Beilinson's Conjectures for Superelliptic Curves

Dissertation
zur Erlangung des Doktorgrades
der Fakultät für Mathematik, Informatik
und Naturwissenschaften
der Universität Hamburg

vorgelegt im
Fachbereich Mathematik

von
Dipl. Math. Vincenz Busch

aus
Hamburg

Hamburg
2016

Als Dissertation angenommen vom Fachbereich
Mathematik der Universität Hamburg

Auf Grund der Gutachten von Prof. Dr. Ulf Kühn

und Prof. Dr. Tim Dokchitser

Hamburg, den 21.09.2016

Prof. Dr. Bernd Siebert
Leiter des Fachbereichs Mathematik

Contents

Introduction

This thesis is concerned with numerical tests for the Beilinson conjectures for algebraic curves. We focus on superelliptic curves. We show in detail how to determine all invariants, including local L-factors at primes of bad reduction and the conductor, necessary to numerically calculate special values of the L-function of such curves using the algorithms described by Dokchitser [18]. We also explain how to calculate the regulator pairing for arbitrary superelliptic curves using numerical integration algorithms, but not with the same level of detail, as we dedicate to the L-functions. We are also able to bring both worlds together in one class of examples. For one member of this class we numerically calculate the Beilinson regulator and numerically check Beilinson's conjecture. We do not make an analysis of the acquired precision and we integrate close to poles, the numerical results of this thesis are unfortunately not satisfactory.

Let K be a number field, $\zeta_K(s)$ the Dedekind zeta function and R_K the regulator of K. The class number formula for the ring of integers $\mathcal{O}_K$ is given by

$$\operatorname*{Res}_{s=1}(\zeta_K) = \frac{2^{r_1}(2\pi)^{r_2}}{w|\,\mathrm{d}_K\,|^{1/2}}\,|\,\mathrm{Cl}(K)|\ \mathrm{R}_K\,.$$

Here, w denotes the number of roots of unity of K, d_K the discriminant of K, $|\,\mathrm{Cl}(K)|$ the class number of K, r_1 the number of real embeddings of K, and r_2 the number of pairs of complex embeddings. For a more detailed introduction to these invariants of the number field K we refer to the first chapter of the thesis. If we include the zeta factor at infinity and consider the completed Dedekind zeta function Z_K, the formula even simplifies:

$$\operatorname*{Res}_{s=1}(\mathrm{Z}_K) = \frac{2^r}{w}\,|\,\mathrm{Cl}(K)|\ \mathrm{R}_K, \tag{0.0.1}$$

where $r = r_1 + r_2$ denotes the number of places at infinity. The Beilinson conjectures are a generalization of formula (0.0.1) to algebraic K-theory. In short, for a wide variety of objects O, e.g. a number field K or ring of integers $\mathcal{O}_K$, and an integer $n \in \mathbb{Z}$ there exist groups $\mathrm{K}_n(O)$. In this thesis algebraic K-theory of non-singular, projective, geometrically irreducible curves over number fields plays a central role. Roughly, Beilinson's conjectures compare two invariants of curves, namely $\Lambda(C,0)$, the special value of the completed L-function of the curve C at 0, and R_C, the regulator of C. The conjecture states that these two values differ only by a non-zero rational number Q:

$$\Lambda(C,0) = Q\,\mathrm{R}_C\,. \tag{0.0.2}$$

We now explain the Beilinson conjectures (0.0.2) in more detail: Let $\mathcal{O}_K$ be the ring of integers of K and $\mathfrak{p}$ be a prime of $\mathcal{O}_K$. Let C be a smooth, projective irreducible curve over K. All curves in this thesis are smooth projective curves, but for simplicity we often work with affine equations. The curve can be reduced modulo $\mathfrak{p}$ by reducing the defining polynomial of C modulo $\mathfrak{p}$. We refer to the reduced curve by $C_{\mathfrak{p}}$. Even though the original curve C is irreducible and non-singular the reduced curve does not need to be irreducible or non-singular. At each prime $\mathfrak{p}$ we can use $C_{\mathfrak{p}}$ to define a polynomial $\mathrm{L}_{\mathfrak{p}}(C,t) \in K[t]$. Taking the product over the inverses of these polynomials defines the L-function of C.

$$\mathrm{L}(s) = \prod_{\mathfrak{p}\text{ prime}} \mathrm{L}_{\mathfrak{p}}(C, p^{-s})^{-1}$$

This L-function converges for all $s \in \mathbb{C}$ with $\mathrm{Re}(s) > \frac{3}{2}$.

The L-function has been proven to be an important function connected to the curve C and there are a lot of conjectures involving it. It is conjectured that the L-function can be made into an entire function $\Lambda(C,s)$ by multiplication with factors at infinity with remarkable properties. The function $\Lambda(C,s)$ is called the completed L-function.

The second invariant that we need of C is the regulator. To define the regulator we need the notion of the K_2-group of a curve. The general definition of higher K-groups is rather complicated and is not part of this thesis. Instead we use a famous theorem of Matsumoto which states that if F is a field, then

$$K_2(F) = F^* \otimes_{\mathbb{Z}} F^* / \langle a \otimes (1-a), a \in F, a \neq 0, 1 \rangle,$$

where $\langle \cdot\,, \cdot \rangle$ denotes the subgroup generated by the elements indicated. With this definition we can define for a regular model $\mathcal{C}$ of C over $\mathcal{O}_K$ a certain group $\mathrm{K}_2^{\mathrm{T}}(\mathcal{C})$ as the kernel

$$\mathrm{K}_2^{\mathrm{T}}(\mathcal{C}) = \ker\left(\mathrm{K}_2(K(C)) \xrightarrow{T} \bigoplus_{\mathcal{D}} \mathbb{F}(\mathcal{D})^* \right),$$

where $K(C)$ is the function field of C, $\mathcal{D}$ runs through all irreducible components of $\mathcal{C}$, $\mathbb{F}(\mathcal{D})$ stands for the residue field at $\mathcal{D}$, and the map T is the tame symbol at x defined by

$$T_{\mathcal{D}} : \{a, b\} \mapsto (-1)^{v_{\mathcal{D}}(a)v_{\mathcal{D}}(b)} \frac{a^{v_{\mathcal{D}}(b)}}{b^{v_{\mathcal{D}}(a)}}(\mathcal{D}) .$$

It turns out that $\mathrm{K}_2^{\mathrm{T}}(\mathcal{C})$ is independent of the choice of $\mathcal{C}$.

We further ignore torsion by defining

$$\mathrm{K}_2(\mathrm{C}; \mathcal{O}_{\mathrm{K}}) = \mathrm{K}_2^{\mathrm{T}}(\mathcal{C})\,/\text{torsion}.$$

We fix an embedding $K \to \mathbb{C}$ and consider C as an curve over $\mathbb{C}$. Let $X = C(\mathbb{C})$ be the Riemann surface consisting of all complex points of C and let $\mathrm{H}_1(X;\mathbb{Z})^-$ denote the part of the homology $\mathrm{H}_1(X;\mathbb{Z})$ of X that is antiinvariant under complex conjugation. The regulator pairing is defined by

$$\langle \cdot\,, \cdot \rangle : \mathrm{H}_1(X;\mathbb{Z})^- \times \mathrm{K}_2(\mathrm{C}; \mathcal{O}_{\mathrm{K}}) \to \mathbb{R} .$$

Now that we have introduced all necessary notation we can state the Beilinson conjectures for K_2 of curves.

Conjecture 0.0.1 (Beilinson conjectures for K_2 of curves)**.** Let $d = [K : \mathbb{Q}]$ be the degree of K over $\mathbb{Q}$ and let g be the genus of C.

1. The group $\mathrm{K}_2(C, \mathcal{O}_K)$ is a free abelian group of rank dg and the regulator pairing is non-degenerate.
2. Let R_C denote the absolute value of the determinant of this pairing with respect to $\mathbb{Z}$-bases of $H_1(X, \mathbb{Z})^-$ and $\mathrm{K}_2(C, \mathcal{O}_K)$, and let $\Lambda(C, 0)$ be the completed L-function of C; then
$$\Lambda(C, 0) = Q\,\mathrm{R}_C$$
for some non-zero rational number Q.

This conjecture was originally stated in a slightly different form (see [19]) in [6]. For an introduction see [41]. The conjectures were then tested by Bloch and Grayson [7] for K_2 of elliptic curves over $\mathbb{Q}$. They found an error in the original formulation of the conjecture which led Beilinson to modify his conjecture. In 1995 Young [54] wrote his thesis about similar calculations for elliptic curves over certain real quadratic number fields. Around the same time Ross [38] wrote his thesis about an element of K_2. This element was used by Kimura [26] to prove the conjecture for the genus two curve $y^2 - y = x^5$. Some theoretical work on the Beilinson conjectures for Fermat motives based on Ross' element was done by Otsubo [36].

Dokchitser, de Jeu and Zagier [19] extended the work of Bloch, Grayson and Young and did numerical calculations for K_2 of hyperelliptic curves over $\mathbb{Q}$.

Elliptic and hyperelliptic curves are among the most studied curves so far. As a generalization we consider curves of the form
$$C: \quad y^m = t(x),$$
where $t(x) \in K[x]$ is a monic polynomial with no double roots and of degree n. These curves are called superelliptic curves. Far less is known about superelliptic curves than about elliptic or hyperelliptic curves.

The goal of this thesis is to further extend the knowledge of the Beilinson conjectures for K_2 for superelliptic curves. We transfer the methods used in [19] to superelliptic curves and show that there exist elements of the given form. In contrast to hyperelliptic curves the methods used produce rarely enough elements in K_2 to even check the Beilinson conjectures. In this thesis we are only able to examine one example that satisfies all necessary requirements. Nevertheless, we also discuss examples where there exist enough elements but which satisfy additional relations or which have additional elements that do not satisfy the integrality condition.

In this thesis we study the following topics:

1. L-functions. We show in Chapter 3 how to effectively determine all invariants necessary to numerically calculate special values of L-functions of superelliptic curves. These results include many available methods to determine local L-factors

at bad primes (Theorem 3.7.2) and the conductor of the curve (Section 3.9). The local L-factors at bad primes are determined using an algorithm due to Stoll. We will provide the first published proof of this algorithm. Knowing these invariants is central for the application of the algorithms for the numerical calculation of special values of the L-function by Dokchitser [18]. This topic is elaborated very thoroughly in this thesis and the emphasis clearly lies on it.

2. Algebraic K-theory of superelliptic curves. We transfer the construction for elements of $\mathrm{K}_2(C, \mathcal{O}_K)$ of Dokchitser, de Jeu and Zagier in Chapter 5 to superelliptic curves and prove new relations for these elements for special classes of superelliptic curves (Proposition 5.2.6). This topic is elaborated to the necessary extent, but the emphasis does not lie on it. Complementary, during the writing of this thesis, Liu and Tang [29] independently extended the theoretical work of constructing elements of K_2 of Dokchitser, de Jeu and Zagier to superelliptic curves and worked out the proofs of some relations and integrality conditions. We will look at the differences between their work and our work in detail in Chapter 5.
3. Numerically testing Beilinson conjectures. We prove that for arbitrary superelliptic curves the constructions available to us can only produce potentially enough elements in $\mathrm{K}_2(C, \mathcal{O}_K)$ if the curve is of the form
$$C: \quad y^3 = t(x)$$
and $K = \mathbb{Q}$ or $K = \mathbb{Q}[\zeta_3]$, where ζ_3 is a third root of unity (Theorem 5.3.1). Within these restrictions we are able to find one class of superelliptic curves for which it is reasonable to numerically check the Beilinson conjectures (Theorem 5.5.1). For this class we can generate enough elements of $\mathrm{K}_2(C, \mathcal{O}_K)$, which potentially do not satisfy any non-trivial linear relation. We do not prove that they indeed do not satisfy any additional relation. We numerically calculate all necessary values for one example. Due to the nature of this class of examples it is difficult to obtain numerical values to high precision, so that the numerical results are unsatisfying. However, since the emphasis of this thesis is on the L-functions, no additional work has been undertaken to improve the numerical results.

The structure of the thesis is as follows.

In the first chapter we study the Dedekind zeta function and the algebraic K-theory of number fields. We then reformulate the original class number formula for number fields in terms of algebraic K-theory, as briefly described in the beginning of this introduction. As mentioned, it is exactly the generalization of this formula which we want to treat in this thesis

Chapter 2 gives a thorough introduction to the L-functions of strictly compatible systems of ℓ-adic representations. This chapter includes a brief introduction to ℓ-adic representations. At the end of the chapter we revisit the Dedekind zeta function from Chapter 1 as an explicit example of a general L-function.

In Chapter 3 we study the L-function of an algebraic curve. Special interest is given to the calculation of all invariants necessary to numerically calculate special values of

L-functions. At the end of the chapter we turn to a concrete example of a superelliptic curve, for which we calculate the special value of the L-function at 2.

In Chapter 4 we study the algebraic K-theory for superelliptic curves. This study is only brief and is aligned with the theory needed for this thesis.

Chapter 5 uses the theory developed in Chapter 4 to determine examples on which we can numerically test the Beilinson conjectures. It turns out that there are only few possibilities for superelliptic curves where the methods in this thesis produce enough elements in $\mathrm{K}_2(C, \mathcal{O}_K)$ to numerically test the Beilinson conjectures. In this chapter we also study the Riemann surface associated to an algebraic curve. We describe a concrete basis for the homology for which we can calculate the regulator pairing.

Chapter 6 covers the source code of all computer programs that were used in the computations done in this thesis.

I would like to thank the research group “Algebra und Zahlentheorie”, especially Anna Posingies and Christian Curilla, for a constructive research atmosphere. Furthermore, I would like to thank the Universität Hamburg, especially the Fachbereich Mathematik, for the aid and the optimal research environment. During my work on this thesis I encountered many mathematicians who helped me by offering suggestions, encouragement and inspiring discussions. To mention a few, I give thanks to Jan Steffen Müller for the hours of enlightening discussion and his detailed remarks on this thesis. I thank Tim Dokchitser and Michael Stoll for the insights they shared with me. I am grateful to my wife Constanze and my son Felix for their endless support. At last, I would like to thank in particular Ulf Kühn for the years of support and encouragement. Without him this thesis could not have been completed.

1 Number Fields

The Beilinson conjectures are a generalization of the class number formula for number fields. To lead the reader to the right insights about the setting for algebraic curves this chapter gives a thorough introduction to the class number formula, algebraic K-theory of number fields, and how the class number formula can be formulated in algebraic K-theory.

1.1 The Riemann Zeta Function

The first ingredient to the class number formula is the zeta function. The most basic example of a zeta function is the Riemann zeta function, which we introduce and study in this section.

Let $\zeta(s)$ be the series

$$\zeta(s) = \sum_{n=1}^{s} \frac{1}{n^s},$$

where s is a complex variable.

This series is called the Riemann zeta function and the first example of an L-function.

The Riemann zeta function is a very interesting function that has been deeply studied by mathematicians. Neukirch expresses the influence of the Riemann zeta function in number theory the following way [35, VII §1]:

> One of the most astounding phenomena in number theory consists in the fact that a great number of deep arithmetic properties of a number field are hidden within a single analytic function, its *zeta function*. This function has a simple shape, but it is unwilling to yield its mysteries. Each time, however, that we succeed in stealing one of these well-guarded truths, we may expect to be rewarded by the revelation of some surprising and significant relationship. This is why zeta functions, as well as their generalizations, the L-function, have increasingly moved to the foreground of the arithmetic scene, and today are more than ever the focus of number-theoretic research. The fundamental prototype of such a function is the Riemann zeta function.

Theorem 1.1.1. [35, VII theorem 1.1] The series $\zeta(s) = \sum_{n=1}^{s} \frac{1}{n^s}$ is absolutely and uniformly convergent in the domain $\mathrm{Re}(s) \geqslant 1 + \delta$, for every $\delta > 0$. It therefore represents an analytic function in the half-plane $\mathrm{Re}(s) > 1$.

One has **Euler's identity**

$$\zeta(s) = \prod_p \frac{1}{1-p^{-s}},$$

where p runs through the prime numbers. $\square$

The Euler identity expresses the Riemann zeta function as a product of factors, one for each prime number. Adding reasonable factors for the infinite prime, i.e. the natural embedding into $\mathbb{C}$, yields the completed Riemann zeta function.

It turns out that this reasonable factor is given in terms of the gamma function.

Let $\Gamma(s)$ be the *gamma function* defined for $\mathrm{Re}(s) > 0$ by the absolutely convergent integral

$$\Gamma(s) = \int_0^\infty e^{-y} y^s \frac{dy}{y}.$$

Using the gamma function we can define a reasonable factor for the infinite prime. This factor is given by

$$\mathrm{Z}_\infty(s) = \pi^{-s/2}\Gamma\left(\frac{s}{2}\right).$$

This PhD thesis will not go into detail about why this is a reasonable factor. See [35] for details.

Using this factor for the infinite prime we can define the completed Riemann zeta function.

Definition 1.1.2. The function

$$\mathrm{Z}(s) = \zeta(s)\,\mathrm{Z}_\infty(s)$$

is called the completed Riemann zeta function.

The completed Riemann zeta function satisfies a very simple functional equation.

Theorem 1.1.3. [35, VII, 1.6] The completed zeta function admits an analytic continuation to $\mathbb{C}\backslash\{0,1\}$, has simple poles at $s=0$ and $s=1$ with residues -1 and 1, respectively, and satisfies the functional equation

$$\mathrm{Z}(s) = \mathrm{Z}(1-s).$$

$\square$

This functional equation can also be expressed in terms of the Riemann zeta function, which follows from the properties of the gamma function.

Corollary 1.1.4. [35, VII Corollary 1.7] The Riemann zeta function $\zeta(s)$ admits an analytic continuation to $\mathbb{C}\backslash\{1\}$, has a simple pole at $s=1$ with residue 1 and satisfies the function equation

$$\zeta(1-s) = 2(2\pi)^{-s}\Gamma(s)\cos\left(\frac{\pi s}{2}\right)\zeta(s).$$

$\square$

1.2 The Dedekind Zeta Function and the Class Number Formula

The Riemann zeta function encodes a lot of information about the rational numbers $\mathbb{Q}$ and can be generalized for an arbitrary number field. This generalization is called the Dedekind zeta function and is introduced and studied in this chapter.

Let K be a number field, with r_1 real embeddings and $2r_2$ complex embeddings into $\mathbb{C}$, so that $d = [K : \mathbb{Q}] = r_1 + 2r_2$.

Definition 1.2.1. [35, VII 5.1] The Dedekind zeta function K is given by the series

$$\zeta_K(s) = \sum_{\alpha} \frac{a}{\mathfrak{N}(\alpha)^s},$$

where α varies over the integral ideals of K, and $\mathfrak{N}(\alpha)$ denotes their absolute norm.

Theorem 1.2.2. [35, VII 5.2] The series $\zeta_K(s)$ converges absolutely and uniformly in the domain $\mathrm{Re}(s) \geqslant 1 + \delta$ for every $\delta > 0$, and one has

$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1 - \mathfrak{N}(\mathfrak{p})^{-s}},$$

where $\mathfrak{p}$ runs through the prime ideals of K. □

The Dedekind zeta function can also be completed. While for the Riemann zeta function one infinite factor was sufficient, for K we have to distinguish between real and complex embeddings into $\mathbb{C}$.

