2 + d_1x + d_0)$ and this only gave a single curve (up to isomorphism). For genus 3 the unit is now $P_{11} + yP_7$, and we try $P_7 = x^2(x^5 + d_4x^4 + d_3x^3 + d_2x^2 + d_1x + d_0)$. Next we take $P_{11} = -1 + (u_1x + u_0)(x^5 + d_4x^4 +$

$d_3x^3 + d_2x^2 + d_1x + d_0)^2$ and solve $P_{11} \equiv 1 \mod (x^4)$. This now gives $d_3 = \frac{5d_1^3}{2d_0^2}$, $d_2 = \frac{3d_1^2}{2d_0}$, $u_1 = -\frac{4d_1}{d_0^3}$ and $u_0 = \frac{2}{d_0^2}$. For $f = \frac{P_{11}^2-1}{P_7^2}$ we then get

$$\begin{aligned} f = \frac{1}{d_0^{10}}&(-d_0 + 2d_1x)(35d_0^3d_1^4 - 8d_0^6d_4 + (-8d_0^6 + 28d_0^2d_1^5 + 8d_0^5d_1d_4)x \\ &+ (8d_0^5d_1 + 35d_0d_1^6 + 4d_0^4d_1^2d_4)x^2 + (4d_0^4d_1^2 + 50d_1^7 + 4d_0^3d_1^3d_4)x^3 \\ &+ (4d_0^3d_1^3 + 40d_0^2d_1^4d_4 - 4d_0^5d_4^2)x^4 + (40d_0^2d_1^4 - 8d_0^5d_4 + 8d_0^4d_1d_4^2)x^5 \\ &+ (-4d_0^5 + 16d_0^4d_1d_4)x^6 + 8d_0^4d_1x^7) \end{aligned}$$

Hence, we now get a possible 3-parameter family. As there is no equivalent of the Igusa-Clebsch invariants for hyperelliptic curves of genus at least 3, we cannot check how many parameters are actually required.

6.2 General Curves

Now suppose the curve we consider is not hyperelliptic. For nontrivial units to exist in the coordinate ring it is still required that there are at least two points at infinity. If there are two points at infinity, called ∞^+ and ∞^-, then just like in the hyperelliptic case, $K[C]^* = K\cdot < h >$ where $h \in K[C]$ is a nonzero function with $\mathrm{div}(h) = n\infty^+ - n\infty^-$ for some $n \in \mathbb{Z}$. The difference with hyperelliptic curves is that for general curves there is no fixed form for the functions in the coordinate ring.

For general curves one can still use Magma to find units, though this is easier for curves over finite fields than over the rational numbers. This is because the "Order" command for divisors does not work for non-hyperelliptic curves. Hence, to find the order of a divisor in the Jacobian, one needs to check for each multiple of the divisor if it is principal. Over finite fields the classnumber of the curve, which is the number of elements of the Jacobian, is still finite and Magma can compute it. For the order of a divisor only the integer divisors of the classnumber need to be considered. Over $\mathbb{Q}$ the number of elements of the Jacobian is not finite, but the order of torsion elements is still bounded by the classnumber of the Jacobian of the curve over an odd prime of good reduction by lemma 3.4. So over $\mathbb{Q}$ an odd prime with good reduction also has to be found.

Consider the following example: Let $C \subset \mathbb{A}^2$ be the genus 3 over $\mathbb{F}_5$ given by $(x-y)^2(x+y)^2 + 1 + y^3 = 0$ and let $\tilde{C}$ be its projective completion, which is given by $(x-y)^2(x+y)^2 + z^4 + y^3z = 0$. The points at infinity are $(1:1:0)$ and $(-1:1:0)$. To compute the order of $(1:1:0) - (-1:1:0)$ in $J(C)$ with Magma the projective completion needs to be used. The following Magma code is used for this.

```
K:=GF(5);
P2<x,y,z>:=ProjectiveSpace(K,2);
f:=(x-y)^2*(x+y)^2+z^4+y^3*z;
C:=Curve(P2,f);
if IsNonSingular(C) eq true then
inf1:=C![1,1,0];
inf2:=C![-1,1,0];
// defining the points at infinity
```

```
FC<x,y>:=FunctionField(C);
D:=Divisor(C,[<Place(inf1),1>,<Place(inf2),-1>]);
for i in Divisors(ClassNumber(C)) do
j:=IsPrincipal(i*D);
// defined like this gives only true or false
if j eq true then
i;
IsPrincipal(i*D);
// when true output is true and a corresponding function
break;
end if;
end for;
end if;
```

With this code one can compute the order and a corresponding function of a divisor for a nonsingular curve over a finite field. The code can be easily adapted to other curves and divisors. For divisors at infinity one does need to know the points at infinity. For our example we find that $(1:1:0)-(-1:1:0)$ has order 22 and that

$$\begin{aligned} h = {} & (2y^8+2y^6+4y^5+2y^4+y+4)x^3+(y^9+3y^7+2y^5+4y^4+3y^3+2y^2+y+4)x^2 \\ & +(2y^{10}+2y^8+3y^6+y^5+3y^3+y^2+y+2)x+3y^{10}+y^9+2y^8+3y^7+4y^5+2y^4 \\ & +4y^3+3y^2+3y+1 \end{aligned}$$

is a generating unit with $\mathrm{div}(h)=22(1:1:0)-22(-1:1:0)$. To check that a function is a unit the following code can be used.

```
K:=GF(5);
A<x,y>:=AffineSpace(K,2);
C:=Curve(A,(x-y)^2*(x+y)^2+1+y^3);
if IsNonSingular(C) eq true then
FC<x,y>:=FunctionField(C);
h:=(2*y^8 + 2*y^6 + 4*y^5 + 2*y^4 + y + 4)*x^3 + (y^9 + 3*y^7 + 2*y^5 + 4*y^4
 + 3*y^3 + 2*y^2 + y + 4)*x^2 + (2*y^10 + 2*y^8 + 3*y^6 + y^5 + 3*y^3 + y^2 +
 y + 2)*x + 3*y^10 + y^9 + 2*y^8 + 3*y^7 + 4*y^5 + 2*y^4 + 4*y^3 + 3*y^2 +
3*y + 1;
divh:=Divisor(h);
Support(divh);
end if;
```

Here, both the affine equation or the equation of the projective completion of the curve can be used as the function fields are isomorphic.

Over $\mathbb{Q}$ one can still use the consequence of Corollary 3.4, which says that for primes p of good reduction the reduction of the Jacobian is injective. For example, consider the genus 3 curve C over $\mathbb{Q}$ given by $(x-my)^2(x-ny)^2+z^4+y^3z=0$ with $m\neq n$. The points $(m:1:0)$ and $(n:1:0)$ are the points at infinity. If we reduce C modulo 5 and 7, then the reduction is always good whenever C is nonsingular. Using the Magma code in B.6 we can

check that the order of $(m:1:0)-(n:1:0)$ in $J_{\mathbb{F}_5}(C)$ and $J_{\mathbb{F}_7}(C)$ is always different, so $(m:1:0)-(n:1:0)$ does not have finite order in $J_{\mathbb{Q}}(C)$ and thus there are no nontrivial units. The same holds for the curves $(x-my)^2(x-ny)^2+z^4+y^3z+x^2z^2+xyz^2=0$ and $(x-my)^2(x-ny)^2+z^4+4y^3z+2x^2yz=0$ with $m\neq n$.

For general curves it is also possible that there are more than two points at infinity, in which case there can be multiple independent generators of the unit group and there are more possibilities for the divisors of units in the coordinate ring. For example, the curve C over $\mathbb{F}_5$ given by $(x-y)^2(x+y)(x-2y)+1+y^3=0$ has $\infty_1=(1:1:0)$, $\infty_2=(-1:1:0)$ and $\infty_3=(2:1:0)$ as the points at infinity. The classnumber of C is 245 and the divisor class of $\infty_1-\infty_2$ has order 249 in J, while the class of $\infty_1+\infty_2-2\infty_3$ has order 49 and $2\infty_1+\infty_2-3\infty_3$ has order 5. Let f and g be functions with divisors $49\infty_1+49\infty_2-98\infty_3$ and $10\infty_1+5\infty_2-15\infty_3$ respectively, then $\mathbb{F}_5[C]^*=\mathbb{F}_5\cdot<f>\cdot<g>$.

For an example over $\mathbb{Q}$ consider the curve C over given by $y^2x^2+y^3x=F_3(x)$ where $F_3(x)$ is a cubic polynomial such that C is nonsingular. The points at infinity are $\infty_1=(1:0:0)$, $\infty_2=(1:-1:0)$ and $\infty_3=(0:1:0)$. From the equation of C we have that $x(y^2x+y^3-\frac{F_3-c}{x})=c$ where c is the constant coefficient of F_3. Thus x is a unit if $c\neq 0$ and the inverse is $\frac{1}{c}(y^2x+y^3-\frac{F_3-c}{x})$. For the divisor we have $\mathrm{div}(x)=2\infty_1+\infty_2-3\infty_3$.

For a genus 3 hyperelliptic curve C over $\mathbb{Q}$ it is not possible for $\infty^+-\infty^-$ to have order 3 in $J(C)$. For a nonhyperelliptic curve this is possible. For example, the curve given by $(x-y+1)(y^3+x+x^2)=1$ has genus 3 and $\mathrm{div}(x-y+1)=3(1:1:0)-3(1:0:0)$. Here $(1:1:0)$ and $(1:0:0)$ are the points at infinity.

For an example over $\mathbb{Q}$ with multiple generators of the unit group, consider the curve C given by $(x-1)(y^2-y+x)(y-x)=1$. The points at infinity are $P_1=(1:1:0), P_2=(1:0:0)$ and $P_3=(0:1:0)$. Now clearly $x-1, y-x\in\mathbb{Q}[C]^*$ and $\mathrm{div}(x-1)=-(P_1)-2(P_2)+3(P_3)$ and $\mathrm{div}(y-x)=3(P_1)-2(P_2)-(P_1)$. From this we see that $x-1$ and $y-x$ are independent and thus $\mathbb{Q}^*\cdot<x-1>\cdot<y-x>=\mathbb{Q}[C]^*$.

Finally, we give an example where there are more generators over a field extension. Consider the curve C given by $(x^2+y^2)(x^2+2y^2)=1$ over $\mathbb{Q}$. Over $\mathbb{Q}(\sqrt{2},i)$ the points at infinity are $P_1=(i:1:0), P_2:=(-i:1:0), P_3=(\sqrt{2}i:1:0)$ and $P_4=(-\sqrt{2}i:1:0)$. Over $\mathbb{Q},\mathbb{Q}(i),\mathbb{Q}(\sqrt{2},i)$ we now get the following unit groups:

$$\begin{aligned}\mathbb{Q}[C]^* &= \mathbb{Q}^*\cdot<x^2+y^2>\\ \mathbb{Q}(i)[C]^* &= \mathbb{Q}(i)^*\cdot<x+iy>\cdot<x-iy>\\ \mathbb{Q}(\sqrt{2},i)[C]^* &= \mathbb{Q}(\sqrt{2},i)^*\cdot<x+iy>\cdot<x-iy>\cdot<x+\sqrt{2}iy>.\end{aligned}$$

From all of these examples we see that there are many more possibilities for the unit group for nonhyperelliptic curves, than for hyperelliptic curves. As such, it will probably be more difficult to classify the different unit groups that can occur and the torsion points of the Jacobians.

7 Conclusion

In this thesis we have investigated the unit group of the coordinate ring of algebraic curves, and in particular of hyperelliptic curves. Functions in the coordinate ring have finitely many zeros and poles at the points of a curve. Nontrivial units in the coordinate ring are characterized by having all their zeros and poles at the points at infinity. In other words, the support of the divisor of a nontrivial unit is a subset of the set of points at infinity of the curve. This means that certain linear combinations of the points at infinity give a principal divisor and thus the existence of nontrivial units is related to the Jacobian of the curve by requiring that there is a nontrivial linear combination of the points at infinity which is of finite order in the Jacobian. Let K be a field and C a smooth algebraic curve with affine part $C_0 \subset \mathbb{A}^2$ and m points at infinity, then $K[C]^* \cong K^* \times \mathbb{Z}^r$ where $r < m$ is the rank of the unit group.

For hyperelliptic curves there are 2 points at infinity, which we denoted by ∞^+ and ∞^-. Let K be a field of characteristic not 2, then we looked at hyperelliptic curves C given by $y^2 = f(x)$ where $f(x) \in K[x]$ is separable and of degree $2g+1$ or $2g+2$ where g is the genus of C. Using the norm map $N : K[C] \to K[x]$, defined by $N(a + b\sqrt{f}) = a^2 - fb^2$, we found that for the existence of nontrivial units it is required that f has even degree and leading coefficient that is a square in K.