Let

$$\begin{aligned} \mathrm{L}_{\mathbb{R}}(s) &= \pi^{-s/2}\Gamma(s/2), \\ \mathrm{L}_{\mathbb{C}}(s) &= 2(2\pi)^{-s}\Gamma(s), \text{ and} \end{aligned}$$

d_K be the discriminant of K.

Definition 1.2.3. We define the function Z_∞ [1] to be

$$\mathrm{Z}_\infty(s) = |\,\mathrm{d}_K\,|^{s/2}\, \mathrm{L}_{\mathbb{R}}^{r_1}(s)\, \mathrm{L}_{\mathbb{C}}^{r_2}(s).$$

Definition 1.2.4. The function

$$\mathrm{Z}_K(s) = \zeta_K(s)\, \mathrm{Z}_\infty(s)$$

is called the completed zeta function of the number field K.

[1] The function $\mathrm{Z}_\infty(s)$ can be viewed as the "Euler factor at infinity" of the zeta function $\zeta_K(s)$.

In analogy to Theorem 1.1.3 for the Riemann zeta function the completed Dedekind zeta function satisfies the following functional equation.

Theorem 1.2.5. [35, VII Corollary 5.10] The completed zeta function $\mathrm{Z}_K(s)$ admits an analytic continuation to $\mathbb{C}\backslash\{0,1\}$ and satisfies the functional equation

$$\mathrm{Z}_K(s) = \mathrm{Z}_K(1-s).$$

□

By Dirichlet's Unit Theorem [35, I §7] the group of units $\mathcal{O}_K^*$ of the ring of algebraic integers $\mathcal{O}_K$ in K is a finitely generated abelian group of rank $r = r_1 + r_2 - 1$. If $u_1, \cdots, u_r$ form a basis of $\mathcal{O}_K^*$/torsion, and $\sigma_1, \cdots, \sigma_{r+1}$ are the complex embeddings of K up to complex conjugation, then the *regulator* of $\mathcal{O}_K^*$ is defined by

$$\mathrm{R} = \frac{2^{r_2}}{[K:\mathbb{Q}]}\left|\det\begin{pmatrix} 1 & \log|\sigma_1(u_1)| & \cdots & \log|\sigma_1(u_r)| \\ \vdots & \vdots & & \vdots \\ 1 & \log|\sigma_{r+1}(u_1)| & \cdots & \log|\sigma_{r+1}(u_r)| \end{pmatrix}\right|.$$

In analogy with Corollary 1.1.4, there exists the following theorem which includes the famous class number formula.

Theorem 1.2.6. [35, VII Corollary 5.11]

1. The Dedekind zeta function $\zeta_K(s)$ has an analytic continuation to $\mathbb{C}\backslash\{1\}$.
2. At $s = 1$ it has a simple pole with residue

   $$\kappa = \frac{2^{r_1}(2\pi)^{r_2}}{w|\,\mathrm{d}_K\,|^{1/2}}|\,\mathrm{Cl}(K)|\,\mathrm{R}\,. \textbf{ (class number formula)}$$

   Here w denotes the number of roots of unity, d_K the discriminant of K and $\mathrm{Cl}(K)$ the class group of $\mathcal{O}_K$.
3. It satisfies the functional equation

   $$\zeta_K(1-s) = A(s)\zeta_K(s)$$

   with the factor

   $$A(s) = |\,\mathrm{d}_K\,|^{s-\frac{1}{2}}\left(\cos\frac{\pi s}{2}\right)^{r_1+r_2}\left(\sin\frac{\pi s}{2}\right)^{r_2}\mathrm{L}_{\mathbb{C}}(s)^n.$$

□

Remark 1.2.7. For $K = \mathbb{Q}$

$$\begin{aligned} r_1 &= 1, \\ r_2 &= 0, \\ w &= 2, \\ \mathrm{d}_{\mathbb{Q}} &= 1, \\ |\,\mathrm{Cl}(K)| &= 1, \\ \mathrm{R} &= 1, \end{aligned}$$

and thus

$$\kappa = 1.$$

Furthermore, the functional equation stated in part 3. is given in Corollary 1.1.4.

There are many ways to generalize the class number formula. The generalization to superelliptic curves is the theme of this thesis. We use algebraic K-theory [see Section 1.3] and L-functions [see Chapter 2] and study how the class number formula can be written in these notations.

1.3 Algebraic K-Theory of Number Fields

Algebraic K-theory consists of two major parts. The first part is the classical theory, worked out by Grothendieck, which centers around the Grothendieck group K_0 to prove his Grothendieck-Riemann-Roch theorem. The second part are the higher algebraic K-groups whose definition requires topological or homological machinery.

This thesis gives only a short introduction to the first part. Besides K_0 only K_1 and K_2 of number fields and algebraic curves are covered. For a thorough introduction of the classical theory and the Grothendieck-Riemann-Roch theorem see Neukirch [35, III]. For a thorough introduction to general K-theory see Weibel [52].

In this section we introduce classical algebraic K-theory for number fields.

The Grothendieck group $\mathrm{K}_0(\mathcal{O}_K)$

In this subsection we introduce and study the Grothendieck group of a number field.

We follow the short exposition by Heller and Reiner [23]. A more complete introduction can be found in Neukirch [35].

Let K be a number field and $F(\mathcal{O}_K)$ be the free abelian group of finitely generated O_K-modules isomorphism classes, i.e.

$$F(\mathcal{O}_K) = \bigoplus_{[M]} \mathbb{Z}[M],$$

where $[M]$ is an isomorphism class of a finitely generated $\mathcal{O}_K$-module M. Let $R(\mathcal{O}_K)$ be the group of elements

$$[M_1] - [M_2] + [M_3],$$

for which there exists a short exact sequence

$$0 \to M_1 \to M_2 \to M_3 \to 0.$$

Definition 1.3.1. [23] The quotient group

$$\mathrm{K}_0(\mathcal{O}_K) = F(\mathcal{O}_K)/R(\mathcal{O}_K)$$

is called the Grothendieck group of $\mathcal{O}_K$. If M is a finitely generated $\mathcal{O}_K$-module then $[M]$ denotes the class it defines in $\mathrm{K}_0(\mathcal{O}_K)$.

The Grothendieck group is the essential element of the Grothendieck-Riemann-Roch theorem [35, III Theorem 7.7].

The following theorem relates $\mathrm{K}_0(\mathcal{O}_K)$ to the ideal class group of K.

Theorem 1.3.2. [33, §1] Let K be a number field and $\mathcal{O}_K$ be the ring of integers, then

$$\mathrm{K}_0(\mathcal{O}_K) \cong \mathrm{Cl}(K) \oplus \mathbb{Z}.$$

□

The Whitehead Group K_1

In this subsection we introduce and study the Whitehead group of a number field. We follow the exposition of Weibel [52].

Let K be a number field, and $\mathcal{O}_K$ its ring of integers.

Identifying each $n \times n$ matrix g with the larger matrix

$$\begin{pmatrix} g & 0 \\ 0 & 1 \end{pmatrix}$$

gives an embedding of $\mathrm{GL}_n(\mathcal{O}_K)$ into $\mathrm{GL}_{n+1}(\mathcal{O}_K)$.

Definition 1.3.3. The union of the resulting sequence

$$\mathrm{GL}_1(\mathcal{O}_K) \subset \mathrm{GL}_2(\mathcal{O}_K) \subset \cdots \subset \mathrm{GL}_n(\mathcal{O}_K) \subset \mathrm{GL}_{n+1}(\mathcal{O}_K) \subset \cdots$$

is called the *infinite general linear group.*

The commutator subgroup $[G, G]$ of a group G is the subgroup generated by its commutators $[g, h] = ghg^{-1}h^{-1}$. It is always a normal subgroup of G and has a universal property: The quotient $G/[G, G]$ is an abelian group and every homomorphism from G to an abelian group factors through $G/[G, G]$.

Definition 1.3.4 ([52] II Definition 1.1)**.** The Whitehead group $\mathrm{K}_1(\mathcal{O}_K)$ of $\mathcal{O}_K$ is defined as

$$\mathrm{K}_1(\mathcal{O}_K) = \mathrm{GL}(\mathcal{O}_K)/[\mathrm{GL}(\mathcal{O}_K), \mathrm{GL}(\mathcal{O}_K)].$$

The universal property of $\mathrm{K}_1(\mathcal{O}_K)$ is:

Every homomorphism from $\mathrm{GL}(\mathcal{O}_K)$ to an abelian group must factor through the natural surjection $\mathrm{GL}(\mathcal{O}_K) \to \mathrm{K}_1(\mathcal{O}_K)$.

The following theorem is important for this thesis.

Theorem 1.3.5. [38, Theorem 2.3.2] The Whitehead group of $\mathcal{O}_K$ satisfies

$$\mathrm{K}_1(\mathcal{O}_K) \cong \mathcal{O}_K^*.$$

$\square$

1.4 The Class Number Formula Revisited

In this section we revisit the class number formula and reformulate the statement using the notion of algebraic K-theory that we introduced in the last section.

The results of the last section included that $\mathrm{K}_0(\mathcal{O}_K) \cong \mathrm{Cl}(K) \oplus \mathbb{Z}$ and $\mathrm{K}_1(\mathcal{O}_K) \cong \mathcal{O}_K^*$. Therefore it follows that

$$|\operatorname{Cl}(K)| = |\operatorname{K}_0(\mathcal{O}_K)_{tor}| \text{ and } w = |\operatorname{K}_1(\mathcal{O}_K)_{tor}|.$$

We can thus view the class number formula of Theorem 1.2.6 as a statement in algebraic K-theory.

Theorem 1.4.1. The class number formula in algebraic K-theory is

$$\operatorname*{Res}_{s=1} \zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}}{|\operatorname{K}_1(\mathcal{O}_K)_{tor}||\operatorname{d}_K|^{1/2}} |\operatorname{K}_0(\mathcal{O}_K)_{tor}| \operatorname{R}.$$

$\square$

It turns out that this formulation can be generalized to $\zeta_K(n)$ for $n \geqslant 2$ and even to special classes of curves.

The first step in generalizing the class number formula was done by Quillen [37]. He proved that $\mathrm{K}_n(\mathcal{O}_K)$ is a finitely generated abelian group for all n. This lead to the question of the rank of $\mathrm{K}_n(\mathcal{O}_K)$, which was calculated by Borel [9]. He proved that for even $n \geqslant 2$ the rank is zero and that for odd n a suitably defined regulator of $\mathrm{K}_{2m-1}(\mathcal{O}_K)$ is a non-zero rational multiple of $\zeta_K(m)/\pi^{mr_\pm}|\operatorname{d}_K|^{1/2}$, where $n = 2m - 1$.

This concluded the generalization for number fields and led Bloch to consider K_2 of elliptic curves. Bloch [8] proved for elliptic curves E defined over $\mathbb{Q}$ with complex multiplication that there is a relation between a regulator associated to $\mathrm{K}_2(E)$ and the value of $\mathrm{L}(E, 2)$.

This result seemed interesting to Beilinson, who anticipated a larger pattern for projective variety, leading him to conjecture similar relations between regulators of K-groups of projective varieties over number fields and values of their L-functions at integers (see [41, §5]).

Bloch and Grayson [7] tested these conjectures numerically for K_2 of elliptic curves over $\mathbb{Q}$. They could not verify the original conjecture using Beilinson's definition of the regulator, but they were able to modify the regulator to save the relation with the value of $L(E, 2)$. We explain the original conjecture and the modification in Section 4.4.

To be able to do that we need to generalize L-functions and K-theory first. We start by introducing general L-functions for rational ℓ-adic representations and using this theory for algebraic curves. Next is algebraic K-theory, which, due to complexity, we cover only in the small setting necessary for this thesis. Both components then allow us to state the Beilinson conjecture for superelliptic curves.

2 General $\mathbb{L}$-Functions

In the previous chapter we studied the Dedekind zeta function which was related via the class number formula to the regulator of the the number field. To be able to generalize this relation to algebraic curves, we first need to find suitable generalizations of the components, especially the L-function and the regulator. In this chapter we give a very broad introduction to the generalization of the Dedekind zeta function, the L-function of an ℓ-adic representation. At the end of this chapter we show that the L-functions defined in this chapter are indeed a generalization of the Dedekind zeta function. The theory of this chapter is used in the next chapter to define the L-function for an algebraic curve.

2.1 Galois Theory of Valuations

In this section we introduce the Galois theory of valued fields. For basic notions on valued fields see for instance [35]. For simpler reading, replace valued field by number field, which is the notion we use later on. The following is contained in [35] Chapter 2 §§8 - 10.

The theory explained in this section is used for studying ℓ-adic representations in the following sections.

Let K be a valued field. We fix an algebraic closure $\overline{K}$, a separable closure K_s, and denote the absolute Galois group of K by $\mathrm{G}_K = \mathrm{Gal}(K_s|K)$.

Denote the set of all valuations of K by $\Sigma_{\mathrm{K}}^{\infty}$. This set is a union

$$\Sigma_{\mathrm{K}}^{\infty} = \Sigma_{\mathrm{K}} \cup \Sigma_{\mathrm{K},\infty}$$

of Σ_{K}, the set of finite or non-archimedean valuations of K, and $\Sigma_{\mathrm{K},\infty}$, the set of archimedean valuations.

Let v be a non-archimedean valuation of K. The residue field κ_v is a finite field with $\mathrm{N}_v = \mathrm{p}_v^{\deg(v)}$ elements, where $\mathrm{p}_v = \mathrm{char}(\kappa_v)$ and $\deg(v)$ is the degree of κ_v over $\mathbb{F}_{\mathrm{p}_v}$.

For every valuation v of K we consider the completion K_v and an algebraic closure $\overline{K}_v$ of K_v. The canonical extension of v to K_v is again denoted by v and the unique extension of this latter valuation to $\overline{K}_v$ by $\overline{v}$.

Let $L|K$ be an algebraic extension. Choosing a K-embedding

$$\tau : L \to \overline{K}_v$$

we obtain by restriction of $\overline{v}$ to τL an *extension*

$$w = \overline{v} \circ \tau$$

of the valuation v to L. In other words, if v, resp. $\overline{v}$, are given by absolute values $|\cdot|_v$, resp. $|\cdot|_{\overline{v}}$, on K, $\overline{K}$, resp. $\overline{K}_v$, where $|\cdot|_{\overline{v}}$ extends precisely the absolute value $|\cdot|_v$ of K_v, then we obtain on L the multiplicative valuation

$$|x|_w = |\tau x|_{\overline{v}}.$$

The mapping $\tau : L \to \overline{K}_v$ is obviously continuous with respect to this valuation. It extends in a unique way to a continuous K-embedding

$$\tau : L_w \to \overline{K}_v,$$

where, in the case of an infinite extension $L|K$, L_w does not mean the completion of L with respect to w, but the union $L_w = \bigcup_i L_{iw}$ of the completions L_{iw} of all finite subextensions $L_i|K$ of $L|K$. This union is henceforth called the *localization* of L with respect to w.

If w extends v we call v the *restriction* of w to K, and we write $v = w|_K$.

Let $L|K$ be a Galois extension with Galois group $G = \mathrm{Gal}(L|K)$, and let $w \in \Sigma_{\mathrm{K}}^{\infty}$.

If w extends v to L, then, for every $\sigma \in G, w \circ \sigma$ also extends v, so that the group G acts on the set of extensions $w|v$.

Definition 2.1.1 ([35, definition II.9.2])**.** The *decomposition group* of an extension w of v to L is defined by

$$\mathrm{G}_w = \mathrm{G}_w(L|K) = \{\sigma \in \mathrm{Gal}(L|K) | w \circ \sigma = w\}.$$

If v is a non-archimedean valuation, then the decomposition group contains two further canonical subgroups

$$\mathrm{G}_w \supseteq \mathrm{I}_w \supseteq \mathrm{R}_w,$$

which are defined as follows. Let $\mathcal{O}_K$, resp. $\mathcal{O}_L$, be the valuation ring and $\mathfrak{p}$, resp $\mathfrak{P}$, the maximal ideal of v, resp w.

Definition 2.1.2 ([35, definition II.9.3])**.** The *inertia group* of $w|v$ is defined by

$$\mathrm{I}_w = \mathrm{I}_w(L|K) = \{\sigma \in \mathrm{G}_w \,|\sigma x \equiv x \mod \mathfrak{P} \text{ for all } x \in \mathcal{O}_L\}$$

and the *ramification group* by

$$\mathrm{R}_w = \mathrm{R}_w(L|K) = \left\{\sigma \in \mathrm{G}_w \,|\frac{\sigma x}{x} \equiv 1 \mod \mathfrak{P} \text{ for all } x \in L^*\right\}.$$

The groups $\mathrm{G}_w, \mathrm{I}_w$, and R_w carry significant information which influences the L-function that we define in Section 2.5. To understand this influence, we need the higher ramification groups which are covered in Section 2.2. The groups $\mathrm{G}_w, \mathrm{I}_w$, and R_w also have functorial properties (see [35, proposition II §9]).

The most important consequence of the functorial properties is the fact that we can determine the decomposition group, the inertia group and the ramification group locally.

Theorem 2.1.3 ([35, proposition II.9.6])**.**

$$\begin{aligned} \mathrm{G}_w(L|K) &\cong \mathrm{G}(L_w|K_v), \\ \mathrm{I}_w(L|K) &\cong \mathrm{I}(L_w|K_v), \\ \mathrm{R}_w(L|K) &\cong \mathrm{R}(L_w|K_v). \end{aligned}$$

□

Remark 2.1.4 ([35, section II.9])**.** The theorem above simplifies problems concerning a single valuation because we can handle the problem locally instead of globally. We identify the decomposition group $\mathrm{G}_w(L|K)$ with the Galois group of $L_w|K_v$ and write for simplification

$$\mathrm{G}_w(L|K) = \mathrm{G}(L_w|K_v),$$

and similar $\mathrm{I}_w(L|K) = \mathrm{I}(L_w|K_v)$ and $\mathrm{R}_w(L|K) = \mathrm{R}(L_w|K_v)$.

Definition 2.1.5 ([35, definitions II.9.7, II.9.10, and II.9.13])**.** The fixed fields of $\mathrm{G}_w, \mathrm{I}_w$, and R_w,

$$\begin{aligned} Z_w &= Z_w(L|K) = \{x \in L | \sigma x = x \text{ for all } \sigma \in \mathrm{G}_w\}, \\ T_w &= T_w(L|K) = \{x \in L | \sigma x = x \text{ for all } \sigma \in \mathrm{I}_w\}, \\ V_w &= V_w(L|K) = \{x \in L | \sigma x = x \text{ for all } \sigma \in \mathrm{R}_w\}, \end{aligned}$$

are called the decomposition field, the inertia field and the ramification field of w over K, respectively.

The importance of these fields comes from the next theorem.

Theorem 2.1.6 ([35, propositions II.9.8, II.9.11, and II.9.14])**.** The decomposition field, the inertia field, and the ramification field satisfy the following properties:

1. The decomposition field of $L|K$ consists of the intersection of L and K_v:

$$Z_w = L \cap K_v$$

2. The extension $T_w|Z_w$ is the maximal unramified subextension of $L|Z_w$.
3. The extension $V_w|Z_w$ is the maximal tamely ramified subextension of $L|Z_w$.