We found the following characterization of the unit group:

$$\begin{aligned} K[C]^* &= \{a + b\sqrt{f} : a, b \in K[x], a^2 - fb^2 \in K^*\} \\ &= \{\phi \in K[C] : \operatorname{div}(\phi) = n(\infty^+) - n(\infty^-) \text{ for some } n \in \mathbb{Z}\} \\ &= K^* \cdot < \varepsilon > . \end{aligned}$$

The generator ε is called a fundamental unit, and we showed that if $\infty^+ - \infty^-$ has order d in $J(C)$, then $\varepsilon = P_d + yP_{d-g-1}$ where $P_d, P_{d-g-1} \in K[x]$ are polynomials of degree $d, d-g-1$ respectively. Orders $d <\leq g$ cannot occur for $\infty^+ - \infty^-$. An interesting result we found is that for $C/\mathbb{Q}$ if ε is given over $\mathbb{Z}$ without a common integer factor in P_d together with P_{d-g-1}, which can always be done, and if p is an odd prime where C has good reduction, then $\varepsilon \mod p$ is a fundamental unit for $\mathbb{F}_p[C]^*$. For a field extension L/K it holds that if the leading coefficient of f is a square in K^*, then $K[C]^* \neq K^*$ if and only if $L[C]^* \neq L^*$, in other words, nontrivial units exist over K if and only if they exist over any field extension of K.

For examples we mostly looked at genus-2 curves over $\mathbb{Q}$ and we tried different methods to find examples. These methods were, brute forcing with Magma, using continued fractions, using mappings to elliptic curves and starting from a unit to construct a hyperelliptic curve. For the existence of nontrvial units it is requried that $\infty^+ - \infty^-$ has finite order in $J(C)$. For the torsion points in the Jacobian, researchers have found examples of genus-2 curves over $\mathbb{Q}$ whose Jacobian have torsion points of order n for $1 \leq n \leq 30$, $32 \leq n \leq 36$ and $n \in \{39, 40, 45, 48, 60, 63, 70\}$. Using Magma we have found genus-2 curves over $\mathbb{Q}$ where $\infty^+ - \infty^-$ has order d for $3 \leq d \leq 15$ and $d \in \{17, 18, 19, 21, 23, 24, 25, 27, 29, 33, 35, 39\}$. With the other methods we have not found any other d's. Using the method of starting from units, we were to parametrize the genus-2 curves where $\infty^+ - \infty^-$ has order 3 and we found 2 different 1-parameter families. For $d = 5$ and 7 we were also able to characterize the curves where $\infty^+ - \infty^-$ has order 5 or 7, but we were unable to see exactly how many different families there are and how many parameters are required. We attempted to do this using Igusa-Clebsch invariants.

For higher genus, the same methods could still work for hyperelliptic curves. For non-hyperelliptic curves there can be more than 2 points at infinity, and this allows for many more possibilities for the unit group. We briefly looked at some examples to see the different kinds of unit groups that can occur. For concrete results, a lot more work will have to be done.

For further research there is still a lot that can be done. We have found many different integers which occur as possible orders of $\infty^+ - \infty^-$, but there are still a lot of integers which are known to occur for the order of torsion points in Jacobians, but of which we do not know yet if they also occur as order of $\infty^+ - \infty^-$ for a certain hyperelliptic curve. The lowest of these integers is 16. At the same time, there also is no n for which we can show that there is no hyperelliptic curve $C/\mathbb{Q}$ of genus g such that $\infty^+ - \infty^-$ has order n in $J(C)$ if $n > g$. Also, the examples we found were mostly over finite fields and over $\mathbb{Q}$. To find examples for other fields, more work needs to be done. Expanding the methods we have used or trying different methods could possibly yield new results.

Finally, we have made a conjecture which says that for the existence of nontrivial units over $\mathbb{Q}$ it is required that f is of the form $a^2x^{2g+2} + 2abx^{2g+1} + (b+2c)x^{2g} + \cdots$ where a, b, c are integers. Here it is assumed that $f \in \mathbb{Z}[x]$ which is always possible for hyperelliptic curves over $\mathbb{Q}$. We have been unable to prove this conjecture, for both hyperelliptic curves and elliptic curves (for elliptic curves the conjecture is slightly different). Further research could be done to try and prove the conjecture.

A Nonsingular Embedding with Quadratic Equations

In this appendix we show that affine curves defined by equations of the form $y^2 = f(x)$ can be used to define hyperelliptic curves.

Let K be a field with $\mathrm{char}(K) \neq 2$. A curve X is defined to be hyperelliptic of genus $g \geq 2$ if there exists a finite morphism $f : X \to \mathbb{P}^1$ of degree 2. Let $f \in K[x]$ be a separable polynomial of degree $2g+1$ or $2g+2$ for some integer $g \geq 2$ and let C_0/K be the affine curve given by the equation $y^2 = f(x)$. Define the map $\phi : C_0 \to \mathbb{P}^{g+2}$ by $\phi(x, y) = (1 : x : x^2 : \cdots : x^{g+1} : y)$ and let C be the projective closure of $\phi(C_0)$. We show that C is smooth, $C \cap \{X_0 \neq 0\} \cong C_0$ and that C is a hyperelliptic curve of genus g.

Let $(u_0 : u_1 : \cdots : u_{g+1} : y)$ be the coordinates in $\mathbb{P}^{g+2}$, then we identify u_i with x^i. For the defining equations of C we will use quadratic relations. For example, for $\phi(C_0)$ we have $u_2 = u_1^2$ and on C this becomes $u_0 u_2 = u_1^2$. This needs to be done for all the relations. To start, we get:

$$\begin{aligned}
u_0 u_2 &= u_1^2 \\
u_0 u_3 &= u_1 u_2 \\
u_0 u_4 &= u_1 u_3 = u_2^2 \\
u_0 u_5 &= u_1 u_4 = u_2 u_3
\end{aligned}$$

In general we have $u_0 u_i = u_j u_{i-j}$ for all i, j with $1 \leq j \leq \lfloor \frac{i}{2} \rfloor$ and $2 \leq i \leq g+1$. The relations that are left are the ones without u_0 in them. From the above relations we can see that they all have to involve u_{g+1}. If $g+1$ is even some of these are the following:

$$\begin{aligned}
u_1 u_{g+1} &= u_2 u_g = u_3 u_{g-1} = \cdots = u_{\frac{g+1}{2}} u_{g+2-\frac{g+1}{2}} \\
u_2 u_{g+1} &= u_3 u_g = u_4 u_{g-1} = \cdots = u_{\frac{g+3}{2}} u_{g+3-\frac{g+3}{2}} \\
u_3 u_{g+1} &= u_4 u_g = u_5 u_{g-1} = \cdots = u_{\frac{g+3}{2}} u_{g+4-\frac{g+3}{2}}
\end{aligned}$$

In general these are the relations $u_i u_{g+1} = u_j u_{g+1+i-j}$ for all i, j with $i+1 \leq j \leq \lfloor \frac{g+1+i}{2} \rfloor$ and $1 \leq i \leq g-1$. These are all the relations of this type that we have. As the affine points of C came from the equation $y^2 = f(x)$, we also need to change this equation into a quadratic one of the form $y^2 = h(u_0, \cdots, u_{g+1})$. There is some choice for this thanks to the above relations. Write $f(x) = \sum_{i=0}^{2g+2} b_i x^i$, then for h we take

$$h(u_0 : \cdots : u_{g+1}) = \sum_{i=0}^{g+1} b_i u_0 u_i + \sum_{i=1}^{g+1} b_{i+g+1} u_i u_{g+1}.$$

All of the quadratic relations combined give the defining equations of C.