□

Definition 2.1.7. Let K be a local field and let w be the valuation of K_s. We denote

$$\begin{aligned} K^{nr} &= T_w(K_s, K) \text{ and} \\ K^{tame} &= V_w(K_s, K). \end{aligned}$$

They are called the maximal unramified and tamely ramified extensions of K.

The inertia group and the decomposition group are contained in a short exact sequence.

Theorem 2.1.8 ([35, proposition II.9.9])**.** The residue class field extension $\kappa_w | \kappa_v$ is normal and we have an exact sequence

$$1 \longrightarrow \mathrm{I}_w \longrightarrow \mathrm{G}_w \longrightarrow \mathrm{Gal}(\kappa_w | \kappa_v) \longrightarrow 1. \tag{2.1.1}$$

□

Theorem 2.1.9 ([35, proposition II.9.12])**.** The ramification group R_w is the unique p-Sylow subgroup of I_w. □

The Galois group $\mathrm{Gal}(\kappa_w \mid \kappa_v)$ is a (pro)finite cyclic group generated by the Frobenius element

$$\mathrm{Frob}_w : \kappa_w \to \kappa_w, x \mapsto x^{\mathrm{N}_v}.$$

We are interested in a lift of Frob_w to G_w, which we also call Frobenius element, and denote by Frob_w.

Definition 2.1.10. An arithmetic Frobenius Frob_w of G_w is any element that reduces to the Frobenius element Frob_w of $\mathrm{Gal}(\kappa_w \mid \kappa_v)$.

Remark 2.1.11. The Frobenius element Frob_w of G_w is only defined up to inertia.

Since the Frobenius element plays an important role in the following studies, we are interested in valuation in which it is uniquely defined.

Definition 2.1.12 ([42, 2.1])**.** The valuation w is called unramified if $\mathrm{I}_w = \{1\}$.

If $L|K$ is a finite extension, then all but a finite set of valuations of K are unramified.

Lemma 2.1.13. If the valuation w is unramified, then the Frobenius element Frob_w of G_w is uniquely determined up to automorphisms. □

Remark 2.1.14. Let $v \in \Sigma_{\mathrm{K}}$ and $w \in \Sigma_{\mathrm{K}s}$ any valuation that extends v. To simplify notations we often write

$$\mathrm{G}_v = \mathrm{G}_w,\ \mathrm{I}_v = \mathrm{I}_w,\ \text{and}\ \mathrm{R}_v = \mathrm{R}_w\,.$$

It is clear from the context, if a valuation lives in an extension $L|K$ or in the absolute extension $K_s|K$.

Example 2.1.15. Let $K = \mathbb{Q}$ and p any non-archimedean valuation, that is a prime of $\mathbb{Z}$. Then

$$Z_p = \mathbb{Q}_p, \quad T_p = \bigcup_{(n,p)=1} \mathbb{Q}_p(\zeta_n), \quad V_p = \bigcup_{(n,p)=1} \mathbb{Q}_p(\zeta_n, \sqrt[n]{p}).$$

Figure 2.1.1 on page 23 shows how the groups and fields are related in this example.

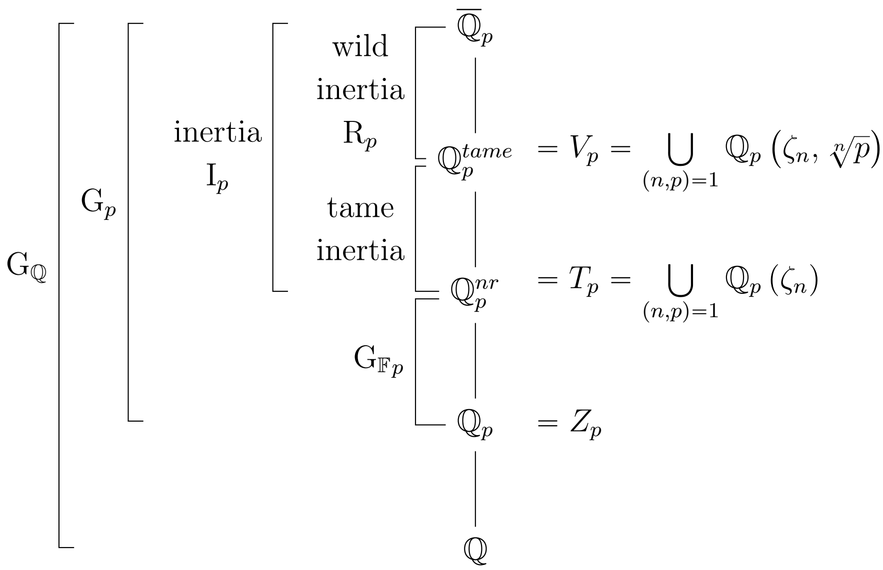
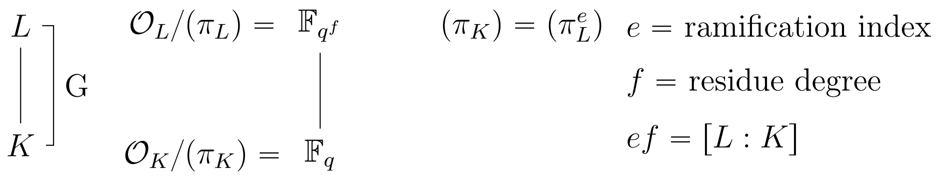


Figure 2.1.1: The decomposition, inertia and ramification group of $\mathbb{Q}_v$

2.2 Higher Ramification Groups

The inertia and the ramification groups are examples of higher ramification groups that we study in this section. These groups are important to define the conductor, which is needed for the functional equation of the L-function.

Let $L|K$ be a finite Galois extension. The inertia group and the ramification group inside the Galois group of valued fields are only the first terms in a whole series of subgroups that we are going to study. To keep the notation clean we use in this section the simplifications of Remark 2.1.4. That is, we assume that $L|K$ is an extension of local fields, let π_K and π_L be uniformizing elements in K and L, respectively. We recall that the ramification index e is such that $(\pi_K) = (\pi_L^e)$ in L and that the residue degree f is such that $\mathcal{O}_L/(\pi) \cong \mathbb{F}_{q^f}$, where $(\mathcal{O}_K/\pi_K) \cong \mathbb{F}_q$. Further we have $[L : K] = ef$.



Let v_K be a discrete normalized valuation of K, with positive residue field characteristic p_v, which admits a unique extension w to L. We denote by $v_L = ew$ the associated normalized valuation of L.

Definition 2.2.1 ([35, definition II.10.1])**.** For every real number $s \geqslant -1$ we define the s-th ramification group of $L|K$ by

$$\mathrm{G}_s = \mathrm{G}_s(L|K) = \{\sigma \in \mathrm{G} \,|\, v_L(\sigma a - a) \geqslant n + 1 \text{ for all } a \in \mathcal{O}_L\}\,.$$

Clearly, $\mathrm{G}_{-1} = \mathrm{G}, \mathrm{G}_0$ is the inertia group $\mathrm{I} = \mathrm{I}(L|K)$, and G_1 the ramification group $\mathrm{R} = \mathrm{R}(L|K)$ which were defined in Definition 2.1.2.

As

$$v_L\left(\tau^{-1}\sigma\tau a - a\right) = v_L\left(\tau^{-1}(\sigma\tau a - \tau a)\right) = v_L\left(\sigma(\tau a) - \tau a\right)$$

and $\tau\mathcal{O}_L = \mathcal{O}_L$, the ramification groups form a chain

$$\mathrm{G} = \mathrm{G}_{-1} \supseteq \mathrm{G}_0 \supseteq \mathrm{G}_1 \supseteq \mathrm{G}_2 \supseteq \ldots$$

of normal subgroups of G.

2.3 ℓ-adic Representations

In this section we introduce the notion of an ℓ-adic representation, which was first introduced by Taniyama [49] and which is the foundation for the definition of the general L-function. Since his paper is not written in the language that we are going to use later on, this chapter follows Serre [42] in his notations. Since Serre does not give the full definition of the L-Series in that book we turn to his paper [43] for the complete definition. For an introduction to representations in general see Serre [44] or Curtis and Reiner [16].

This section starts with an introduction of general ℓ-adic representations and studies the properties of them.

The reason to use ℓ-adic representation is that complex Galois representations always have a finite image (see Taylor [50]). This implies that the representation is a representation of a finite extension. These so called Artin representations were studied by Artin and others. Choosing an embedding of $\mathbb{Q} \subset \mathbb{Q}_\ell \subset \overline{\mathbb{Q}}_\ell \subset \mathbb{C}$ we can establish a bijection between Artin representations and ℓ-adic representations with a finite image. Thus, Artin representations are a special case of ℓ-adic Galois representations.

Since ℓ-adic representations may have an infinite image, they do not need to be semi-simple, i.e. they do not necessarily decompose into a direct sum of irreducible representations. This fact requires us to define the semi-simplification of a representation, such that we can use some facts about semi-simple representations in the next section.

At the end of this section we connect the notion of ℓ-adic representations with the notion of the inertia group. This allows us to associate polynomials to each prime which we will use in the definition of the L-function.

Let K be a number field and $\mathrm{G}_K = \mathrm{Gal}(\overline{\mathrm{K}}\,|K)$ the absolute Galois group of K. The group G_K with the Krull topology is compact and totally disconnected. Let ℓ be a prime number, and let V be a finite dimensional vector space over the field $\mathbb{Q}_\ell$ of ℓ-adic numbers. The full linear group $\mathrm{Aut}(V)$ is an ℓ-adic Lie group, its topology being induced by the natural topology of $\mathrm{End}(V)$; if $n = \dim(V)$, we have $\mathrm{Aut}(V) \cong \mathrm{GL}(n, \mathbb{Q}_\ell)$.

Definition 2.3.1 ([42, 1.1]). An *ℓ-adic representation* of G_K (or, by abuse of language, of K) is a continuous homomorphism $\rho : \mathrm{G}_K \to \mathrm{Aut}(V)$.

Before we move on with our definitions we take a look at some examples. We study in this section the same content as Serre, but examples 1 and 5 are worked out in deep detail in Sections 2.6 and 3.1.

Example 2.3.2 ([42, 1.2]).

1. **The trivial representation**

   Let $V = \mathbb{Q}_\ell$ and
   $$\mathbb{1} : \mathrm{G}_K \to \mathrm{Aut}\, v,\ \mathbb{1}(g) = \mathrm{id}\,.$$
   The representation $\mathbb{1}$ is called the trivial representation of G.

2. **The cyclotomic representation**[42, 1.1]

   Let $\ell \neq \mathrm{char}(K)$. The group G_K acts on the group μ_m of ℓ^m-th roots of unity, and hence also on $\mathrm{T}_\ell(\mu) = \varprojlim \mu_m$. The $\mathbb{Q}_\ell$ vector space $\mathrm{V}_\ell(\mu) = \mathrm{T}_\ell(\mu) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ is of dimension 1, and the homomorphism $\chi_\ell : \mathrm{G}_K \to \mathrm{Aut}(\mathrm{V}_\ell(\mu)) = \mathbb{Q}_\ell^*$ defined by the action of G_K on $\mathrm{V}_\ell(\mu)$ is a 1-dimensional ℓ-adic representation of G_K. The representation χ_ℓ is called the cyclotomic representation of G_K.

   This is also the first example of an ℓ-adic representation that is not an Artin representation, i.e. a representation with infinite image.

3. **The Tate module of an elliptic curve**

   Let $\ell \neq \mathrm{char}(K)$. Let E be an elliptic curve defined over K with a given rational point $\mathcal{O}$. We know that there is a unique structure of group variety on E with $\mathcal{O}$ as neutral element. Let E_m be the kernel of multiplication by ℓ^m in $E(\overline{\mathrm{K}})$, and let
   $$\mathrm{T}_\ell(E) = \varprojlim E_m,\ \mathrm{V}_\ell(E) = \mathrm{T}_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$
   The Tate module $\mathrm{T}_\ell(E)$ is a free $\mathbb{Z}_\ell$-module on which G_K acts (cf. [28, chapter VII]). The corresponding homomorphism $\phi_\ell : \mathrm{G}_K \to \mathrm{Aut}(\mathrm{V}_\ell(E))$ is an ℓ-adic representation of G_K. The group $\mathrm{G}_\ell = \mathrm{Im}(\pi_\ell)$ is a closed subgroup of $\mathrm{Aut}(T_\ell(E))$, a 4-dimensional Lie group isomorphic to $\mathrm{GL}(2, \mathbb{Z}_\ell)$.

4. **The Tate module of an abelian variety**

Let A be an abelian variety over K of dimension d. If $\ell \neq \mathrm{char}(K)$, we define $\mathrm{T}_\ell(A), \mathrm{V}_\ell(A)$ in the same way as in example 4. The group $\mathrm{T}_\ell(A)$ is a free $\mathbb{Z}_\ell$-module of rank $2d$ (cf. [28, chapter VII]) on which G_K acts.

5. **The Tate module of an algebraic curve**

   Let C be an algebraic curve over K. In Chapter 3 we define for each algebraic curve C a corresponding abelian variety $\mathrm{Jac}(C)$. Then $\mathrm{T}_\ell(C), \mathrm{V}_\ell(C)$ can be defined as $\mathrm{T}_\ell(\mathrm{Jac}(C)), \mathrm{V}_\ell(\mathrm{Jac}(C))$ in the same way as in example 5.

6. **Cohomology representation**

   Let X be an algebraic variety defined over the number field K, and let $X_s = X \times_K \overline{\mathrm{K}}$ be the corresponding variety over $\overline{\mathrm{K}}$. Let $\ell \neq \mathrm{char}(K)$, and let i be an integer. Using the etale cohomology of Artin-Grothendieck [2] we let

$$\begin{aligned} \mathrm{H}^i(X_s, \mathbb{Z}_\ell) &= \varprojlim \mathrm{H}^i\left((X_s)_{et}, \mathbb{Z}/\ell^n\mathbb{Z}\right), \\ \mathrm{H}^i_\ell(X_s) &= \mathrm{H}^i(X_s, \mathbb{Z}_\ell) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell. \end{aligned}$$

   The group $\mathrm{H}^i_\ell(X_s)$ is a vector space over $\mathbb{Q}_\ell$ on which G_K acts (via the action of G_K on X_s). It is finite dimensional, at least if $\mathrm{char}(K) = 0$ or if X is proper. We thus get a an ℓ-adic representation of G_K associated to $\mathrm{H}^i_\ell(X_s)$; by taking duals we also get homology ℓ-adic representations. Examples 3, 4, 5, and 6 are particular examples where $i = 1$ and X is respectively the multiplicative group $\mathbb{G}_m$, the elliptic curve E, and abelian variety A, or the Jacobian $\mathrm{Jac}(C)$.

We now look at the construction of new representations from known representations.

Let $\rho^V : \mathrm{G}_K \to \mathrm{Aut}(V)$ and $\rho^W : \mathrm{G}_K \to \mathrm{Aut}(W)$ be two ℓ-adic representations.

Definition 2.3.3 ([44, 1.3])**.** The direct sum $\rho^V \oplus \rho^W$ of ρ^V and ρ^W is the ℓ-adic representation

$$\begin{aligned} \rho^V \oplus \rho^W : \mathrm{G}_K &\to \mathrm{Aut}(V \oplus W) = \mathrm{Aut}(V) \oplus \mathrm{Aut}(W) \\ \sigma &\mapsto \left(\rho^V \oplus \rho^W\right)(\sigma) = \left(\rho^V(\sigma), \rho^W(\sigma)\right). \end{aligned}$$

Definition 2.3.4. The tensor product $\rho^V \otimes \rho^W$ of ρ^V and ρ^W is the ℓ-adic representation

$$\begin{aligned} \rho^V \otimes \rho^W : \mathrm{G}_K &\to \mathrm{Aut}(V \otimes W) = \mathrm{Aut}(V) \otimes \mathrm{Aut}(W) \\ \sigma &\mapsto \left(\rho^V \otimes \rho^W\right)(\sigma) = \rho^V(\sigma) \otimes \rho^W(\sigma). \end{aligned}$$

Let U be a vector subspace of V.

We are interested in subspaces which are compatible with the structure of the representation.

Definition 2.3.5 ([44, 1.3])**.** A subspace U is called stable under the action of G_K, if $x \in U$ implies $\rho^V(\sigma)x \in U$ for all $\sigma \in \mathrm{G}_K$.

Suppose the subspace U is stable under the action of G_K. It is clear that the restriction ρ^U of ρ^V to U is an ℓ-adic representation of G_K in U.

Definition 2.3.6 ([44, 1.3])**.** The representation

$$\begin{aligned} \rho^U : \mathrm{G}_K &\to \mathrm{Aut}(U) \\ \sigma &\mapsto \rho^V(\sigma) \end{aligned}$$

is said to be a subrepresentation of ρ^V.

Definition 2.3.7 ([44, 1.4])**.** Let $V \neq 0$. We call a representation $\rho^V : \mathrm{G}_K \to \mathrm{Aut}(V)$ *irreducible* or *simple*, if no subspace of V is stable under G_K, except 0 and V.

Next to subrepresentations we also need quotient representations. If we form the quotient space V/U we can define an ℓ-adic representation

$$\begin{aligned} \rho^{V/U} : \mathrm{G}_K &\to \mathrm{Aut}(V/U) \\ \sigma + U &\mapsto \rho^V(\sigma) + U. \end{aligned}$$

Definition 2.3.8 ([44, 1.3])**.** The representation

$$\begin{aligned} \rho^{V/U} : \mathrm{G}_K &\to \mathrm{Aut}(V/U) \\ \sigma + U &\mapsto \rho^V(\sigma) + U. \end{aligned}$$

is said to be the quotient representation of V under U.

Irreducible representations are a class of representations for which many results can be proven. It is thus understandable to use these representations as building blocks for another class of representations.

Definition 2.3.9. We call a representation $\rho^V : \mathrm{G}_K \to \mathrm{Aut}(V)$ *semi-simple* if it is the direct sum of simple representations.

Let G be a finite group, V be a vector space, and $\rho^V : G \to \mathrm{Aut}(V)$ be a representation. Since G is a finite group we know that ρ^V is a semi-simple representation [44, 1.4 Theorem 2]. This fact reduces the study of an arbitrary representation of a finite group to the study of irreducible representations of finite groups.

This fact is not true for G_K since G_K is infinite. But since semi-simple representations are so important we associate a semi-simple representation to each representation that admits a composition series.

Definition 2.3.10 ([42, 2.3])**.** If V has a composition series

$$V = V_0 \supset V_1 \supset \cdots \supset V_q = 0$$

of ρ^V-invariant subspaces with $V_i/V_{i+1} \quad (0 \leqslant i \leqslant q-1)$ simple, then the ℓ-adic representation ρ_{SS}^V of K, defined by

$$V_{SS} = \sum_{i=0}^{q-1} V_i/V_{i+1},$$

is called the semi-simplification of V.

Remark 2.3.11. To simplify notation we from now on denote the representation

$$\rho : \mathrm{G}_K \to \mathrm{Aut}(V)$$

simply by ρ or even V.

Remark 2.3.12.

1. The semi-simplification ρ_{SS} of an arbitrary representation ρ is, if it exists, semi-simple by construction.
2. The semi-simplification ρ_{SS} of a semi-simple representation ρ is isomorphic to the representation ρ.

Definition 2.3.13 ([1, section 2])**.** Let G be a group. A subgroup $H \leqslant G$ acts unipotently if any element of H is unipotent, i.e. if the characteristic polynomial of $\rho(h) = (T-1)^{\dim(V)}$ for all $h \in H$.

Definition 2.3.14 ([21, definition 1.22])**.** Let ρ be an ℓ-adic representation of K with $\rho : \mathrm{G}_K \to \mathrm{Aut}(V)$ and $v \in \Sigma_{\mathrm{K}}$.

1. We say that ρ is unramified or has good reduction at v if I_v acts trivially.
2. We say that ρ has potentially good reduction at v if $\rho(\mathrm{I}_v)$ is finite, in other words, if there exists a finite extension K' of K contained in $\overline{\mathrm{K}}$ such that ρ, as an ℓ-adic representation of $\mathrm{Gal}(\overline{\mathrm{K}}\,|K')$, has good reduction.
3. We say that V is semi-stable at v if I_v acts unipotently, in other words, if the semi-simplification of V has good reduction.
4. We say that V is potentially semi-stable at v, if there exists a finite extension K' of K contained in $\overline{\mathrm{K}}$ such that ρ is semi-stable as a representation of $\mathrm{Gal}(\overline{\mathrm{K}}\,|K')$.
5. We say that ρ is tamely ramified at v if R_v acts trivially.

Remark 2.3.15. By definitio,n an unramified representation is also a semi-stable representation.

Lemma 2.3.16. Let ρ be a semi-stable ℓ-adic representation. Then ρ is tamely ramified.

Proof. Let $g \in \mathrm{R}_v$. Since ρ is semi-stable $\rho(g)$ is unipotent. Since R_v is the p-Sylow subgroup of I_v the order of $\rho(g)$ is a power of p and is especially finite. Therefore, $\rho(g) = 1$ and R_v acts trivially. □

Lemma 2.3.17 ([42, 2.1])**.** Let $H = \ker(\rho)$ be kernel of ρ and L be the fixed field of H. Then ρ is unramified at v, if and only if, v is unramified in $L|K$. □

Definition 2.3.18 ([42, 2.1])**.** If the representation ρ is unramified at v, then the restriction of ρ to G_w factors through $\mathrm{G}_w / \mathrm{I}_w$ for any $w|v$. Hence, $\rho(\mathrm{Frob}_w) \in \mathrm{Aut}(V)$ is defined. We call $\rho(\mathrm{Frob}_w)$ the Frobenius of w in the representation ρ, and we denote it by $\mathrm{Frob}_{w,\rho}$. The conjugacy class of $\mathrm{Frob}_{w,\rho}$ in $\mathrm{Aut}(V)$ only depends on v; it is denoted by $\mathrm{Frob}_{v,\rho}$.

Definition 2.3.19 ([42, 2.1])**.** If v is unramified with respect to ρ, we let $P_{v,\rho}(T)$ denote the characteristic polynomial $P_{v,\rho}(T) = \det\left(1 - \mathrm{Frob}_{v,\rho}^{-1} T\right)$.

Remark 2.3.20. We define the polynomial P in terms of Frob^{-1} instead of Frob as in Serre [42, 2.1]. This is in accordance with Serre's article [43, 2.2]. The element Frob^{-1} is also called the geometric Frobenius, in contrast to the arithmetic Frobenius Frob defined above.

If v is ramified with respect to ρ then the Frobenius element can not be uniquely defined, since the inertia group does not act trivially on V. To include the ramified places, we define the Frobenius on the fixed space V^{I_w}. This is possible due to the fact that I_w acts trivially on V^{I_w}.

Definition 2.3.21. Let w be any valuation extending v. Let ρ^{I_w} be the subrepresentation of ρ acting on V^{I_w}, i.e. the space on which I_w acts trivially,

$$\rho^{\mathrm{I}_w} : \mathrm{G}_K \to \mathrm{Aut}\left(V^{\mathrm{I}_w}\right).$$

The representation ρ^{I_w} is by definition unramified at v.

Definition 2.3.22 ([43, 2.2])**.** Let $v \in \Sigma_{\mathrm{K}}$ be a non-archimedean value. We extend the definition of $P_{v,\rho}(T)$ to ramified v by

$$P_{v,\rho}(T) = \det\left(1 - \mathrm{Frob}_{v,\rho}^{-1} T | V^{\mathrm{I}_w}\right) = \det\left(1 - \mathrm{Frob}_{v,\rho^{\mathrm{I}_w}}^{-1} T\right).$$

Obviously, the two definitions are the same for unramified values v.

2.4 Rational ℓ-adic Representations

In this section we study rational ℓ-adic representations. These are ℓ-adic representations which associated polynomials, of Definition 2.3.22, have rational coefficients. Rational ℓ-adic representations always admit a semi-simplification, which is also rational. At the end of this chapter we define the notion of compatible systems of ℓ-adic representations, which we use in the next chapter to define the general L-function.

Definition 2.4.1 ([42, 2.3])**.** The ℓ-adic representation ρ is said to be rational (resp. integral) if for all $v \nmid \ell$ the coefficients of $P_{v,\rho}(T)$ belong to $\mathbb{Q}$ (resp. to $\mathbb{Z}$).

Example 2.4.2. The ℓ-adic representations of K, given in Example 2.3.2, are rational (even integral) for 1, 2, 3, 4, and 5. The rationality of the cohomology representation in 7 is a well-known open question.

Lemma 2.4.3 ([42, 2.3])**.** Any rational representation ρ admits a semi-simplification ρ_{SS}, which is also rational. □

Definition 2.4.4 ([42, 2.3])**.** Let ℓ, ℓ' be primes, ρ (resp. ρ') an ℓ-adic (resp. ℓ') representation of K, and assume that ρ, ρ' are rational. Then ρ, ρ' are said to be compatible if

$$P_{v,\rho}(T) = P_{v,\rho'}(T) \text{ for } v \nmid \ell\ell'.$$

Lemma 2.4.5 ([42, 2.3])**.** The semi-simplification $(\rho)_{SS}$ of a rational representation ρ is compatible with ρ. □

Theorem 2.4.6 ([42, 2.3])**.** Let ρ be a rational ℓ-adic representation of K, and let ℓ' be a prime. Then there exists at most one (up to isomorphism) ℓ'-adic representation ρ' of K which is semi-simple and compatible with ρ. □

Definition 2.4.7 ([42, 2.3])**.** For each prime ℓ let $\rho_\ell : \mathrm{G}_K \to \mathrm{Aut}(V)$ be a rational ℓ-adic representation of K. The system $(\rho_\ell)_\ell$ is said to be strictly compatible if ρ_ℓ and $\rho_{\ell'}$ are compatible for any two primes ℓ and ℓ'. That is, $(\rho_\ell)_\ell$ is strictly compatible if

1. $P_{v,\rho_\ell}(T)$ has rational coefficients and
2. $P_{v,\rho_\ell}(T) = P_{v,\rho_{\ell'}}(T)$ if $v \nmid \ell\ell'$.

Example 2.4.8. The systems of ℓ-adic representations given in Example 2.3.2 are strictly compatible for examples 1, 2, 3, 4, and 5.

2.5 The General L-Function

In this section we define the general L-function for strictly compatible systems of ℓ-adic representations. For the conjectured functional equation we need to define the conductor using the higher ramification groups. This section takes a very general approach on the L-function. In the next section we revisit the Dedekind zeta function and see how it connects to the theory explained in this section.

Let K be a number field. Let $\rho = (\rho_\ell)$, $\rho_\ell : \mathrm{G}_K \to \mathrm{Aut}(V)$ be a strictly compatible system of rational ℓ-adic representations.

Definition 2.5.1 ([42, 2.5])**.** For all $v \in \Sigma_{\mathrm{K}}$, we denote the rational polynomial $P_{v,\rho_\ell}(T)$, for any $\ell \neq \mathrm{p}_v$ by $\mathrm{L}_v(\rho_\ell, T)$. By assumption, this polynomial does not depend on the choice of ℓ. Let s be a complex number. We define

$$\mathrm{L}(\rho_\ell, s) = \prod_{v \in \Sigma_{\mathrm{K}}} \left(\mathrm{L}_v(\rho_\ell, N_v^{-s})\right)^{-1}. \tag{2.5.1}$$

The L-function of (2.5.1) is conjectured to satisfy a functional equation if one also includes the archimedean values. These local factors at infinite places are essentially a product of Γ-functions that depend on the Hodge realization of the vector spaces V.

Following Serre we define

Definition 2.5.2 ([43]). Let $\Gamma_{\mathbb{R}}$ and $\Gamma_{\mathbb{C}}$ be given by

$$\Gamma_{\mathbb{R}}(s) = \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right) \text{ and} \tag{2.5.2}$$

$$\Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s}\Gamma(s). \tag{2.5.3}$$

The two Γ-factors satisfy the relation

$$\Gamma_{\mathbb{C}}(s) = \Gamma_{\mathbb{R}}(s)\Gamma_{\mathbb{R}}(s+1).$$

Let $v : K \to \mathbb{C} \in \Sigma_{\mathrm{K},\infty}$ be an archimedean valuation. We denote by $V_{\mathbb{C}} = V \otimes \mathbb{C}$ the complex vector space associated to ρ_ℓ.

The factors we have to add to the L-function depend on whether K_v is isomorphic to $\mathbb{R}$ or to $\mathbb{C}$.

$K_v = \mathbb{C}$. If K_v is isomorphic to $\mathbb{C}$, then a complex Hodge decomposition of $V_{\mathbb{C}}$ is a direct sum $V_{\mathbb{C}} = \bigoplus V_{\mathbb{C}}^{p,q}$, indexed over $\mathbb{Z} \times \mathbb{Z}$. We set

$$h(p,q) = \dim(V^{p,q}).$$

The Γ-factor attached to v is defined by the product

$$\mathrm{L}_v(\rho_\ell, s) = \prod_{p,q} \Gamma_{\mathbb{C}}\left(s - \inf(p,q)\right)^{h(p,q)}.$$

$K_v = \mathbb{R}$. A real Hodge $\mathbb{R}$-decomposition of $V_{\mathbb{C}}$ is a pair consisting of a Hodge $\mathbb{C}$-decomposition $(V_{\mathbb{C}}^{p,q})$ and an automorphism σ of $V_{\mathbb{C}}$ such that $\sigma^2 = 1$ and $\sigma(V_{\mathbb{C}}^{p,q}) = V_{\mathbb{C}}^{p,q}$ for all (p,q).

If V admits such a structure we denote again

$$h(p,q) = \dim(V_{\mathbb{C}}^{p,q}).$$

If n is an integer the automorphism σ leaves $V_{\mathbb{C}}^{n,n}$ fixed and, therefore, we can decompose $V_{\mathbb{C}}^{n,n}$ into a direct sum of two subspaces

$$V_{\mathbb{C}}^{n,n} = V_{\mathbb{C}}^{n,+} \oplus V_{\mathbb{C}}^{n,-},$$

with

$$\begin{aligned} V_{\mathbb{C}}^{n,+} &= \{x | x \in V_{\mathbb{C}}^{n,n},\ \sigma(x) = (-1)^n x\}\,, \\ V_{\mathbb{C}}^{n,-} &= \left\{x | x \in V_{\mathbb{C}}^{n,n},\ \sigma(x) = (-1)^{n+1} x\right\}. \end{aligned}$$

We define

$$\begin{aligned} h(n,+) &= \dim(V_{\mathbb{C}}^{n,+}) \text{ and} \\ h(n,-) &= \dim(V_{\mathbb{C}}^{n,-}). \end{aligned}$$

Therefore,

$$h(n,n) = h(n,+) + h(n,-).$$

The Γ-factor attached to v is defined by the product

$$\mathrm{L}_v(\rho_\ell, s) = \prod_n \Gamma_{\mathbb{R}}(s-n)^{h(n,+)} \Gamma_{\mathbb{R}}(s-n+1)^{h(n,-)} \prod_{p<q} \Gamma_{\mathbb{C}}(s-p)^{h(p,q)}.$$

We now set the L-function for the infinite primes to be

$$\mathrm{L}_\infty(\rho_\ell, s) = \prod_{v|\infty} \mathrm{L}_v(\rho_\ell, s).$$

Remark 2.5.3. If (ρ_ℓ) is a compatible system of ℓ-adic representations then the L-function for the infinite primes $\mathrm{L}_\infty(\rho_\ell, s)$ does not depend on the prime ℓ.

The conductor

To state the functional equation of the L-function we need to define the conductor.

Let $v \in \Sigma_{\mathrm{K}}$ be a non-archimedean valuation that is a prime ideal of K. As defined in Definition 2.3.14 (ρ_ℓ) is unramified if $\rho_\ell(\mathrm{I}_v) = 1$. The conductor is a finer invariant of ramified representations.

Definition 2.5.4. The conductor exponent is an integer $\mathfrak{f}_{\rho,\,v}$ defined by

$$\mathfrak{f}_{\rho,\,v} = \mathfrak{f}_{\rho,\,v}^T + \mathfrak{f}_{\rho,\,v}^W,$$

where $\mathfrak{f}_{\rho,\,v}^T$ and $\mathfrak{f}_{\rho,\,v}^W$ are the tame and the wild part and are defined by

$$\mathfrak{f}_{\rho,\,v}^T = \operatorname{codim} V^{I_v} = \dim V - \dim V^{I_v} \tag{2.5.4}$$

$$\mathfrak{f}_{\rho,\,v}^W = \sum_{i=1}^{\infty} \frac{|\,\mathrm{G}_i\,|}{|\,\mathrm{G}_0\,|} \operatorname{codim}(V)_{\mathrm{ss}}^{\mathrm{G}_i}, \tag{2.5.5}$$

where the G_i are the higher ramification groups of v, $\mathrm{G}_0 = \mathrm{I}_v, \mathrm{G}_1 = \mathrm{R}_v$ (see Definition 2.2.1). Note that $\operatorname{codim}(V)_{\mathrm{ss}}^{G_i} = 0$ for large i, since $G_i = \{0\}$ for large i.

The following lemma follows directly from the definitions and Lemma 2.3.16.

Lemma 2.5.5.

1. Let ρ be an unramified representation at v, then
$$\mathfrak{f}_{\rho,v} = 0 \quad .$$
2. Let ρ be an tamely ramified representation at v, then
$$\mathfrak{f}^W_{\rho,v} = 0 \quad .$$
3. Let ρ be a semi-stable representation at v, then
$$\mathfrak{f}^W_{\rho,v} = 0 \quad .$$

□

The Artin conductor is the corresponding ideal in K.

Definition 2.5.6. The Artin conductor is defined by
$$\mathcal{N} = \prod_{v \nmid \infty} \pi_v^{\mathfrak{f}_{\rho,\,v}},$$
where π_v is any element with $v(\pi_v) = 1$.

The functional equation

Let D be
$$\mathrm{D} = \begin{cases} |\,\mathrm{d}_{K|\mathbb{Q}}\,| & \text{if } K \text{ is a number field,} \\ q^{2g-2} & \text{if } K \text{ is a function field,} \end{cases}$$
where $\mathrm{d}_{K|\mathbb{Q}}$ is the discriminant of the number field K or K is the function field of degree g over the finite field of q elements. Let
$$\mathrm{N} = \prod_{v \in \Sigma_K} \mathrm{Nm}(\mathcal{N}) = \prod_{v \in \Sigma_K} \mathrm{N}_v^{\mathfrak{f}(\rho_\ell, v)}$$
be the norm of the Artin conductor.

Using the information above, we now can define the complete L-function
$$\Lambda(\rho_\ell, s) = \mathrm{N}^{\frac{s}{2}}\, \mathrm{D}^{\frac{s \dim(V)}{2}}\, \mathrm{L}(\rho_\ell, s)\, \mathrm{L}_\infty(\rho_\ell, s).$$

Conjecture 2.5.7. The functions $\mathrm{L}(\rho_\ell, s)$ and $\Lambda(\rho_\ell, s)$ admit a meromorphic continuation to $\mathbb{C}$. Furthermore, there exists a weight $\mathrm{w} \geqslant 0$ and a sign $\epsilon = \pm 1$, such that the function $\Lambda(\rho_\ell, s)$ satisfies the functional equation

$$\Lambda(\rho_\ell, s) = \epsilon\, \Lambda(\rho_\ell, \mathrm{w} + 1 - s).$$

Example 2.5.8. The system of ℓ-adic representations given in Example 2.3.2 satisfies the functional equation for 1 and 3. For the rest of the examples this is still a conjecture.

Remark 2.5.9. Let X be a smooth projective variety defined over $\mathbb{Q}$ and ρ_ℓ be the system of cohomology representations of Example 2.3.2 with integer i. All the conjectures concerning L-functions are often combined as the standard conjectures of arithmetic geometry. They can be stated as follows(see [24, 3.1]):

1. $\mathrm{L}(\rho_\ell, T) \in \mathbb{Z}[x]$ is independent of the prime ℓ.
2. The Euler product $\mathrm{L}(\rho_\ell, s) = \prod_p \mathrm{L}_p(\rho_\ell, p^{-s})^{-1}$ converges absolutely for $\mathrm{Re}(s) > \frac{i}{2} + 1$, and does not vanish in this region.
3. $\mathrm{L}(\rho_\ell)$ admits a meromorphic continuation to the whole complex plane with at most a pole at $s = \frac{i}{2} + 1$ when i is even. In particular, $\mathrm{L}(\rho_\ell, s)$ extends to an entire function when i is odd.
4. $\mathrm{L}(\rho_\ell, \frac{i}{2} + 1) \neq 0$.
5. The functional equation $\Lambda(\rho_\ell, s) = \pm\, \Lambda(\rho_\ell, i + 1 - s)$ holds.

The Artin formalism

The Artin formalism explains how relations between representations are inherited by the corresponding L-function. We only cover the Artin formalism for tensor products and short exact sequences of representations. The Artin formalism is used in Section 3.7 to prove the algorithm which determines the L-factor at primes of bad reduction.

Theorem 2.5.10 ([32, 6.2.2])**.** If $\rho : \mathrm{G}_K \to \mathrm{GL}(V)$ and ρ' are two representations of G_K, then

1. $$\mathrm{L}(\rho \oplus \rho', s) = \mathrm{L}(\rho, s)\, \mathrm{L}(\rho', s).$$
2. Let
$$0 \to U \to V \to W \to 0$$
be an exact sequence of subspaces of V. Let ρ_U, ρ_W be the corresponding subrepresentations of ρ. Then
$$\mathrm{L}(\rho, s) = \mathrm{L}(\rho_U, s)\, \mathrm{L}(\rho_W, s).$$

2.6 The Dedekind Zeta Function Revisited

In the last section we took a very general approach to define the L-function. In this section we revisit the Dedekind zeta function to better understand the abstract notion on a basic example that was already explained in fundamental terms in Section 1.2.

Let K be a number field. Using the methods of Chapter 2, we look at a special L-function of K. The Dedekind ζ-function of K is the L-function associated to the system of trivial representations $\mathbb{1} = \mathbb{1}_\ell : \mathrm{G}_K \to \mathbb{Q}_\ell$ with $\mathbb{1}(g) = 1$ for all $g \in G$ and all $\ell \in \Sigma_\mathrm{K}$.

By definition, $\mathbb{1}$ is a strictly compatible system, satisfying

$$\mathrm{L}_v(\mathbb{1}, T) = P_{v,\mathbb{1}}(T) = 1 - T,$$

and $\mathbb{1}$ is unramified at all $v \in \Sigma_\mathrm{K}$.