A map $\psi : C \cap \{u_0 \neq 0\} \to C_0$ is $\psi(1 : u_1 : \cdots : u_{g+1} : y) = (u_1, y)$. Then ψ is a morphism and $\psi(\phi(x, y)) = (x, y)$ and $\phi(\psi(1 : u_1 : \cdots : u_{g+1} : y)) = (1 : u_1 : u_1^2 : \cdots : u_1^{g+1} : y) = (1 : u_1 : \cdots : u_{g+1} : y)$. As ϕ is a morphism as well, it follows that C_0 and $C \cap \{u_0 \neq 0\}$ are isomorphic. We will usually use the notation $(x, y) \in C$ for the point $\phi(x, y)$ with $(x, y) \in C_0$. The points of C with $u_0 = 0$ are called the points at infinity of C_0. We determine what these points are.

From $u_0u_{2i} = u_i^2$ we get $u_i = 0$ for $i \leq \lfloor \frac{g+1}{2} \rfloor$. From $u_{2i-g-1}u_{g+1} = u_i^2$ we then get $u_i = 0$ for $\lfloor \frac{g+1}{2} \rfloor + 1 \leq i \leq g$. The other relations do not give any more information. Next, from $y^2 = h(u_0, \cdots, u_{g+1})$ we get $y^2 = bu_{g+1}^2$ where $b = 0, b_{2g+2}$ depending on the parity of the degree of f. Hence, the points at infinity are $(0 : \cdots : 0 : 1 : \pm\sqrt{b_{2g+2}})$ if $\deg(f)$ is even and it is $(0 : \cdots : 0 : 1 : 0)$ if $\deg(f)$ is odd. For notation we will use $\infty^+ = (0 : \cdots : 0 : 1 : \sqrt{b_{2g+2}})$, $\infty^- = (0 : \cdots : 0 : 1 : -\sqrt{b_{2g+2}})$ and $\infty = (0 : \cdots : 0 : 1 : 0)$.

Next we show that C is smooth. We first take the open part $(u \neq 0)$. For the smoothness of the affine points we don't need all the relations, we will only use $u_i - u_1u_{i-1} = 0$ for $2 \leq i \leq g+1$. The matrix of derivatives of these relations and $y^2 - h = 0$ in a point $(P : y)$ where $P = (u_1 : \cdots : u_{g+1})$ is:

$$A := \begin{pmatrix} \frac{\partial h}{\partial u_1}(P) & \frac{\partial h}{\partial u_2}(P) & \frac{\partial h}{\partial u_3}(P) & \frac{\partial h}{\partial u_4}(P) & \frac{\partial h}{\partial u_5}(P) & \cdots & \frac{\partial h}{\partial u_{g+1}}(P) & -2y \\ -2u_1 & 1 & 0 & \cdots & & & & 0 \\ -u_2 & -u_1 & 1 & 0 & \cdots & & & 0 \\ -u_3 & 0 & -u_1 & 1 & 0 & \cdots & & 0 \\ \vdots & \vdots & & & & & & \vdots \\ -u_g & 0 & \cdots & & 0 & -u_1 & 1 & 0 \end{pmatrix}$$

The rank of this matrix needs to be $g+1$. All the columns with a 1 in them are all linearly independent and there are g of these. Also, if $y \neq 0$, then the last $g+1$ columns are linearly independent and so the point is smooth. Now suppose $y = 0$. Let B be the minor of A consisting of all rows and columns of A except the first row and last column, then the columns of B are linearly dependent. Denote the columns of B by $v_1, \cdots v_{g+1}$. We want to write $v_1 = \sum_{i=2}^{g+1} a_i v_i$ with $a_i \in K$. From the structure of B we must have that $a_2 = -2u_1$. Then $-u_2 = a_3 - a_2u_1 = a_3 + 2u_1^2$, so $a_3 = -u_2 - 2u_1^2 = -3u_2$. Next we get $a_4 = -u_3 - 3u_2u_1 = -4u_3$. This continues on like this and we find that $a_i = -iu_{i-1}$. So we have that $v_1 = \sum_{i=2}^{g+1} -iu_{i-1}v_i$.

Now we want to know if the same holds in A, so if $\frac{\partial h}{\partial u_1}(P) = \sum_{i=2}^{g+1} -iu_{i-1}\frac{\partial h}{\partial u_i}(P)$. Here we are in the open part $(u_0 \neq 0)$, so here

$$h(u_1, \cdots, u_{g+1}) = b_0 + \sum_{i=1}^{g+1} b_i u_i + \sum_{i=1}^{g+1} b_{i+g+1} u_i u_{g+1}.$$

Then $\frac{\partial h}{\partial u_i} = b_i + b_{i+g+1}u_{g+1}$ if $i \neq g+1$ and $\frac{\partial h}{\partial u_{g+1}} = b_{g+1} + \sum_{i=1}^{g} b_{i+g+1}u_i + 2b_{2g+2}u_{g+1}$. If we now substitute back $u_i = x^i$, then we get

$$
\begin{aligned}
\frac{\partial h}{\partial u_1} + \sum_{i=2}^{g+1} i u_{i-1} \frac{\partial h}{\partial u_i} &= b_1 + b_{g+2} u_{g+1} + \sum_{i=2}^{g} i u_{i-1}(b_i + b_{i+g+1} u_{g+1}) \\
&+ (g+1) u_g (b_{g+1} + \sum_{i=1}^{g} b_{i+g+1} u_i + 2 b_{2g+2} u_{g+1}) \\
&= b_1 + b_{g+2} x^{g+1} + \sum_{i=2}^{g} i x^{i-1}(b_i + b_{i+g+1} x^{g+1}) \\
&+ (g+1) x^g (b_{g+1} + \sum_{i=1}^{g} b_{i+g+1} x^i + 2 b_{2g+2} x^{g+1}) \\
&= \sum_{i=1}^{g} i b x^{i-1} + b_{g+2} x^{g+1} + \sum_{i=2}^{g} i b_{i+g+1} x^{g+i} \\
&+ \sum_{i=1}^{g} (g+1) b_{i+g+1} x^{g+i} + 2(g+1) b_{2g+2} x^{2g+1} \\
&= \sum_{i=1}^{2g+2} b_i x^{i-1} \\
&= \frac{\partial f}{\partial x}.
\end{aligned}
$$