Therefore,

$$\zeta_K(s) = \mathrm{L}(\mathbb{1}, s) = \prod_{v \in \Sigma_\mathrm{K}} (1 - \mathrm{N}_v^{-s})^{-1}.$$

Theorem 2.6.1 ([35, proposition VII.5.2])**.** The Dedekind zeta function of the number field K can be given by the series

$$\zeta_K(s) = \sum_{\mathfrak{a}} \mathrm{Nm}(\mathfrak{a})^{-s}$$

where a varies over the integral ideals $\mathfrak{a}$ of K, and $\mathrm{Nm}(\mathfrak{a})$ denotes their absolute norm. The series $\zeta_K(s)$ converges absolutely and uniformly in the domain $\mathrm{Re}(s) > 1 + \delta$ for every $\delta > 0$. □

Let r_1 and r_2 be the number of real and pairs of conjugate complex embeddings of K, such that $r_1 + 2r_2 = [K : \mathbb{Q}]$.

Let $v \in \Sigma_{\mathrm{K},\infty}$ be an embedding of K in $\mathbb{C}$. The Hodge decomposition of $V_\mathbb{C} = \mathbb{Q}_\ell \otimes \mathbb{C} = \mathbb{C}$ is $V_\mathbb{C} = \bigoplus V_\mathbb{C}^{p,q}$, where

$$V_\mathbb{C}^{p,q} = \begin{cases} \mathbb{C} & \text{for } p = q = 0 \text{ and} \\ 0 & \text{otherwise.} \end{cases}$$

Furthermore,

$$h(n, +) = h(p, q) = \begin{cases} 1 & \text{for } p = q = n = 0 \text{ and} \\ 0 & \text{otherwise.} \end{cases}$$

The L-factor at infinity is therefore given by

$$\mathrm{L}_\infty(\mathbb{1}, s) = \Gamma_\mathbb{R}(s)^{r_1} \Gamma_\mathbb{C}(s)^{r_2}$$

The Artin conductor is trivial because $\mathbb{1}$ is unramified at all $v \in \Sigma_\mathrm{K}$.

The completed L-function is given by

$$\begin{aligned} \mathrm{Z}_K &= |\,\mathrm{d}_{K|\mathbb{Q}}\,|^{\frac{s}{2}}\Gamma_{\mathbb{R}}(s)^{r_1}\Gamma_{\mathbb{C}}(s)^{r_2}\zeta_K(s) \\ &= |\,\mathrm{d}_{K|\mathbb{Q}}\,|^{\frac{s}{2}}\Gamma_{\mathbb{R}}(s)^{r_1+r_2}\Gamma_{\mathbb{R}}(s+1)^{r_2}\zeta_K(s) \\ &= \left(\frac{|\,\mathrm{d}_{K|\mathbb{Q}}\,|}{\pi^n}\right)^{\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)^{r_1+r_2}\Gamma\left(\frac{s+1}{2}\right)^{r_2}\zeta_K(s). \end{aligned}$$

With this definition we can state the following theorems.

Theorem 2.6.2 ([35, corollary VII 5.11])**.**

1. The Dedekind zeta function $\zeta_K(s)$ has an analytic continuation to $\mathbb{C}\backslash\{1\}$.
2. At $s = 1$ it has a simple pole with residue

$$\operatorname*{Res}_{s=1}\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}}{w\sqrt{|d_K|}}hR. \tag{2.6.1}$$

□

The equation (2.6.1) is commonly known as the analytic class number formula.

Furthermore, we can specify the constants of Conjecture 2.5.7. The weight is $\mathrm{w} = 0$ and the sign is $\epsilon = +1$.

Theorem 2.6.3 ([35, corollary VII.5.10])**.** The completed zeta function satisfies the functional equation

$$\mathrm{Z}_K(1-s) = \mathrm{Z}_K(s).$$

□

The Artin formalism tells us how the ζ-function of K is composed of the L-function of all irreducible representations of the group $\mathrm{Gal}(K|\mathbb{Q})$.

Remark 2.6.4. Let $\rho : \mathrm{G}_K \to \mathrm{Aut}(V)$ be an Artin representation. The system of representation

$$\mathbb{1} \otimes \rho = \rho$$

for all $\ell \in \Sigma_{\mathrm{K}}$ is strictly compatible.

Theorem 2.6.5 ([32, 6.2.3])**.** The Dedekind zeta function of K admits the factorization

$$\begin{aligned} \zeta_K(s) &= \zeta(s)\prod_{\rho\neq\mathbb{1}}\mathrm{L}(\mathbb{1}\otimes\rho, s)^{\deg(\rho)} \\ &= \zeta(s)\prod_{\rho\neq\mathbb{1}}\mathrm{L}(\rho, s)^{\deg(\rho)} \end{aligned}$$

where the product is over all non-trivial irreducible representation ρ of $\mathrm{Gal}(K|\mathbb{Q})$. □

3 L-Functions of Algebraic Curves

So far, this thesis only considered number fields and representations, while algebraic curves only appeared in Example 2.3.2. This chapter works out the algebraic curve case in full detail. The next chapter explains K-theory for algebraic curves and combines both components to state the Beinlinson conjectures.

3.1 The Tate Module

To define the L-function of an algebraic curve using the methods of Chapter 2 we need a compatible system of representations. It turns out that such a compatible system of representations is given by the Tate module. Since the Tate module is only defined for abelian varieties, we first need to associate an abelian variety to the algebraic curve. The next theorem states that we can associate such an abelian variety to any smooth, geometrically connected, projective curve.

Theorem 3.1.1 ([30, theorem 7.4.39]). Let C be a smooth, geometrically connected, projective curve of genus g over a field K. Then, there exists an abelian variety J of dimension g over K such that $J(L) = \mathrm{Pic}^0(C_L)$ for any extension $L|K$ verifying $C(L) \neq \varnothing$. Moreover, the isomorphism is compatible with field extensions. □

Definition 3.1.2 ([30, definition 7.4.40]). The abelian variety J above is called the Jacobian of C and is denoted by $\mathrm{Jac}(C)$.

To every abelian variety we can construct the Tate module, which was already defined in Example 2.3.2. We restate the definition to keep this section self-contained.

Definition 3.1.3 ([32, section 5.4.1]). Let A be an abelian variety of dimension g defined over K. Then, the Tate module is defined by

$$\begin{aligned}
\mathrm{T}_\ell(A) &= \varprojlim_n A[\ell^n] \cong \mathbb{Z}_\ell^{2g} \\
\mathrm{V}_\ell(A) &= \mathrm{T}_\ell(A) \otimes \mathbb{Q}_\ell \cong {\mathbb{Q}_\ell}^{2g} .
\end{aligned}$$

The modules $\mathrm{T}_\ell\, A$, $\mathrm{V}_\ell\, A$ and $\mathrm{Aut}(\mathrm{V}_\ell\, A)$ are known as the ℓ-adic representations of A. Since G_K acts on these modules, we have the representations

$$\begin{aligned}
&\psi_\ell : \mathrm{G}_K \to \mathrm{Aut}(T_\ell A) \text{ and} \\
&\phi_\ell : \mathrm{G}_K \to \mathrm{Aut}(\mathrm{V}_\ell\, A) \cong \mathrm{GL}_{2g}(\mathbb{Q}_\ell).
\end{aligned}$$

The Jacobian allows us to define the Tate module for an algebraic curve.

Definition 3.1.4. Let C be a smooth, geometrically connected, projective curve of genus g over a field K. The Tate module of C is defined to be

$$\mathrm{T}_\ell(C) = \mathrm{T}_\ell(\mathrm{Jac}(C)) \cong \mathbb{Z}_\ell^{2g}$$
$$\mathrm{V}_\ell(C) = \mathrm{V}_\ell(\mathrm{Jac}(C)) \cong \mathbb{Q}_\ell{}^{2g}\,.$$

3.2 The L-Function

Let C be a smooth, geometrically connected, projective curve of genus g over a field K. To define the L-function of an algebraic curve we can use the Tate module defined in the last section.

Definition 3.2.1. Let ρ_ℓ be the system of representations defined by

$$\rho_\ell : \mathrm{G}_K \to \mathrm{Aut}\left(\mathrm{V}_\ell(C)^*\right),$$

i.e. ρ_ℓ acts on the dual of the Tate module $\mathrm{V}_\ell(C)^*$ of C, which is the dual of the Tate module of the Jacobian $\mathrm{Jac}(C)$.

Lemma 3.2.2 ([53])**.** The system of representations of Definition 3.2.1 is compatible. □

Definition 3.2.3. We define the L-function of C to be the L-function of the system ρ_ℓ:

$$\mathrm{L}(C, K, s) = \mathrm{L}(\rho_\ell, s).$$

All that is known about these L-functions is that they define a holomorphic function on the right half plane.

Theorem 3.2.4 ([19])**.** The L-function $\mathrm{L}(C, K, s)$ of an algebraic curve over K converges absolutely to a holomorphic function for $\mathrm{Re}(s) > \frac{3}{2}$. □

Let r_1 and r_2 be the number of real and complex embeddings of K, such that $r_1 + 2r_2 = d = [K : \mathbb{Q}]$.

Let $v \in \Sigma_{\mathrm{K},\infty}$ be an embedding of K into $\mathbb{C}$. The Hodge decomposition of $V_\mathbb{C} = \mathrm{V}_\ell(C)^* \otimes \mathbb{C}$ is $V_\mathbb{C} = \bigoplus V_\mathbb{C}^{p,q}$, where

$$V_\mathbb{C}^{p,q} = \begin{cases} \mathbb{C}^g & \text{for } (p,q) = (1,0), (0,1) \text{ and} \\ 0 & \text{otherwise.} \end{cases}$$

Therefore,

$$h(p,q) = \begin{cases} g & \text{for } (p,q) = (1,0), (0,1) \text{ and} \\ 0 & \text{otherwise.} \end{cases}$$

The L-factor at infinity is therefore given by

$$\mathrm{L}_\infty(C,K,s) = \Gamma_{\mathbb{C}}(s)^{dg}.$$

The representation ρ_ℓ is ramified at v if, and only if, C has bad reduction at v. The Artin conductor is therefore a product of the primes of bad reduction of C to some power. In Sections 3.8 and 3.9 we determine the conductor in more detail.

As in Section 2.5 we define

$$\Lambda(C,K,s) = \mathrm{N}^{\frac{s}{2}}\,\mathrm{D}^{\frac{s\dim(V)}{2}}\,\mathrm{L}(C,K,s)\,\mathrm{L}_\infty(C,K,s).$$

All the other conjectures about general L-function (e.g. the functional equation) have also not bee proven in this case. It is assumed, that for curves the weight is $\mathrm{w} = 1$ and the sign ϵ can be ± 1 and depends on the curve C.

Conjecture 3.2.5 (Hasse-Weil)**.**

1. $\mathrm{L}(C,K,s)$ extends to an entire function.
2. The functional equation

$$\Lambda(C,K,s) = \pm\,\Lambda(C,K,2-s) \tag{3.2.1}$$

   holds.

3.3 Computing Special Values of the L-function

To check Beilinson's conjecture we need to calculate $\Lambda(C,K,0)$. If Conjecture 3.2.5 holds, then $\mathrm{L}^{(0)}(C,0) = \cdots = \mathrm{L}^{(g-1)}(C,0) = 0$ and

$$\frac{\mathrm{L}^{(g)}(C,K,0)}{g!} = \lim_{s\to 0}\frac{\mathrm{L}(C,K,s)}{s^g} = \Lambda(C,K,0) = \epsilon\,\Lambda(C,K,2) = \frac{\epsilon\,N}{(2\pi)^{2g}}\,\Lambda(C,K,2) \neq 0\ ,$$

because $\Gamma(s)$ has a pole of order one at $s = 0$ with residue 1.

Remark 3.3.1 (cf. [19] Remark 2.2)**.** If the Hasse-Weil conjectures (Conjecture 3.2.5) hold, we need to calculate the value of $\mathrm{L}(C,K,s)$ only at $s = 2$, where the defining Euler product is absolutely convergent. This convergence is not practical to calculate the value of $\mathrm{L}(C,K,2)$, since it is very slow. Instead, we use the algorithms described in [18] for numerical calculations. These algorithms have been implemented in the PARI package ComputeL by Tim Dokchitser.

Let K be a number field of degree $n = [K:\mathbb{Q}]$ and C/K be an algebraic curve of genus g.

To calculate special values of the L-function ComputeL has to know

1. the dimension d,
2. the Hodge numbers $\lambda_1, \ldots, \lambda_d$,
3. the weight w,
4. a finite number of the local L-polynomials L_p, for p up to an integer M, that depends on the required precision,
5. the conductor N, and
6. the sign ϵ.

We already know (see Section 3.2) that in the case of algebraic curves

1. the dimension is $d = 2gn$,
2. the Hodge numbers are

$$\lambda_i = \begin{cases} 0 & \text{for } 1 \leqslant i \leqslant gn \text{ and} \\ 1 & \text{for } gn < i \leqslant 2gn, \end{cases}$$

   and
3. the weight is $w = 2$.

Therefore, to calculate special values of the L-function only the rest of the invariants have to be calculated. These are

4. a finite number of the local L-polynomials L_p, for p up to an N,
5. the conductor N and
6. the sign ϵ.

The calculation of the local L-polynomials can be split up into two parts. On the one hand, into the primes of good reduction that can be handled by counting points in finite fields, which is done in Section 3.6. On the other hand, into the primes of bad reduction whose local L-polynomials can be deduced from the regular model. To do that we need a certain amount of formal background, which is explained in Section 3.4, where we study the structure of the Tate module, and Section 3.5, which contains information on the calculation of regular models. In Section 3.7 we describe an algorithm that deduces the local factors.

The calculation of the conductor N can also be split up into two parts: The tame part and the wild part. The tame part N^T can be deduced from the regular model. This is the content of Section 3.8. In Section 3.9 we gather information on how to determine the wild part N^W of the conductor. The wild part can be deduced with the knowledge of a semi-stable model of the number field over which the curve is defined. Since most of the time it is algorithmically cumbersome to find a semi-stable model it is often not possible to directly determine the wild part of the conductor. Due to work of Lockhart, Rosen and Silverman [31], and Brumer and Kramer [12], it is possible to determine an upper bound for the conductor. With this knowledge it is possible to let the computer check a finite amount of possibilities, if they satisfy a functional equation.

A method to calculate the sign without testing the functional equation is still unknown. Until now, there exist only conjectures about the origin of the sign. But since it can only be ± 1 the computer can check which sign satisfies the functional equation.

3.4 The Structure of the Tate Module

Let K be a number field with algebraic closure $\overline{\mathrm{K}}$ and A be a connected algebraic group.

In this section we study the structure of the Tate module. The facts explained give a good understanding how the structure of the Tate module depends on the different primes of $\mathcal{O}_K$. The theory developed is also used in Section 3.7 to prove an algorithm to determine the local factors at primes of bad reduction.

Let ψ_ℓ and ϕ_ℓ be the corresponding ℓ-adic representations given by

$$\begin{aligned} \psi_\ell &: \mathrm{G}_K \to \mathrm{Aut}(T_\ell A) \text{ and} \\ \phi_\ell &: \mathrm{G}_K \to \mathrm{Aut}(\mathrm{V}_\ell\, A) \cong \mathrm{GL}_{2g}(\mathbb{Q}_\ell). \end{aligned}$$

We are interested in the structure of these representations. The following theorem tells us about the components of connected algebraic groups.

Theorem 3.4.1. Every connected algebraic group is an extension of an abelian variety $\mathfrak{A}$ by a linear group H and $H = \mathfrak{T} \times \mathfrak{U}$, where $\mathfrak{T}$ is a torus and $\mathfrak{U}$ is unipotent. That is, there exist exact sequences

$$\begin{aligned} &1 \to H \to A \to \mathfrak{A} \to 1 \quad \text{and} \\ &1 \to \mathfrak{T} \to H \to \mathfrak{U} \to 1. \end{aligned} \tag{3.4.1}$$

Proof. The theorem follows from a theorem due to Chevalley [39, Theorem 16] and Waterhouse [51, Theorem 9.5]. □

The results for connected algebraic groups carry over to the Tate module.

Lemma 3.4.2 ([25, lemma 2.33])**.** Let M, N and P be connected algebraic groups such that the sequence

$$1 \to M \to N \to P \to 1$$

is exact. If the multiplication by ℓ is a bijection on M, then there exists an exact sequence of G_K-modules

$$1 \to \mathrm{T}_\ell\, M \to \mathrm{T}_\ell\, N \to \mathrm{T}_\ell\, P \to 1.$$

Moreover, if M is a unipotent group, then $\mathrm{T}_\ell\, N = \mathrm{T}_\ell\, P$. □

The study of the Tate module of a connected algebraic group therefore reduces to the study of the Tate module of abelian varieties and toric groups.

Remark 3.4.3. Let A be a connected algebraic group of dimension d.

1. If A is an abelian variety then
$$\dim(\mathrm{V}_\ell(A)) = 2d.$$
2. If A is a toric group then
$$\dim(\mathrm{V}_\ell(A)) = d.$$
3. If A is a unipotent group then
$$\dim(\mathrm{V}_\ell(A)) = 0.$$

Let now K be a number field and A an abelian variety over K.

For a prime v of $\mathcal{O}_K$, the reduction $\widetilde{A}_v$ of $A \mod v$ does not need to be an abelian variety over κ_v, the residue field of $K \mod v$.

Definition 3.4.4. We say that the abelian variety A has good reduction at v if $\widetilde{A}_v$ is an abelian variety over the residue field κ_v. Otherwise, we say that A has bad reduction at v.

In the case of bad reduction Néron proved that there exists a smooth scheme for abelian varieties that satisfies an important mapping property.

Definition 3.4.5 ([10, definition 1.2.1])**.** Let A be an abelian variety. A Néron model of A is a model $\mathcal{A}$ which is smooth, separated, and of finite type. Furthermore, it needs to satisfy the following universal property, called Néron mapping property:

For each abelian variety B over K and each K-morphism $u_K : B \to A$ there is a unique $\mathrm{Spec}(\mathcal{O}_K)$-morphism $u : \mathcal{B} \to \mathcal{A}$ extending u_K.

Let v be a prime of $\mathcal{O}_K$. The connected component $\mathcal{A}_v^0$ of the special fiber $\mathcal{A}_v$ of the Néron model of A is a connected algebraic group and therefore we have:

Corollary 3.4.6. Let A be an abelian variety. The connected component $\tilde{\mathcal{A}}_v^0$ of the special fiber of the Néron model is an extension of an abelian variety $\mathfrak{A}$ by a linear group H and $H = \mathfrak{T} \times \mathfrak{U}$, where $\mathfrak{T}$ is a torus and $\mathfrak{U}$ is unipotent. That is, there exist exact sequences

$$\begin{aligned} &1 \to H \to \tilde{\mathcal{A}}_v^0 \to \mathfrak{A} \to 1 \quad \text{and} \\ &1 \to \mathfrak{T} \to H \to \mathfrak{U} \to 1. \end{aligned} \tag{3.4.2}$$

□

Definition 3.4.7. We call $\mathfrak{A}$ the abelian part, $\mathfrak{T}$ the toric part and $\mathfrak{U}$ the unipotent part of $\tilde{\mathcal{A}}_v^0$. Furthermore, we define $a_v = \dim \mathfrak{A}$, $t_v = \dim \mathfrak{T}$ and $u_v = \dim \mathfrak{U}$. For an algebraic curve C we define $\mathfrak{A}, \mathfrak{T}, \mathfrak{U}, a_v, t_v$ and u_v as the invariants of the Jacobian $\mathrm{Jac}(C)$ of C for every prime v.

The importance of these invariants comes from the following lemma.

Lemma 3.4.8 ([25, lemma 2.50])**.** Let ℓ be a prime such that $\ell \neq \mathrm{p}_v$ and $\ell \nmid \#(\tilde{\mathcal{A}}/\tilde{\mathcal{A}}^0)$. Then, there exists an isomorphism of $\mathrm{Gal}(\overline{K}_v|K_v)$-modules

$$\mathrm{T}_\ell(\mathcal{A}_v^0) = \mathrm{T}_\ell(\mathcal{A}_v) = (\mathrm{T}_\ell(A))^{\mathrm{I}_v}.$$

□

Lemma 3.4.9. The dimension of the connected component is equal to the dimension of the abelian variety A, i.e.

$$\dim(\mathcal{A}_v^0) = \dim(A).$$

□

Corollary 3.4.10. Let A be an abelian variety of dimension g and $v \in \Sigma_\mathrm{K}$. Then

$$g = a_v + t_v + u_v.$$

□

Definition 3.4.11. We say that the abelian variety A has semi-stable reduction at v if $u_v = 0$.

Corollary 3.4.12. Let C be a smooth, projective, geometrically irreducible algebraic curve of genus g and $v \in \Sigma_\mathrm{K}$. Then

$$g = a_v + t_v + u_v.$$

□

Grothendieck connected the notion of semi-stable reduction at v with the notion of a semi-stable representation (see Definition 2.3.14).

Theorem 3.4.13 ([22, proposition 3.5],[46, theorem 4.1], Galois Criterion for Semi-stable Reduction)**.** The following statements are equivalent:

1. The abelian variety A is semi-stable at v.
2. The Tate module $\mathrm{V}_\ell(A)$ is semi-stable at v.

□

3.5 Models of Algebraic Curves

Let K be a number field, $\mathcal{O}_K$ be the ring of integers of K, $S = \operatorname{Spec} \mathcal{O}_K$, and η be the generic point of S. Let C be a smooth projective geometrically irreducible algebraic curve and $\mathfrak{p}$ be a prime of $\mathcal{O}_K$.

To determine the local L-polynomials and the conductor (of the Jacobian $\mathrm{Jac}(C)$) it is not sufficient to know the reduction of a curve modulo $\mathfrak{p}$. These invariants require information that depends on the equation over K. We can use the information over K to construct a model of the curve. A model of C is a scheme over S whose generic fiber is isomorphic to C. It turns out that there exists a special kind of model, called regular models, which contain more information than the reduction modulo $\mathfrak{p}$. This model contains enough information to calculate the local L-polynomial and the tame part of the conductor, but it is still not enough information to calculate the wild part of the conductor. How these invariants can be deduced from the regular model is covered in Sections 3.7 and 3.8. We look at methods to calculate the wild part of the conductor in Section 3.9.

Models of algebraic curves is a topic that has been treated by many authors. This thesis follows the book "Algebraic Geometry and Arithmetic Curves" by Qing Liu [30].

Let us start by defining what we understand by a model of C.

Definition 3.5.1 ([30, remark 10.1.6])**.** A model for C over S is a S-scheme $\mathcal{C}$, surjective and flat over S, endowed with an isomorphism $\mathcal{C}_\eta = \mathcal{C}_K = \mathcal{C} \times_S \operatorname{Spec} K \cong_K C$, where $\mathcal{C}_\eta$ is the generic fiber of $\mathcal{C}$.

In the following we look at certain types of models with additional structure. We start by defining the additional structure independently of models.

Definition 3.5.2 ([30] section 8.3.1 definition 3.1)**.** We call an integral, projective, flat S-scheme $\pi : X \to S$ of dimension 2 a fibered surface over S. A fiber X_s with $s \in S$ closed is called a closed fiber. X is also called a projective flat S-curve. Note that the flatness of π is equivalent to the surjectivity of π. We say that X is a normal (resp. regular) fibered surface if X is normal (resp. regular).

A morphism (resp. a rational map) between fibered surfaces is a morphism (resp. a rational map) that is compatible with the structure of S-schemes.

The simplest example of a fibered surface is the Zariski closure.

Example 3.5.3. Let C/K be given by the equation

$$C: \quad F(X_1, \ldots, X_n) = 0$$

such that all coefficients of $F(X_1, \ldots, X_n)$ are contained in $\mathcal{O}_K$.

The Zariski closure of C over S is the fibered surface

$$\mathfrak{C} = \operatorname{Proj} \mathcal{O}_K[X_1, \cdots X_n]/(F(X_1, \ldots X_n)).$$

The Zariski closure of C is a model of C over S, which depends on the choice of F.

Regular fibered surfaces possess multiple important properties.

Definition 3.5.4 ([30] section 8.3.1 Definition 3.14)**.** We call a regular fibered surface $X \to S$ an arithmetic surface.

The Zariski closure of an algebraic curve is of dimension 2, but in general it is not regular or even normal.

Since the regularity is imporant for a lot of applications, it is natural to try to find a regular model of C.

Definition 3.5.5 ([30] section 9.3.2 Definition 3.14)**.** A regular model of C over S is an arithmetic surface which is as a model of C over S

Now that we have defined regular models we need to check if they exist.

Definition 3.5.6 ([30] section 8.3.4 Definition 3.39)**.** Let X be a reduced locally Noetherian scheme. A proper birational morphism $\pi : Z \to X$ with Z regular is called a desingularization of X (or a resolution of singularities of X). If π is an isomorphism above every regular point of X, we say that it is a desingularization in the strong sense.

Theorem 3.5.7 ([30] section 8.3.4 Corollary 3.45)**.** Every fibered surface $X \to S$ admits a desingularization in the strong sense. □

Remark 3.5.8. The desingularization $\mathcal{C}$ of a Zariski closure of C is a regular model of C over S.

In Definition 2.3.14 we stated the notion of semi-stability for representations. Through the Tate module we now have a connection between algebraic curves and representations and it is interesting to study how the notion of semi-stability transfers to the language of curves. Using the language of models we are able to study the connection between the two notions. But first we need to define a notion of semi-stability for curves, which requires a few technical definitions.

Definition 3.5.9 ([30, Definition 10.3.1])**.** Let C be an algebraic curve over an algebraically closed field k. We say that C is semi-stable if it is reduced, and if its singular points are ordinary double points.

Definition 3.5.10 ([30, Definition 10.3.2])**.** We say that a curve C over a field k is semi-stable if its extension $C_{\overline{k}}$ to an algebraic closure $\overline{k}$ of k is a semi-stable curve over $\overline{\mathrm{K}}$.

Definition 3.5.11 ([30, Definition 10.3.14])**.** Let $f : Y \to S$ be a model of C over S. For $s \in S$ we say that f (or Y) is semi-stable at s, if the special fiber Y_s is a semi-stable curve. We call f (or Y) semi-stable, it is semi-stable at all $s \in S$.

Definition 3.5.12 ([30, Definition 10.3.27])**.** We say that C has semi-stable reduction at $s \in S$ if there exists a model $\mathcal{C}$ of C over S that is semi-stable at s.

We say that C has semi-stable reduction over S if C is semi-stable at all $s \in S$.

Deligne and Mumford [17] carried Grothendieck's result (Theorem 3.4.13) over to curves and proved the connection between the two notions of semi-stability.

Theorem 3.5.13 ([17, theorem 2.4])**.** The following are equivalent:

1. the algebraic curve C has semi-stable reduction at v;
2. the Tate module $\mathrm{V}_\ell(C)$ is semi-stable at v.

□

3.6 Local L-factors at Primes of Good Reduction

Let C/K be a smooth projective algebraic curve of genus g, and $v \in \Sigma_{\mathrm{K}}$ a prime of $\mathcal{O}_K$ of good reduction and $q = \mathrm{N}_v$. This section illustrates how the local L-polynomial can be calculated by counting points over $\mathbb{F}_q, \ldots, \mathbb{F}_{q^g}$.

The main ingredient is that the fiber $\mathfrak{C}_v$, i.e. the reduction of C modulo v, is a smooth projective curve over $\mathbb{F}_q$ and the local L-polynomial can be connected with the zeta function of $C/\mathbb{F}_q$.

For any algebraic variety defined over $\mathbb{F}_q$, let N_k denote the number of $\mathbb{F}_{q^k}$-rational points on X.

Let the local L-factor at v be

$$\mathrm{L}_v(C, K, T) = a_{2g}T^{2g} + a_{2g-1}T^{2g-1} + \cdots + a_2T^2 + a_1T^1 + a_0.$$

In this section we prove the theorem:

Theorem 3.6.1. The local L-factor at a prime of good reduction v can be calculated from $\mathrm{N}_1, \cdots, \mathrm{N}_g$.

In detail:

1. For $k = 0$ the coefficient is given by
$$a_0 = 1.$$
2. For $1 \leqslant k \leqslant g$ we can determine the coefficient a_k recursively by
$$a_k = -\frac{1}{k}\sum_{i=1}^{k} a_{k-i}b_i,$$
where
$$b_k = \sum_{i=0}^{2g} \alpha_i^k = q^k + 1 - \mathrm{N}_k\,.$$

3. For $g < k \leqslant 2g$ the coefficient is given by

$$a_{2g-k} = q^{g-k} a_k. \tag{3.6.1}$$

Remark 3.6.2. In the examples of this thesis,we calculate the L-factors only for curves up to genus 4. In this case, the a_i are given by

$$\begin{aligned} a_0 &= 1 \\ a_1 &= -b_1 \\ a_2 &= -\frac{b_1^2 + b_2}{2} \\ a_3 &= -\frac{b_1^3 + 3b_1b_2 + 2b_3}{6} \\ a_4 &= -\frac{b_1^4 + 6b_1b_2 + 3b_1^2 + 8b_3b_1 + 6b_4}{24} \end{aligned}$$

where $b_k = q^k + 1 - \mathrm{N}_k$. This defines all the coefficients by (3.6.1).

To prove the theorem, we define the Zeta-function of a variety.

Definition 3.6.3 ([14, definition 8.2])**.** The zeta function $\mathrm{Z}(C/\mathbb{F}_q, T)$ of C over $\mathbb{F}_q$ is the generating function

$$\mathrm{Z}(C/\mathbb{F}_q, T) = \exp\left(\sum_{k=1}^{\infty} \frac{\mathrm{N}_k}{k} T^k\right).$$

Weil [53] proved the following theorem on the Zeta-function.

Theorem 3.6.4 ([14, theorem 8.3], Hasse-Weil Conjectures)**.** Let C be a smooth projective curve of genus g defined over a finite field with q elements.

1. Rationality: $\mathrm{Z}(C/\mathbb{F}_q; T) \in \mathbb{Q}[[T]]$ is a rational function.
2. Functional equation: $\mathrm{Z}(T) = \mathrm{Z}(C/\mathbb{F}_q; T)$ satisfies

$$\mathrm{Z}\left(\frac{1}{qT}\right) = \pm q^g T^{2g}\, \mathrm{Z}(T).$$

3. Riemann hypothesis: there exists a polynomial $P_1(T) \in \mathbb{Z}[T]$, such that

$$\mathrm{Z}(C/\mathbb{F}_q; T) = \frac{P_1(T)}{P_0(T) \cdot P_2(T)}$$

with $P_0(T) = 1 - T, P_2(T) = 1 - q^n T$ and

$$P_1(T) = \prod_{i=1}^{2g} (1 - \alpha_i T)$$

where the α_i are algebraic integers of absolute value $q^{1/2}$.

□

The L-function and the Zeta-function of a variety are deeply connected.

Theorem 3.6.5 ([14, Proposition 8.4])**.** The zeta function of C is given by

$$\mathrm{Z}(C/\mathbb{F}_q;T) = \frac{\mathrm{L}_v(C,K,T)}{(1-T)(1-pT)}. \tag{3.6.2}$$

□

Now we can use Theorem 3.6.4 to prove Theorem 3.6.1.

Proof of Theorem 3.6.1. The proof of Part 1. follows from the Riemann hypothesis, because

$$\mathrm{L}_v(C,K,T) = \prod_{i=1}^{2g}(1-\alpha_i T).$$

Now, we prove Part 2. Taking the logarithms of (3.6.2) we get

$$\ln(\mathrm{Z}(C)/\mathbb{F}_q,T) = \sum_{k=1}^{\infty}\frac{\mathrm{N}_k}{k}T^k = \sum_{i=1}^{2g}\ln(1-\alpha_i T) - \ln(1-T) - \ln(1-qT).$$

Since $\ln(1-sT) = -\sum_{i=1}^{\infty}\frac{(sT)^k}{k}$, we get

$$\sum_{k=1}^{\infty}\frac{\mathrm{N}_k}{k}T^k = -\sum_{i=1}^{2g}\sum_{k=1}^{\infty}\frac{(\alpha_i T)^k}{k} + \sum_{k=1}^{\infty}\frac{(T)^k}{k} + \sum_{k=1}^{\infty}\frac{(qT)^k}{k}.$$

Therefore, by comparing the coefficients of T^k we get

$$\mathrm{N}_k = q^k + 1 - \sum_{i=1}^{2g}\alpha_i^k.$$

On the other hand, we can write

$$\begin{aligned}\mathrm{L}_v(C,K,T) &= a_{2g}T^{2g} + a_{2g-1}T^{2g-1} + \cdots + a_2T^2 + a_1T^1 + a_0\\ &= \prod_{i=1}^{2g}(1-\alpha_i T)\,.\end{aligned}$$

Thus, for $0 \leqslant i \leqslant 2g$

$$a_i = \prod_{1\leqslant j_1<\cdots<j_i\leqslant 2g}\alpha_{j_1}\cdot\cdots\cdot\alpha_{j_i}.$$

Therefore, the proof of Part 2. reduces to the expression of the a_i's in terms of sums $\sum_{i=1}^{2g}\alpha_i^k$ for $1 \leqslant k \leqslant g$.

Let $b_k = \sum_{i=0}^{2g} \alpha_i^k = q^k + 1 - \mathrm{N}_k$, then

$$\begin{aligned} a_{k-1} \cdot b_1 &= k \cdot \prod_{1 \leqslant j_1 < \cdots < j_k \leqslant 2g} \alpha_{j_1} \cdot \cdots \cdot \alpha_{j_k} + \prod_{\substack{l \neq j_* \\ 1 \leqslant j_1 < \cdots < j_{k-2} \leqslant 2g}} \alpha_l^2 \cdot \alpha_{j_1} \cdot \cdots \cdot \alpha_{j_{k-2}} \\ &= k \cdot a_k + \prod_{\substack{l \neq j_* \\ 1 \leqslant j_1 < \cdots < j_{k-2} \leqslant 2g}} \alpha_l^2 \cdot \alpha_{j_1} \cdot \cdots \cdot \alpha_{j_{k-2}}. \end{aligned}$$

and for $1 < i < k$

$$a_{k-i} \cdot b_i = \prod_{\substack{l \neq j_* \\ 1 \leqslant j_1 < \cdots < j_{k-i} \leqslant 2g}} \alpha_l^i \cdot \alpha_{j_1} \cdot \cdots \cdot \alpha_{j_{k-i}} + \prod_{\substack{l \neq j_* \\ 1 \leqslant j_1 < \cdots < j_{k-i-1} \leqslant 2g}} \alpha_l^{i+1} \cdot \alpha_{j_1} \cdot \cdots \cdot \alpha_{j_{k-i-1}}$$

where the product always runs over all $1 \leqslant l \leqslant 2g$ and $1 \leqslant j_1 < \cdots < j_n \leqslant 2g$ ($n = k-2, k-i$ or $k-i-1$) and $l \neq j_m$ for all $1 \leqslant m \leqslant n$.

Therefore,

$$a_k = \frac{1}{k} \sum_{i=0}^{k-1} (-1)^i a_{k-i} b_{i+1}.$$

The proof of Part 3. follows from the functional equation.

□

3.7 Local L-factors at Primes of Bad Reduction

Let C/K be a smooth, geometrically irreducible, projective algebraic curve of genus g and $v \in \Sigma_\mathrm{K}$ be a prime of $\mathcal{O}_K$ of bad reduction. This section illustrates how the local L-polynomial can be calculated using the information about a regular model.

The algorithm explained in this section was posted by Stoll on the sage-nt google group [48]. Since there exists no published proof of it, we are going to prove it in this section.

Algorithm 3.7.1 (Stoll [48])**.** Let $\mathcal{C}/\mathcal{O}_v$ be a regular model of $C \times K_v$. Such a model always exists by Corollary 3.5.7.

Let $X = \mathcal{C}_v$ be the fiber at v. Let $\mathcal{C}_1, \ldots, \mathcal{C}_k$ be the irreducible components of $\mathcal{C}_v$ and $g_1, \ldots, g_k$ the corresponding geometric genera of the components.

We define the "dual graph" G_v to the fiber at v by the following construction.

The graph G_v is a bipartite graph with two kinds of vertices. One kind of vertices are the components $\mathcal{C}_1, \ldots, \mathcal{C}_k$ of $\mathcal{C}_v$ and the other kind of vertices are all points $P_1, \ldots P_l$ of $\mathcal{C}_v$ that lie on more than one local branch. Two vertices P_i and $\mathcal{C}_j$ are connected by an edge, if the point P_i is contained in the component $\mathcal{C}_j$. Furthermore, there can be more than one edge between two vertices. The number of edges between P_i and $\mathcal{C}_j$ is given by the number of local branches of $\mathcal{C}_j$ at P_i.

In the rest of this section we prove the theorem:

Theorem 3.7.2 (Stoll)**.** The local L-polynomial at v is given by

$$\mathrm{L}_v(C, K, T) = \det(1 - \mathrm{Frob}_v \cdot T | \mathrm{H}_1(G_v, \mathbb{Z})) \cdot \prod_{\substack{\mathcal{C}_i \\ g_i > 0}} \det(1 - \mathrm{Frob}_v \cdot T | \mathrm{V}_\ell(\mathcal{C}_i))$$

where $\mathrm{H}_1(G_v, \mathbb{Z})$ is the first homology group of G_v and $\det(1 - \mathrm{Frob}_v \cdot T | \mathrm{V}_\ell(\mathcal{C}_i))$ can be calculated with the methods of Section 3.6, since the normalisation of $\mathcal{C}_i$ is a smooth projective curve of genus g_i over $\mathbb{F}_{\mathrm{N}_v}$.

Proof. We first show that the inertia invariant part of $\mathrm{V}_\ell(C)^*$ is isomorphic to the etale cohomology $\mathrm{H}^1_{et}(X_r, \mathbb{Q}_\ell)$, where X_r is the reduced part of the fiber $\mathcal{C}_v$.

Lemma 3.7.3. Let $\mathcal{C}$ be a regular model, $X = \mathcal{C}_v$ the special fiber at v and X_r the reduced part of X. Then

$$(\mathrm{V}_\ell(C)^*)^{\mathrm{I}_v} \cong (\mathrm{H}^1_{et}(C, \mathbb{Q}_\ell))^{\mathrm{I}_v} \cong \mathrm{H}^1_{et}(X, \mathbb{Q}_\ell) \cong H^1_{et}(X_r, \mathbb{Q}_l)$$

as Galois modules.