Now, for the point P we have $h(P) = 0$. Also, P corresponds with a point $Q = x_0$ in K for which we have $f(x_0) = 0$. Then $\frac{\partial f}{\partial x}(x_0) \neq 0$ if and only if x_0 is not a double root of f. So $\frac{\partial h}{\partial u_1}(P) + \sum_{i=2}^{g+1} i u_{i-1} \frac{\partial h}{\partial u_i}(P) \neq 0$ if and only if x_0 is not a double root of f. Thus all points in the open part $(u_0 \neq 0)$ are smooth if and only if f is separable.

Now for the points at infinity, the points $(0 : \cdots : 0 : 1 : \pm\sqrt{b_{2g+2}})$ if $\deg(f)$ is even and $(0 : \cdots : 0 : 1 : 0)$ if $\deg(f)$ is odd. For the smoothness of these points we take the open part $(u_{g+1} \neq 0)$. For notation we use $h(0) := h(0 : \cdots : 0 : 1)$. In this open part, let $R = (0, \cdots, 0, y_0)$ be a point on C. For the smoothness we use the relations $u_0 - u_1 u_g = 0$ and $u_i - u_{i+1} u_g = 0$ for $1 \leq i \leq g-1$. The matrix of derivatives for these relations and $y^2 - h = 0$ is here in R:

$$
\begin{pmatrix}
\frac{\partial h}{\partial u_0}(0) & \frac{\partial h}{\partial u_1}(0) & \frac{\partial h}{\partial u_2}(0) & \cdots & \frac{\partial h}{\partial u_{g-1}}(0) & \frac{\partial h}{\partial u_g}(0) & -2y_0 \\
1 & 0 & 0 & \cdots & 0 & 0 & 0 \\
0 & 1 & 0 & \cdots & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & \cdots & 0 & 0 \\
\vdots & \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & 0 & 1 & 0 & 0
\end{pmatrix}
$$

If $\deg(f)$ is even, then $y_0 \neq 0$, so the matrix has rank $g+1$. If $\deg(f)$ is odd, then $h = u_g u_{g+1} + h_0(u_0 : \cdots : u_g)$ for some quadratic homogeneous polynomial h_0, so $\frac{\partial h}{\partial u_g}(0) \neq 0$, thus the matrix has rank $g+1$ in this case as well. This shows that the points at infinity are always smooth. We conclude that the curve C given by $y^2 = h(u_0, \cdots, u_{g+1})$ and the relations $u_0 u_i = u_j u_{i-j}$, for $i \leq j \leq \lfloor \frac{i}{2} \rfloor$ and $2 \leq i \leq g+1$, and $u_i u_{g+1} = u_j u_{g+1+i-j}$ for $i+1 \leq j \leq \lfloor \frac{g+1+i}{2} \rfloor$ and $1 \leq i \leq g-1$ is nonsingular if and only if the corresponding affine curve C_0 given by $y^2 = f(x)$ is nonsingular, which is equivalent to f being separable.

Now to show that C is hyperelliptic. We define the map $\tau : C \to \mathbb{P}^1$ by $\tau(P) = [x, 1]$ if $P \in C \cap \{u_0 \neq 0\}$ and where $\psi(P) = (x, y) \in C_0$ and $\tau(P) = [0, 1]$ if P is a point at infinity. Then τ is a morphism and for the corresponding map of function fields $\tau^* : K(\mathbb{P}^1) \to K(C)$ we get $\tau^*(K(\mathbb{P}^1)) = K(x)$. For the function field of C we get $K(C) \equiv K(C_0)$ as $C \cap \{u_0 \neq 0\} \equiv C_0$. As $K(C_0) = K(x, \sqrt{f})$ we find that $\deg(\tau) = [K(C) : \tau^*(K(\mathbb{P}^1))] = 2$. This shows that C is hyperelliptic.

For the genus of C we use the Riemann-Roch theorem 2.1. We will find a canonical divisor on C and determine its degree which is equal to $2g - 2$ where g is the genus of C. We take the function $x \in K(C_0)$ and we claim that $\operatorname{div}(dx)$ is a canonical divisor. For this we only need to show that it is nonzero. We will use that $dx = d(x - \alpha) = -x^2 d(\frac{1}{x})$ for any $\alpha \in \overline{K}$ and proposition 2.1d.

Let $P = (\alpha, \beta) \in C$, then $(x - \alpha)(P) = 0$. If $\beta \neq 0$, then $\operatorname{ord}_P(x - \alpha) = 1$ and thus by proposition 2.1 we have $\operatorname{ord}_P(d(x - \alpha)) = 0$. If $\beta = 0$, then $\operatorname{ord}_P(x - \alpha) = 2$ and so $\operatorname{ord}_P(d(x - \alpha)) = 1$. Write $f(x) = b_d \prod_{i=1}^{d}(x - \alpha_i)$ with $\alpha_i \in \overline{K}$ where $d = \deg(f)$, then $\operatorname{ord}_P(d(x - \alpha)) = 1$ only if $\alpha = \alpha_j$ for some j.

Now suppose that P is a point at infinity. We then have that $\frac{1}{x}(P) = 0$. If d is odd, so $d = 2g + 1$ for some $g \in \mathbb{Z}_{>1}$, then $P = \infty$ and $\operatorname{ord}_\infty(\frac{1}{x}) = 2$. As $\operatorname{char}(K) \neq 2$ we can use proposition 2.1 to get $\operatorname{ord}_\infty(dx) = \operatorname{ord}_\infty(-x^2 d(\frac{1}{x})) = -4 + 2 - 1 = -3$. We thus get $\operatorname{div}(dx) = \sum_{i=1}^{2g+1}(\alpha_i, 0) - 3\infty$. Then $\deg(\operatorname{div}(dx)) = 2g - 2$ and thus the genus of C is g.

If d is even, so $d = 2g + 2$ for some $g \in \mathbb{Z}_{>1}$, then $P = \infty^+$ or $P = \infty^-$ and $\operatorname{ord}_P(\frac{1}{x}) = 1$. For the differential we then get $\operatorname{ord}_P(dx) = \operatorname{ord}_P(-x^2 d(\frac{1}{x})) = -2 + 1 - 1 = 2$. The divisor is then $\operatorname{div}(dx) = \sum_{i=1}^{2g+2}(\alpha_i, 0) - 2\infty^+ - 2\infty^-$. Then $\deg(\operatorname{div}(dx)) = 2g - 2$ and thus the genus of C is g.

B Magma Codes

In this section we present more Magma code that is used for examples.

B.1 Finding units by taking modulo primes

This code is an alternative to finding the unit group of a hyperelliptic curve over $\mathbb{Q}$. The code works by finding two primes of good reduction, computing the order of $\infty^+ - \infty^-$ in the Jacobian over the curve modulo these primes and comparing if they are the same. If they are the same order d, the dimension of $\mathcal{L}(d(\infty^+ - \infty^-))$ is checked. If it is nonzero, the output is the order d and a basis for $\mathcal{L}(d(\infty^+ - \infty^-))$. If the dimension is zero or if different orders are found modulo the primes then no output is given.

```
K:=Rationals();
P<x>:=PolynomialRing(K);
b:=1;
f:=b^2*x^6+1;
//f any separable polynomial of even degree with leading coefficient b^2
i:=2;
j:=0;
d:=[0,0];

while j le 2 do
i:=NextPrime(i);
Fp:=GF(i);
R<x>:=PolynomialRing(Fp);
fp:=R!(f);
a:=IsHyperellipticCurve([fp,0]);
if a eq true and b mod i ne 0 then
j:=j+1;
else;
continue;
end if;
C:=HyperellipticCurve(fp);
inf1:=C![1,b,0];
inf2:=C![1,-b,0];
//inf1 and inf2 are how Magma sees the points at infinity
d[j]:=Order(inf1-inf2);
end while;

if d[1] eq d[2] then
C:=HyperellipticCurve(f);
inf1:=C![1,b,0];
inf2:=C![1,-b,0];
D1:=Divisor(inf1);
D2:=Divisor(inf2);
D:=D1-D2;
```

```
F<x,y>:=FunctionField(C);
R:=RiemannRochSpace(d[1]*D);
if Dimension(R) ne 0 then
d[1];
Basis(d[1]*D)[1];
end if;
end if;
```

B.2 Finding units by for loop

This Magma code is another alternative to finding the unit group of a hyperelliptic curve over $\mathbb{Q}$. This code works by finding a prime p of good reduction and computing the classnumber h of the curve over $\mathbb{F}_p$, which is the number of elements of the Jacobian. As the order of $\infty^+ - \infty^-$ must be a divisor of h, a for loop is used to check the dimension of $\mathcal{L}(d(\infty^+ - \infty^-))$ for each divisor d of h. As soon this dimension is nonzero the for loop is stopped and the output is the order d and a basis for $\mathcal{L}(d(\infty^+ - \infty^-))$. If for each d the dimension of $\mathcal{L}(d(\infty^+ - \infty^-))$ is zero, then no output is given.

```
K:=Rationals();
b:=1;
P<x>:=PolynomialRing(K);
f:=b^2*x^6+1;
//f any separable polynomial of even degree with leading coefficient b^2
i:=2;
j:=0;

while j le 1 do
i:=NextPrime(i);
Fp:=GF(i);
R<x>:=PolynomialRing(Fp);
fp:=R!(f);
a:=IsHyperellipticCurve([fp,0]);
if a eq true and b mod i ne 0 then
j:=j+1;
else;
continue;
end if;
C:=HyperellipticCurve(fp);
h:=ClassNumber(C);
end while;

C:=HyperellipticCurve(f);
inf1:=C![1,1,0];
inf2:=C![1,-1,0];
D1:=Divisor(inf1);
D2:=Divisor(inf2);
D:=D1-D2;
F<x,y>:=FunctionField(C);
for d in Divisors(h) do
R:=RiemannRochSpace(d*D);
if Dimension(R) ne 0 then
d;
Basis(d*D)[1];
break;
end if;
end for;
```

B.3 Brute Force Method

The following Magma code is used to determine what kind of orders appear for $\infty^+ - \infty^-$ in $J(C)$ for hyperelliptic curves C of genus 2 given by $y^2 = f$ where $\deg(f) = 6$ and the coefficients of f are small (less than 10 in absolute values). The output of the code is a list with all found orders and for each order a list with the coefficients of an f plus the order for which the given order occurs as order of $\infty^+ - \infty^-$. The for-loop for i only needs to go from -10 to 0 instead of 10 because by the coordinate transformation $x \mapsto -x$ we get the results for positive i. Note that this code takes many hours to run.

```
K:=Rationals();
Orderlist:=[];
r:=0;
for b:=1 to 3 do
for i:=-10 to 0 do
for j:=-10 to 10 do
for k:=-10 to 10 do
for l:=-10 to 10 do
for m:=-10 to 10 do
for n:=-10 to 10 do
P<x>:=PolynomialRing(K);
f:=b^2*x^6+i*x^5+j*x^4+k*x^3+l*x^2+m*x+n;
a:=IsHyperellipticCurve([f,0]);
if a eq true then
C:=HyperellipticCurve(f);
inf1:=C![1,b,0];
inf2:=C![1,-b,0];
d:=Order(inf1-inf2);
if d ne 0 then
D1:=Divisor(inf1);
D2:=Divisor(inf2);
D:=d*(D1-D2);
R:=RiemannRochSpace(D);
if Dimension(R) ne 0 then
if d in Orderlist then
continue;
end if;
r:=r+1;
Orderlist[r]:=d;
<b^2,i,j,k,l,m,n,d>;
end if;
end if;
end if;
end for;
end for;
end for;
end for;
end for;
```

```
i;
end for;
Orderlist;
```

Adding in what conjecture 5.1 gives as requirement for the existence of nontrivial units reduces the run time significantly. This can be done by adding

```
if i mod b ne 0 then
i;
continue;
end if;
```

after the second for-loop and

```
if Integers()!(i/b) mod 2 ne j mod 2 then
continue;
end if;
```

after the third for-loop.