Proof. The fact that $\mathrm{V}_\ell(C)^* \cong \mathrm{H}^1_{et}(C, \mathbb{Q}_\ell)$ is a basic fact of etale cohomology. By Lemma 3.4.8 or [45, Lemma 2] $H^1_{et}(C, \mathbb{Q}_\ell)^{\mathrm{I}_v} \cong \mathrm{H}^1_{et}(\mathscr{J}^0_v, \mathbb{Q}_\ell)$ where $\mathscr{J}^0_v$ is the connected component of the Néron model of the Jacobian of C. We can use Theorem 2.5 of [17] to deduce that $\mathscr{J}^0_s = \mathrm{Pic}(X/k)$. Therefore,

$$H^1_{et}(X, \mathbb{Q}_\ell) \cong \mathrm{H}^1_{et}(\mathscr{J}^0_v, \mathbb{Q}_\ell)$$

Let $\mathscr{I} \subset \mathcal{O}_X$ be the ideal of nilpotent elements in the structure sheaf of X. Filtering $\mathscr{I}$ by a chain of ideals $\mathscr{I}_k$ such that $\mathscr{I} \cdot \mathscr{I}_k \subset \mathscr{I}_{k+1}$ and using the exact sequence

$$0 \to \mathscr{I}_k / \mathscr{I}_{k+1} \to (\mathcal{O}_X / \mathscr{I}_{k+1})^* \to (\mathcal{O}_X / \mathscr{I}_k)^* \to 0$$

it is easy to deduce that $\mathrm{Pic}^0(X/k)$ is an extension of $\mathrm{Pic}^0(X_r, k)$ by a unipotent group. Since H^1_{et} forgets the unipotent part (see Lemma 3.4.2), it follows that

$$H^1_{et}(X, \mathbb{Q}_\ell) \cong H^1_{et}(X_r, \mathbb{Q}_\ell).$$

This proves the lemma. □

For the rest of the proof let X_r be the reduced part of the fiber $\mathcal{C}_v$ and $\pi : X_n \to X_r$ be the normalization.

We prove the theorem by comparing two sheafs on X_r.

Let $\mathbb{Q}_\ell$ be the constant sheaf, where each stalk is equal to $\mathbb{Q}_\ell$. We compare this sheaf on X_r with the direct image sheaf of $\mathbb{Q}_\ell$ on X_n under π. That is, we look at the sequence of sheafs on X_r

$$0 \to \mathbb{Q}_\ell \to \pi_*(\mathbb{Q}_\ell) \to \mathcal{F} \to 0. \tag{3.7.1}$$

The sheaf $\pi_*(\mathbb{Q}_\ell)$ can be described on the stalks as

$$\pi_*(\mathbb{Q}_\ell)_P = \mathbb{Q}_\ell^{\#\pi^{-1}(P)},$$

for every point $P \in X_r$. Since the exact sequence (3.7.1) implies for every point $P \in X_r$ an exact sequence on the stalks

$$0 \to (\mathbb{Q}_\ell)_P \to \pi_*(\mathbb{Q}_\ell)_P \to \mathcal{F}_P \to 0$$

we can describe the sheaf $\mathcal{F}$ on each stalk as

$$\mathcal{F}_P = \mathbb{Q}_\ell^{\#\pi^{-1}(P)-1}.$$

The support of $\mathcal{F}$ is a closed set not containing any generic points of X_r, since $\#\pi^{-1}(P) = 1$ for almost all points $P \in X_r$. Therefore $\mathcal{F}$ is a skyscraper sheaf.

Taking cohomology yields a long exact sequence

$$\begin{aligned} 0 &\to \mathrm{H}^0(X_r, \mathbb{Q}_\ell) \to \mathrm{H}^0(X_r, \pi_*(\mathbb{Q}_\ell)) \to \mathrm{H}^0(X_r, \mathcal{F}) \\ &\to \mathrm{H}^1(X_r, \mathbb{Q}_\ell) \to \mathrm{H}^1(X_r, \pi_*(\mathbb{Q}_\ell)) \to \mathrm{H}^1(X_r, \mathcal{F}) \end{aligned} \tag{3.7.2}$$

To understand this long exact sequence we need a few lemmata.

Lemma 3.7.4. Let $f : X \to Y$ be a surjective map and $\mathcal{F}$ a sheaf on X. For each $i \in \mathbb{N}$

$$\mathrm{H}^i(Y, f_*(\mathcal{F})) = \mathrm{H}^i(X, \mathcal{F}).$$

Proof. Let $\mathcal{J}$ be a flasque resolution of $\mathcal{F}$ on X, then $f_*(\mathcal{J})$ is a flasque resolution of $f_*(\mathcal{F})$ on Y, and for each i,

$$\Gamma(X, \mathcal{J}^i) = \Gamma(Y, f_*(\mathcal{J}^i)) = \Gamma(Y, f_*(\mathcal{J})^i).$$

So we get

$$H^i(X, \mathcal{F}) = H^i(Y, f_*(\mathcal{F})), \text{ for all } i.$$

□

Lemma 3.7.5. Let $\mathcal{F}$ be a skyscraper sheaf on a compact scheme X. Then

$$\begin{aligned} H^0(X, \mathcal{F}) &= \bigoplus_{x \in X} \mathcal{F}_x \text{ and} \\ H^i(X, \mathcal{F}) &= 0, \text{ for } i > 0. \end{aligned}$$

Proof. The first statement is described in [34, p. 275f]: For a skyscraper sheaf $\mathcal{F}$ formed by taking the sections of a totally discontinuous sheaf which have discrete support, the group of global sections are those X-tuples with discrete support. If X is compact, then we need to have only finite support; therefore, the group of global sections in this case is the direct sum of the point groups:

$$\mathrm{H}^0(X, \mathcal{F}) = \bigoplus_{x \in X} \mathcal{F}_x \,.$$

The second statement is [34, proposition IX.4.3]. □

Therefore, the sequence (3.7.2) becomes

$$0 \to \mathrm{H}^0(X_r, \mathbb{Q}_\ell) \to \mathrm{H}^0(X_n, \mathbb{Q}_\ell) \to \mathrm{H}^0(X_r, \mathcal{F}) \to \mathrm{H}^1(X_r, \mathbb{Q}_\ell) \to \mathrm{H}^1(X_n, \mathbb{Q}_\ell) \to 0, \quad (3.7.3)$$

which we can write as

$$0 \to \mathbb{Q}_\ell \to \mathbb{Q}_\ell^n \to \bigoplus_{P \in X_r} \mathbb{Q}_\ell^{\#\pi^{-1}(P)-1} \to \mathrm{H}^1(X_r, \mathbb{Q}_\ell) \to \mathrm{H}^1(X_n, \mathbb{Q}_\ell) \to 0. \quad (3.7.4)$$

We are interested in separating this exact sequence, such that we get two exact sequences

$$0 \to \mathbb{Q}_\ell \to \mathbb{Q}_\ell^n \xrightarrow{f} \bigoplus_{P \in X_r} \mathbb{Q}_\ell^{\#\pi^{-1}(P)-1} \to \operatorname{coker}(f) \to 0 \quad (3.7.5)$$

$$0 \to \operatorname{coker}(f) \to \mathrm{H}^1(X_r, \mathbb{Q}_\ell) \to \mathrm{H}^1(X_n, \mathbb{Q}_\ell) \to 0. \quad (3.7.6)$$

We now use (3.7.5) to calculate $\operatorname{coker}(f)$, then we can use (3.7.6) to prove the theorem.

Lemma 3.7.6. The cokernel of the map f is exactly the group $\mathrm{H}_1(G_v, \mathbb{Z})$, i.e.

$$\operatorname{coker}(f) = \mathrm{H}_1(G_v, \mathbb{Z}).$$

Proof. Let G_v be the graph constructed in Algorithm 3.7.1. Since the special fiber $\mathcal{C}_v$ is connected, the graph G_v is also connected. Let V be the set of vertices and E be the set of edges. The graph G_v is a tree, i.e. a graph without loops, if it has the minimal number of edges to be connected. In this case the graph has $|V| - 1$ edges. Every additional edge adds a generator to the first homology group, so that $\mathrm{H}_1(G_v, \mathbb{Z})$ is a free group of order $|E| - |V| + 1$. By (3.7.5) this is exactly the dimension of $\operatorname{coker}(f)$. □

By Lemma 3.7.6 the exact sequence (3.7.6) can be written as

$$0 \to \mathrm{H}_1(G_v, \mathbb{Z}) \to \mathrm{H}^1(X_r, \mathbb{Q}_\ell) \to \mathrm{H}^1(X_n, \mathbb{Q}_\ell) \to 0. \quad (3.7.7)$$

Since

$$\mathrm{H}^i(X, \mathbb{Q}_\ell) = (\mathrm{H}^i_{et}(X))^{\mathrm{I}_v}$$

the exact sequence (3.7.7) becomes

$$0 \to \mathrm{H}_1(G_v, \mathbb{Z}) \to \mathrm{H}^1_{et}(X_r) \to \mathrm{H}^1_{et}(X_n) \to 0. \tag{3.7.8}$$

Since by definition $\mathrm{H}^1_{et}(X_r) = \mathrm{V}_\ell(X_r)^*$ and $\mathrm{H}^1_{et}(X_r) = \mathrm{V}_\ell(X_r)^*$, we have an exact sequence

$$0 \to \mathrm{H}_1(G_v, \mathbb{Z}) \to (\mathrm{V}_\ell(X_r)^*)^{\mathrm{I}_v} \to (\mathrm{V}_\ell(X_n)^*)^{\mathrm{I}_v} \to 0.$$

Thus, by Theorem 2.5.10

$$\begin{aligned}&\det(1 - \mathrm{Frob}_v^{-1} \cdot T|(\mathrm{V}_\ell(X_r))^*) = \\ &\det(1 - \mathrm{Frob}_v^{-1} \cdot T|(\mathrm{H}_1(G_v, \mathbb{Z})) \cdot \det(1 - \mathrm{Frob}_v^{-1} \cdot T|(\mathrm{V}_\ell(X_n))^*).\end{aligned}$$

This finishes the proof of Theorem 3.7.2.

□

We can also state an important corollary of Theorem 3.7.2, which helps us in the next sections to calculate the conductor.

Corollary 3.7.7. Let C be an algebraic curve of genus g and $v \in \Sigma_\mathrm{K}$. Then

$$\begin{aligned}\dim(\mathrm{V}_\ell\, C)^{\mathrm{I}_v} &= \dim \mathrm{V}_\ell\, \mathfrak{A} + \dim \mathrm{V}_\ell\, \mathfrak{T} \\ &= 2 \cdot a_v + t_v \\ &= 2 \cdot \sum_{\substack{\mathcal{C}_i \subset \mathcal{C}_v \\ g_i > 0}} g_i + \dim\left(\mathrm{H}_1(G_v, \mathbb{Z})\right).\end{aligned}$$

□

3.8 The Tame Part of the Conductor

In the previous section we explained in detail how the local L-factors at primes of bad reduction can be deduced using the information about a regular model. The same information also lets us deduce the tame part of the conductor, which is explained in this section. On the other hand, this information is not sufficient to calculate the wild part of the conductor. The next section explains which information is necessary to calculate the wild part of the conductor and a simple algorithm to find an upper bound for the wild part.

The tame part of the conductor measures the tame inertia of C in v.

Theorem 3.8.1. The tame part of the conductor at v is given by

$$\mathcal{N}_p^T = g - 2 \cdot \sum_{\substack{\mathcal{C}_i \subset \mathcal{C}_v \\ g_i > 0}} g_i + \dim\left(\mathrm{H}^1(G_v, \mathbb{Z})\right).$$

Proof. As expressed in (2.5.4) the tame part of the conductor is given by the equation

$$\mathfrak{f}^T_{\rho,\,v} = \operatorname{codim}(\mathrm{V}_\ell\, C)^{I_v} = \dim(\mathrm{V}_\ell\, C) - \dim(\mathrm{V}_\ell\, C)^{I_v}.$$

By Corollary 3.7.7 this is the same as

$$\begin{aligned} \mathfrak{f}^T_p &= t_p + 2u_p, \text{ and therefore} \\ \mathcal{N}^T_p &= p^{t_p + 2u_p}, \end{aligned}$$

where t_p is the dimension of the torical part and u_p is the dimension of the unipotent part. □

All necessary information for the tame part of the conductor can also be deduced from Corollary 3.7.7.

3.9 The Wild Part of the Conductor

The previous section explained the calculation of the tame part of the conductor. Since the wild part of the conductor measures the wild inertia of C in p, the information about the regular model is not enough to calculate the wild part of the conductor. Instead we need a regular model over each fixed field of the higher ramification groups G_i. In general, it is very cumbersome to determine the higher ramification groups and their corresponding regular models. On the other hand there exists a simple algorithm to determine an upper bound of the wild part of the conductor. If we further assume that the functional equation holds, then we can test a finite amount of possible conductors if the functional equation holds. This test is done much quicker in practice than the necessary calculations.

Let C/K be an algebraic curve. As expressed in Equation (2.5.5) the wild part of the conductor is given by the equation

$$\mathcal{N}^W_p = \sum_{i=1}^{\infty} \frac{|\,\mathrm{G}_i\,|}{|\,\mathrm{G}_0\,|} \operatorname{codim} \mathrm{V}_\ell(C)^{\mathrm{G}_i},$$

where the G_i are the higher ramification groups of the group I_{K_p} (cf. Definition 2.2.1).

The only way to calculate the wild inertia of C is to find a semi-stable model over a field L and then observe what kind of reduction exists in the fixed fields of the groups G_i. This is explained in detail at the end of this section. Since it is not always possible to actually calculate a semi-stable model of a curve C, it is necessary to work out other possibilities to determine the wild part of the conductor. By the work of Brumer and Kramer [12] there exists a bound for the size of the conductor.

An upper bound for the Artin conductor.

Let K be a p-adic field with absolute ramification index $e_K = \nu_K(p)$.

Brumer and Kramer define the following function on integers:

$$\lambda_p : \mathbb{Z} \to \mathbb{Z}, n \mapsto \sum_{i=0}^{s} i r_i p^i,$$

where $n = \sum_{i=0}^{s} r_i p^i$ is the p-adic expansion of n, with $0 \leqslant r_i \leqslant p-1$.

The central theorem of [12] is

Theorem 3.9.1 ([12] theorem 6.2)**.** Let A be an abelian variety of dimension g defined over the p-adic field K. We have the following bound for the exponent of the conductor:

$$\mathfrak{f}(A/K) = 2g + e_K \cdot [pd + (p-1)\lambda_p(d)],$$

where d is the greatest integer in $2g/(p-1)$. □

This is, in general, the best possible approximation of the conductor. Better approximation can only be found if more detail is known about the curve, for example over which extension exists a semi-stable model.

Calculating the wild part of the Artin conductor

It is possible to calculate the wild conductor of C if we know the extensions for which a semi-stable model of C exists.

Let C/K be an algebraic curve.

The exponent of the wild part of the conductor is defined by

$$\mathfrak{f}_p^W = \sum_{i=1}^{\infty} \frac{|\,\mathrm{G}_i\,|}{|\,\mathrm{G}_0\,|} \operatorname{codim} \mathrm{V}_\ell(C)^{\mathrm{G}_i}.$$

We are going to use the following result to calculate the wild part of the conductor.

Let $\mathfrak{C}/L$ be a semi-stable model of C, where L is a finite extension of K, so again a p-adic field.

Theorem 3.9.2 (Serre/Tate [45])**.** If $\mathfrak{C}/L$ is a semi-stable model of C then the Artin conductor of C/L is tame. That is

$$\mathcal{N}_{C/L} = \mathcal{N}_{C/L}^T \text{ and}$$
$$\mathcal{N}_{C/L}^W = 0.$$

□

Theorem 3.9.2 implies that all wild ramification of C is contained in the Galois group $G = G(L/K)$. Therefore, to calculate the wild part of the conductor we have to

1. determine all the higher ramification groups of G and
2. determine a regular model for C over all the fixed fields L^{G_i} of the higher ramification groups.

Recall the definition of the higher ramification groups:

$$G_i = \{\sigma \in G : \ \sigma(x) \equiv x \pmod{\pi^{i+1}} \quad \forall x \in \mathcal{O}_L\}.$$

But this definition is not practical to actually calculate the higher ramification groups. The following lemma allows the concrete calculation of the G_i.

Lemma 3.9.3. There exists an element $x \in \mathcal{O}_L$ such that

$$G_i = \{\sigma \in G : \ \sigma(x) \equiv x \pmod{\pi^{i+1}}\}.$$

Proof. Number theory states that there exists an element $x \in \mathcal{O}_L$, such that $\mathcal{O}_L = \mathcal{O}_K[x]$. This element therefore satisfies the relation of the lemma. □

Now that the higher ramification groups are known, the problem comes down to the calculation of $\operatorname{codim} \mathrm{V}_\ell(C)^{\mathrm{G}_i}$.

Lemma 3.9.4. Let $F_i = L^{G_i}$ be the fixed field of the group G_i and let $\mathfrak{U}_i$ be the unipotent part of A_i^0, the connected component of the fiber over p of the Néron model of the Jacobian of C over the field F_i. Then

$$\operatorname{codim} \mathrm{V}_\ell(C)^{\mathrm{G}_i} = 2 \cdot \dim(\mathfrak{U}_i).$$

□

Lemma 3.9.4 allows the calculation of $\operatorname{codim} \mathrm{V}_\ell(C)^{\mathrm{G}_i}$ by the calculation of a regular model of C over F_i and Corollary 3.8.1.

Example 3.9.5. Let $E/\mathbb{Q}$ be the elliptic curve defined by

$$y^2 = x^3 + 9.$$

The discriminant of E is $\Delta_E = -34992 = -2^4 3^7$ and therefore has bad reduction at 2 and 3.

In this example we calculate the conductor exponent $\mathfrak{f}_3$ at 3. The curve E has additive reduction (type IV) at 3 over $\mathbb{Q}$ [47, IV.9 table 4.1].

The tame part of the conductor at 3 is already known by this data, so

$$\mathfrak{f}_3^T = 2.$$

The curve E achieves semi-stable reduction over $K/\mathbb{Q}$, where K is the splitting field of the polynomial $x^{12}-3$. Let z_1 be a root of $x^{12}-3$. The field K can be described as

$$K = \mathbb{Q}[z_1, z_2],$$

where z_2 is a root of the polynomial $x^2 + z_1^2$. Thus, all the inertia that acts on $T_\ell(E)$ is contained in $G = \mathrm{Gal}_{K/\mathbb{Q}}$.

The first thing that needs to be done is the calculation of the higher inertia groups of $G_p = \mathrm{Gal}(K_p/\mathbb{Q}_p)$.

The Galois group G_p of $K_p/\mathbb{Q}_p$ is a group of order 24 given by

$$G = \{\zeta_{12}, \sigma\},$$

where ζ_{12} is a twelfth root of unity and σ is of order two.