The following code can instead be used to get all the hyperelliptic curves with nontrivial units that are found. Due to the high run time and the high amount of curves found, there are less for-loops here. The run time is around 30 minutes. One can also add another for loop for the constant coefficient or the square leading coefficient, but this makes it take much longer to run.

```
K:=Rationals();
b:=1;
for i:=-10 to 0 do
for j:=-10 to 10 do
for k:=-10 to 10 do
for l:=-10 to 10 do
for m:=-10 to 10 do
P<x>:=PolynomialRing(K);
f:=b^2*x^6+i*x^5+j*x^4+k*x^3+l*x^2+m*x+1;
a:=IsHyperellipticCurve([f,0]);
if a eq true then
C:=HyperellipticCurve(f);
inf1:=C![1,b,0];
inf2:=C![1,-b,0];
d:=Order(inf1-inf2);
if d ne 0 then
D1:=Divisor(inf1);
D2:=Divisor(inf2);
D:=d*(D1-D2);
R:=RiemannRochSpace(D);
if Dimension(R) ne 0 then
<b,i,j,k,l,m,d>;
```

```
end if;
end if;
end if;
end for;
end for;
end for;
end for;
end for;
```

B.4 Igusa-Clebsch Invariants

The Magma code here is used to help compute the dimension of the image of $\psi : \mathbb{A}^3 - \to \mathbb{A}^3$ given by $\psi(a, b, c) = (i_1, i_2, i_3)$ where i_1, i_2, i_3 are the Igusa-Clebsch invariants of the genus hyperelliptic curve. As the dimension of the full image is too difficult too compute, most of the time, the dimension is only computed for a particular subset of $\mathbb{A}^3$. In particular, the Magma code presented here is used for the 7-torsion example in subsection 5.4, but it can easily be adapted to other curves.

```
F<b,c>:=FunctionField(Rationals(),2);
P<x>:=PolynomialRing(F);
a:=0;
f:=(-c+2*b*x)*(2*b*x^5+(4*a*b-c)*x^4+(2*a^2*b+4*b^2-2*a*c)*x^3
+(4*a*b^2-a^2*c+2*b*c)*x^2+(2*b^3+2*a*b*c-2*c^2)*x+(3*b^2*c-2*a*c^2));
C:=HyperellipticCurve(f);
I:=IgusaClebschInvariants(C);
I2:=I[1];
I4:=I[2];
I6:=I[3];
I10:=I[4];
i1:=I2^5/I10;
i2:=I2^3*I4/I10;
i3:=I2^2*I6/I10;
A2<b,c>:=AffineSpace(Rationals(),2);
A3<x,y,z>:=AffineSpace(Rationals(),3);
phi:=map<A2->A3|[i1,i2,i3]>;
Dimension(Image(phi));
```

B.5 3-Torsion parametrization

The Magma code in this section is used for the parametrization of 3-torsion of $\infty^+ - \infty^-$ in subsection 5.4. We start with the curve given by $y^2 = (x^3 - x)(x^3 + ax^2 + bx + c)$.

```
Qabc<a,b,c>:=FunctionField(Rationals(),3);
P<x>:=PolynomialRing(Qabc);
C:=HyperellipticCurve((x^3+a*x^2+b*x+c)*(x^3-x));
J:=Jacobian(C);
inf12:=C![1,-1,0];
inf21:=C![1,1,0];
D:=Divisor([<Place(inf1),1>,<Place(inf2),-1>]);
JD:=J!D;
R:=(2*JD)[1];
R;
Denominator(ConstantCoefficient(R));
```

After solving when this denominator is zero for c, we substitute it back into the equation. It gives $c = \frac{-16+8a^2-5a^4-32b+24a^2b-16b^2}{32a}$.

```
Qabc<a,b>:=FunctionField(Rationals(),2);
P<x>:=PolynomialRing(Qabc);
c:=-(1/32)*(5*a^4-24*a^2*b-8*a^2+16*b^2+32*b+16)/a;
C2:=HyperellipticCurve((x^3+a*x^2+b*x+c)*(x^3-x));
J2:=Jacobian(C2);
inf22:=C2![1,-1,0];
inf12:=C2![1,1,0];
D2:=Divisor([<Place(inf12),1>,<Place(inf22),-1>]);
JD2:=J2!D2;
R2:=(2*JD2)[1];
R2;
Denominator(ConstantCoefficient(R2));
```

We solve again when this denominator is zero, but now for b. This gives $b = -1 + \frac{a^2}{4}, -1 - a + \frac{a^2}{4}$ or $-1 + a + \frac{a^2}{4}$. Substituting $b = -1 + \frac{a^2}{4}$ into the equation we get the last part of the Magma codes. This shows that $2(\infty^+ - \infty^-) = -(\infty^+ - \infty^-)$ in $J(C)$ and gives a generating unit.

```
Qabc<a>:=FunctionField(Rationals());
P<x>:=PolynomialRing(Qabc);
b:=1/4 *(-4 + 4* a + a^2);
c:=-(1/32)*(5*a^4-24*a^2*b-8*a^2+16*b^2+32*b+16)/a;
C3:=HyperellipticCurve((x^3+a*x^2+b*x+c)*(x^3-x));
F<x,y>:=FunctionField(C3);
J3:=Jacobian(C3);
inf23:=C3![1,-1,0];
inf13:=C3![1,1,0];
D3:=Divisor([<Place(inf13),1>,<Place(inf23),-1>]);
```

```
JD3:=J3!D3;
-JD3;
2*JD3;
Basis(3*D3);
```

B.6 General Curves with mod p

The Magma code here is used to check if the curve in subsection 6.2, the curve given by $(x-my)^2(x-ny)^2+z^4+y^3z=0$ with $m \neq n$, always has good reduction modulo a certain prime and when two such primes are known to check if the order of $\infty^+ - \infty^-$ modulo both primes are ever the same. If this happens, we check if $\infty^+ - \infty^-$ has the same order over $\mathbb{Q}$. The following code checks the good reduction.

```
p:=7;
K:=GF(p);
PK<x,y,z>:=ProjectiveSpace(K,2);
for m:=0 to p-1 do
for n:=0 to m-1 do
Q:=Rationals();
R<x,y,z>:=PolynomialRing(Q,3);
PQ<x,y,z>:=ProjectiveSpace(Q,2);
f:=(x-m*y)^2*(x-n*y)^2+z^4+y^3*z;
CQ:=Curve(PQ,f);
if IsNonSingular(CQ) eq false then
continue;
else
C:=Curve(PK,f);
if IsNonSingular(C) eq true then
else
<p,m,n>;
break;
end if;
end if;
end for;
end for;
```

For $p=5,7$ the curve has good reduction. The following code checks the order of $\infty^+ - \infty^-$ modulo both primes, and if they are equal it checks if $\infty^+ - \infty^-$ has the same order over $\mathbb{Q}$.

```
for m:=0 to 34 do
for n:=0 to m-1 do

Q:=Rationals();
R<x,y,z>:=PolynomialRing(Q,3);
PQ<x,y,z>:=ProjectiveSpace(Q,2);
f:=(x-m*y)^2*(x-n*y)^2+z^4+y^3*z;
CQ:=Curve(PQ,f);
if IsNonSingular(CQ) eq false then
continue;
end if;

p1:=5;
K1:=GF(p1);
```

```
PK1<x,y,z>:=ProjectiveSpace(K1,2);
CK1:=Curve(PK1,f);

p2:=7;
K2:=GF(p2);
PK2<x,y,z>:=ProjectiveSpace(K2,2);
CK2:=Curve(PK2,f);

inf11:=CK1![m,1,0];
inf12:=CK1![n,1,0];
FC1<a,b>:=FunctionField(CK1);
h1:=ClassNumber(CK1);

inf21:=CK2![m,1,0];
inf22:=CK2![n,1,0];
FC2<a,b>:=FunctionField(CK2);
h2:=ClassNumber(CK2);
s:=Gcd(h1,h2);

if s eq 1 then
continue;
end if;

i1:=-1;
i2:=-2;

d1:=Divisor(CK1,[<Place(inf11),1>,<Place(inf12),-1>]);
for i in Divisors(s) do
j1:=IsPrincipal(i*d1);
if j1 eq true then
i1:=i;
break;
end if;
end for;

d2:=Divisor(CK2,[<Place(inf21),1>,<Place(inf22),-1>]);
for i in Divisors(s) do
j2:=IsPrincipal(i*d2);
if j2 eq true then
i2:=i;
break;
end if;
end for;

if i1 eq i2 then
<m,n,i1>;
infQ1:=CQ![m,1,0];
```

```
infQ2:=CQ![n,1,0];
FC<a,b>:=FunctionField(CQ);
d:=Divisor(CQ,[<Place(infQ1),1>,<Place(infQ2),-1>]);
IsPrincipal(i1*d);
end if;

end for;
m;
end for;
```

References

[1] William W. Adams and Michael J. Razar. Multiples of points on elliptic curves and continued fractions. *Proc. London Math. Soc.*, 41(3):481–498, 1980.

[2] Ivan Boyer. *Variétés abéliennes et jacobiennes de courbes hyperelliptiques, en particulier à multiplication réelle ou complexe.* PhD thesis, Université Paris VII - Denis Diderot, 2013.

[3] Noam D. Elkies. Curves of genus 2 over q whose jacobians are absolutely simple abelian surfaces with torsion points of high order. `http://www.math.harvard.edu/~elkies/g2_tors.html`. Retrieved 06-08-2014.

[4] E. V. Flynn. Large rational torsion on abelian varieties. *Journal of Number Theory*, 36:257–265, 1990.

[5] Robin Hartshorne. *Algebraic geometry.* Graduate Texts in Mathematics. Springer, 1997.

[6] Everett W. Howe. Genus-2 jacobians with torsion points of large order. `http://arxiv.org/abs/1407.2654`, 2014.

[7] Everett W. Howe, Franck Leprévost, and Bjorn Poonen. Large torsion subgroups of split jacobians of curves of genus two or three. *Forum Math*, pages 315–364, 2000.

[8] Jun-Ichi Igusa. Arithmetic variety of moduli for genus two. *Annals of Mathematics*, 72(3):612–649, 1960.

[9] 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.

[10] 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 Math.*, 313(11):771–774, 1991.

[11] Franck Leprévost. Torsion sur des familles de courbes de genre g. *Manuscripta Math.*, 75(3):303–326, 1992.

[12] Franck Leprévost. Jacobiennes de certaines courbes de genre 2: torsion et simplicité. *Journal de Theorie des Nombres de Bordeaux*, 7(1):283–306, 1995.

[13] Franck Leprévost. Sur une conjecture sur les points de torsion rationnels des jacobiennes de courbes. *J. Reine Angew. Math.*, 473:59–68, 1996.

[14] Barry Mazur. Modular curves and the eisenstein ideal. *Publications Mathematiques de l' I.H.E.S.*, 47:33–186, 1977.

[15] Barry Mazur. Rational points of modular curves. *Modular Functions of One Variable V, Lecture Notes in Math.*, 601:107–148, 1977.

[16] J. F. Mestre. Construction de courbes de genre 2 à partir de leurs modules. *Mathematical Programming*, 94:313–334, 1991.

[17] J. S. Milne. Abelian varieties (v2.00), 2008. Available at www.jmilne.org/math/.

[18] J. S. Milne. Algebraic geometry (v5.22), 2012. Available at www.jmilne.org/math/.

[19] David Mumford. *Tata lectures on theta II.* Progress in Mathematics. Jacobian theta functions and differential equations. Birkhäuser Boston Inc., 1984. With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura.

[20] Hiroyuki Ogawa. Curves of genus 2 with a rational torsion divisor of order 23. *Proc. Japan Acad. Ser. A Math. Sci.*, 70(3):295–298, 1994.

[21] Frans Oort. Units in number fields and in function fields. *Expositiones Mathematicae*, 17:97–116, 1999.

[22] V. P. Platonov and M. M. Petrunin. New orders of torsion points in jacobians of curves of genus 2 over the rational number field. *Dokl. Math.*, 85(2):286–288, 2012.

[23] V. P. Platonov and M. M. Petrunin. On the torsion problem in jacobians of curves of genus 2 over the rational number field. *Dokl. Math.*, 86(2):642–643, 2012.

[24] Zachary L. Scherr. *Rational polynomial Pell equations.* PhD thesis, The University of Michigan, 2013.

[25] A. Schinzel. On some problems of the arithmetical theory of continued fractions. *Acta Arithmetica*, VI:393–413, 1961.

[26] Wolfgang M. Schmidt. On continued fractions and diophantine approximation in power series fields. *Acta Arithmetica*, XCV(2), 2000.

[27] T. Shaska, N. Pjero, and M. Ramasaço. Degree even coverings of elliptic curves by genus 2 curves. *Albanian Journal of Mathematics*, 2(3):241–248, 2008.

[28] Alice Silverberg. *Open Questions in Arithmetic Algebraic Geometry*, volume 9 of *IAS/Park City Mathematics Series*, pages 83–142. American Mathematical Society, 2001.

[29] Joseph H. Silverman. *The arithmetic of elliptic curves.* Graduate Texts in Mathematics. Springer Science+Business Media, second edition, 2009.

[30] P. Stevenhagen. Number rings. `http://websites.math.leidenuniv.nl/algebra/ant.pdf`, 2012.

[31] Jaap Top. A remark on the rank of jacobians of hyperelliptic curves over q over certain elementary abelian 2-extensions. *Tohoku Mathematical Journal*, 1988.

[32] William A. Webb and Hisashi Yokota. Polynomial pell's equation. In *Proceedings of the American Mathematical Society*, volume 131, pages 993–1006, 2002.