The Inertia group $\mathrm{I}_{K_p/\mathbb{Q}_p}$ is a group of order 12 given by

$$\mathrm{I}_{K_p/\mathbb{Q}_p} = G_0 = \{\zeta_{12}\}.$$

The higher ramification groups are given by

$$G_1 = G_2 = G_3 = G_4 = G_5 = G_6 = \left\{\zeta_3 = \zeta_{12}^4\right\}$$

and

$$G_i = \{\mathrm{id}\}, \quad \text{for } i \geqslant 7.$$

Since $G_1 = \cdots = G_6$ are the only nontrivial higher ramification groups, it is only necessary to determine the regular model over the fixed field L of $G_1, \ldots, G_6$.

Let z_1' be a root of $x^4 - 3$. The field K^{G_1} can be described as

$$K^{G_1} = \mathbb{Q}[z_1', z_2'],$$

where z_2' is a root of the polynomial $x^2 + z_1'^2$.

The fiber of the minimal regular model of E over K^{G_1} is also additive (type IV), so that

$$\operatorname{codim} T_\ell(E)_{ss}^{G_i} = \operatorname{codim} T_\ell(E)^{G_i} = 2, \quad \text{for } i = 1, \ldots 6,$$

since

$$\operatorname{codim} T_\ell(E)^{G_i} = 2 \cdot \dim(\mathrm{Jac}(E)_2^U),$$

where $\mathrm{Jac}(E)_2^U$ is the unipotent part of the connected component of the Néron model of the Jacobian of E.

Since G_i is trivial for $i \geqslant 7$

$$\operatorname{codim} T_\ell(E)_{ss}^{G_i} = 0, \quad \text{for } i \geqslant 7.$$

The formula for the wild part of the conductor

$$\mathfrak{f}_p^W = \sum_{i=1}^{\infty} \frac{|\,\mathrm{G}_i\,|}{|\,\mathrm{G}_0\,|} \operatorname{codim} \mathrm{V}_\ell(C)^{\mathrm{G}_i},$$

becomes

$$\mathfrak{f}_3^W = \sum_{i=1}^{6} \frac{3}{12} \cdot 2 = 6 \cdot \frac{1}{2} = 3.$$

Therefore, the complete conductor at 3 is given by

$$\mathcal{N}_3 = \mathcal{N}_3^T \cdot \mathcal{N}_3^W = 3^{\mathfrak{f}_3^T} \cdot 3^{\mathfrak{f}_3^W} = 3^2 \cdot 3^3 = 3^5.$$

Remark 3.9.6. To effectively use Theorem 3.9.2 one needs to determine a semi-stable model of C over an extension L of K. An approach to the construction of a semi-stable model was worked out by Arzdorf, Bouw, and Wewers ([3], [4] and [11]) . This approach was used in [13] to calculate the L-series of some hyper- and superelliptic curves.

3.10 Computing the L-Function of the Curve $y^3 = 59319x^4 + (-40x + 1)^3$

In the following sections we numerically calculate the local L-factors, the conductor and the special value of the L-function at 2. As explained in Section 5.5 (Theorem 5.5.1) the curve is of special interest because it is reasonable to check the Beilinson conjecture numerically.

Let C be the curve given by the equation

$$C: \; y^3 = t(x) = 59319x^4 + (-40x + 1)^3 = 59319x^4 + f(x)^3. \tag{3.10.1}$$

The curve C has the following properties:

Lemma 3.10.1.

1. The genus of C is $g(C) = 3$.
2. The discriminant of f is

$$-189781108303677696 = -2^8 \cdot 3^{12} \cdot 13^6 \cdot 17^2.$$

3. The arithmetic surface $C/\mathbb{Z}$ defined by (3.10.1) has singular points only in the fibers above

$$2, 3, 13 \text{ and } 17.$$

Proof.

1. Calculated with Magma. See Section 6.1.
2. Calculated with Magma. See Section 6.1.
3. The arithmetic surface defined by (3.10.1) has singular points only in the fibers C_p where the Jacobi Matrix is of rank less than two. This happens only if the point (x, y) satisfies (3.10.1) as well as the derivatives in x and y modulo p. Therefore it is necessary for $f(x)$ to have double roots modulo p. These primes are exactly the factors of the discriminant of f.

□

The curve will be denoted $C_{1,3}$ in Section 3.10.

3.11 The Regular Model of the Curve $y^3 = 59319x^4 + (-40x + 1)^3$

This section describes a proper regular model $\mathcal{C}$ over $\operatorname{Spec}\mathbb{Z}$ of the curve C given by equation (3.10.1) on page 58. This model was calculated using Magma. See Section 6.1.

Let p **be different from** $2, 3, 13$ **or** 17. Since p does not divide the discriminant of $t(x)$ the special fiber at p consists of one non-singular component of genus 3.

Let p **equal** 2. The fiber $\mathcal{C}_2$ of the regular model $\mathcal{C}$ consists of two components C_1 and C_2, each of multiplicity 1. The component C_1 has genus 0 and C_2 has genus 1. The components have the intersection matrix

$$\begin{pmatrix} -3 & 3 \\ 3 & -3 \end{pmatrix}.$$

The full data reveal that the components are arranged according to Figure 3.11.1, p. 60.

Let p **equal** 3. The fiber $\mathcal{C}_3$ of the regular model $\mathcal{C}$ consists of ten components $\mathcal{C}_1, \ldots, \mathcal{C}_{10}$, each of genus 0 and $C_1, \cdots, C_5$ of multiplicity 1 and $C_6, \cdots, C_{10}$ of multiplicity 2. The components have the intersection matrix

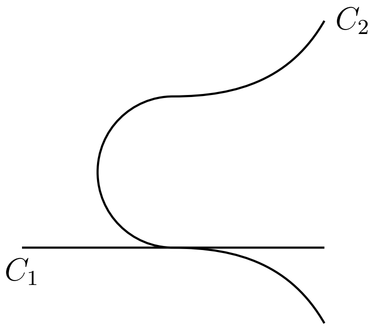


Figure 3.11.1: The fiber $\mathcal{C}_2$ of the regular model $\mathcal{C}$

$$\begin{pmatrix}
-2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & -3 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & -3 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & -4 & 2 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 2 & -2 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & -2 & 1 & 1 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & -2 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & -2 & 0 & 1 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -2 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & -2
\end{pmatrix}.$$

The full data reveal that the components are arranged according to Figure 3.11.2, p. 60.

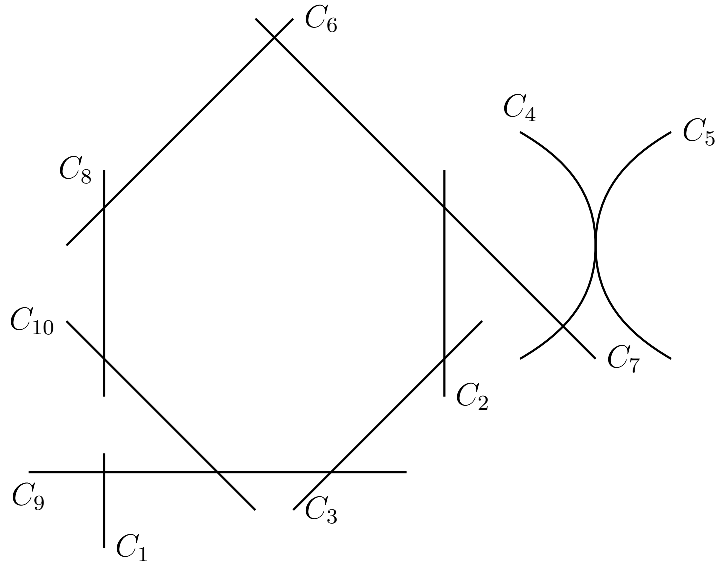


Figure 3.11.2: The fiber $\mathcal{C}_3$ of the regular model $\mathcal{C}$

Let p **equal** 13. The fiber $\mathcal{C}_{13}$ of the regular model $\mathcal{C}$ consists of ten components $\mathcal{C}_1, \ldots \mathcal{C}_{10}$, C_5 of genus 1, all other of genus 0 and $C_1, \cdots, C_5$ of multiplicity 1 and $C_6, \cdots, C_{10}$ of multiplicity 2. The components have the intersection matrix

$$\begin{pmatrix} -2 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -2 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -3 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & -3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & -2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & -2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & -2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & -2 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -2 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & -2 \end{pmatrix}.$$

The full data reveal that the components are arranged according to Figure 3.11.3, p. 61.

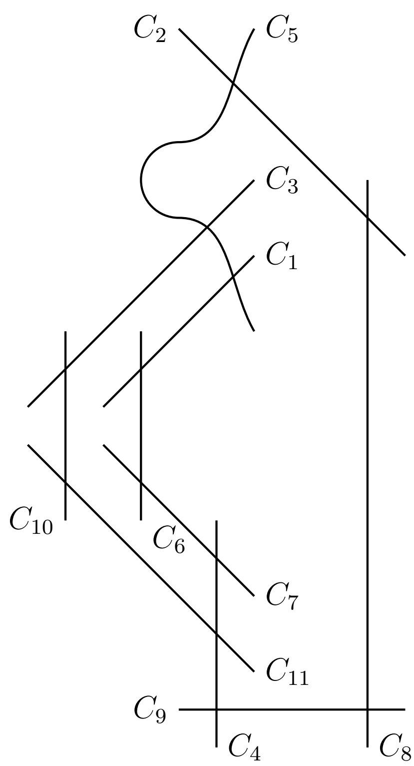


Figure 3.11.3: The fiber $\mathcal{C}_{13}$ of the regular model $\mathcal{C}$

Let p **equal** 17. The fiber $\mathcal{C}_{17}$ of the regular model $\mathcal{C}$ consists of three components C_1, C_2 and C_3, each of multiplicity 1. The component C_1 has genus 2 and C_2 and C_3

have genus 0. The components have the intersection matrix

$$\begin{pmatrix} -2 & 1 & 1 \\ 1 & -2 & 1 \\ 1 & 1 & -2 \end{pmatrix}.$$

The full data reveal that the components are arranged according to Figure 3.11.4, p. 62.

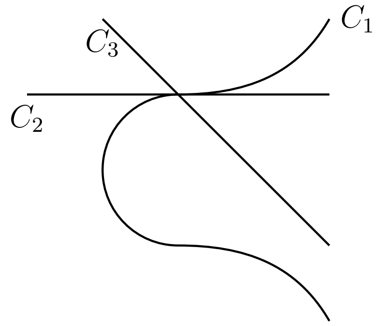


Figure 3.11.4: The fiber $\mathcal{C}_{17}$ of the regular model $\mathcal{C}$

3.12 The L-Series of the Curve $y^3 = 59319x^4 + (-40x + 1)^3$

This section describes all the necessary invariants that have to be computed to be able to calculate special values of the L-function of the curve C.

To calculate the L-function of the curve over $K = \mathbb{Q}$, it is necessary to

1. calculate the local L-polynomials of the curve over $\mathbb{Q}$,
2. calculate the conductor of the curve over $\mathbb{Q}$,
3. calculate the global root number of C .

While the calculation of the local L-polynomials at good primes can be done quickly by the computer it is necessary for the information at the primes of bad reduction to calculate a regular model. This has been done in Section 3.11. The local L-polynomials and the conductor can only be limited to a finite amount of choices. The actual value of the conductor, as well as the global root number, have to be found by numerically checking which values satisfy the functional equation. By Lemma 3.10.1 the curve has bad reduction at the primes $2, 3, 13$ and 17.

Calculating the local L-Polynomials of C.

Due to Section 3.3 it is enough for numerical calculations to know a finite number of L-polynomials, where the amount needed depends on the desired precision. The calculation of the local L-polynomials L_p splits into two parts depending on whether the curve has good reduction at the prime p.

Let p be a prime of good reduction. These are almost all primes and the required amount of L-polynomials can be computed by calculating $C_p(\mathbb{F}_p^k)$ for $0 < k \leqslant g = 3$. This can be done by the computer (cf. Section 6.3 and 6.2). For the results see Listing 6.3.1 on page 123.

Let p be a prime of bad reduction. By Section 3.11 p is equal to $2, 3, 13$ or 17. The local L-polynomial at p can be calculated by applying Stoll's Algorithm 3.7.1 to the regular model of Section 3.11.

Let p equal 2. To apply Stoll's Algorithm 3.7.1 it is necessary to construct the graph G_2 (Figure 3.12.1, p. 63). Since there are no loops in G_2 there is no toric part and the local L-polynomial is the local L-polynomial of the component C_2.

$$\mathrm{L}_2(C, T) = \mathrm{L}_2(C_2, T) = 2T^2 + 1.$$

The exponent of the tame part of the conductor is thus

$$\mathfrak{f}_2^T = 4.$$

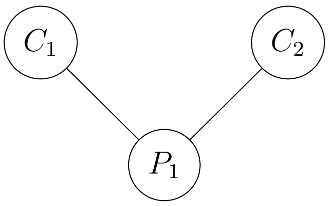


Figure 3.12.1: Graph G_2 to the fiber over 2 of C

Let p equal 3. To apply Stoll's Algorithm 3.7.1 it is necessary to construct the graph G_3 (Figure 3.12.2 page 64). Since there is one loop in G_3 but no components of positive genus in $\mathcal{C}_3$ the algorithm ensures that the Jacobian of the fiber is a variety with a toric part of dimension 1 and a unipotent part of dimension 2. Frobenius acts trivially on the graph G_3. Therefore, the local L-polynomial by Stoll's algorithm is

$$\mathrm{L}_3(C, T) = 1 - T.$$

The exponent of the tame part of the conductor is thus

$$\mathfrak{f}_3^T = 5.$$

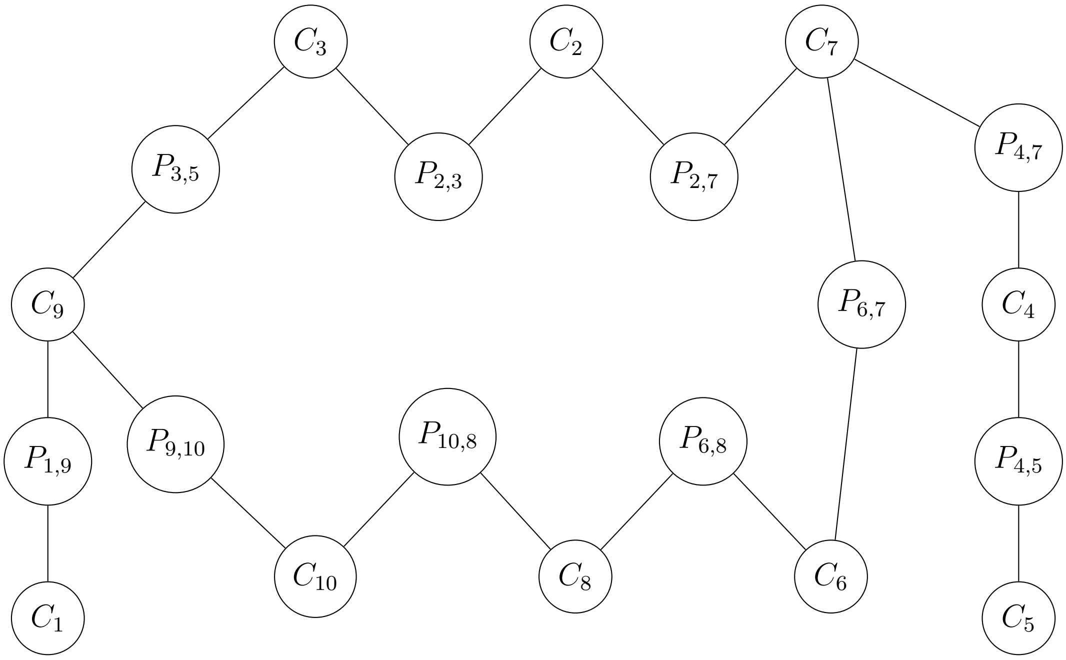


Figure 3.12.2: Graph G_3 to the fiber over 3 of C

Let p **equal** 13. To apply Stoll's Algorithm 3.7.1 it is necessary to construct the graph G_{13} (Figure 3.12.3 p. 65). Since there are two loops in G_{13} and one component of positiv genus in $\mathcal{C}_{13}$ the algorithm ensures that the Jacobian of the fiber is a variety with a toric part of dimension 2 and a unipotent part of dimension 0. Frobenius acts trivially on the graph G_{13}. Therefore, the local L-polynomial by Stoll's algorithm is

$$\mathrm{L}_{13}(C,T) = \mathrm{L}_{13}(C_5,T)(1-T)^2 = (13T^2 - 5T + 1)(1-T)^2.$$

The exponent of the conductor is thus

$$\mathfrak{f}_{13} = \mathfrak{f}_{13}^T = 2.$$

Let p **equal** 17. To apply Stoll's Algorithm 3.7.1 it is necessary to construct the graph G_{17} (Figure 3.12.4, p. 65). Since there are no loops in G_{17} there is no toric part and the local L-polynomial is the local L-polynomial of the component C_1.

$$\mathrm{L}_{17}(C,T) = \mathrm{L}_{17}(C_1,T) = 289T^4 - 2T^2 + 1.$$

The exponent of the conductor is thus

$$\mathfrak{f}_{17}^T = 2.$$

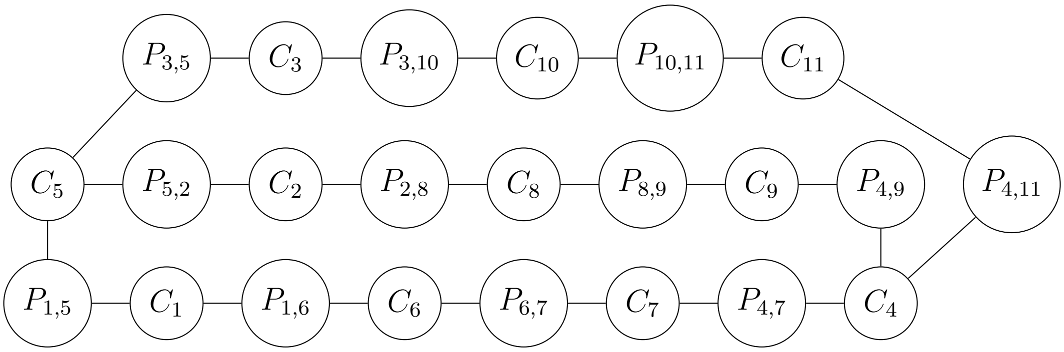


Figure 3.12.3: Graph G_{13} to the fiber over 13 of C

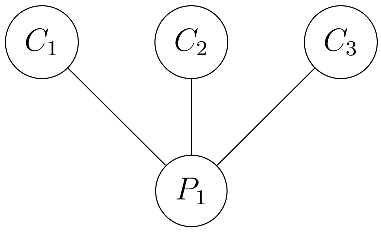


Figure 3.12.4: Graph G_2 to the fiber over 17 of C

Calculating the conductor.

The conductor is the invariant of the functional equation that is most difficult to calculate. To actually calculate the conductor it would be necessary to be able to determine a number field for which there exists a semi-stable model of C. This is rather difficult to do, so for the present work it is sufficient to calculate a lower and an upper bound for the conductor and determine the actual value of the conductor by checking the functional equation.

A lower bound for the conductor of C. The conductor is made of two parts: the tame and the wild part (cf. Section 3.8 and 3.9). The tame part is defined by

$$\mathcal{N} = \prod_{p \subset \mathbb{Z}} p^{a_p}, \quad a_p = T + 2U,$$

where T is the dimension of the torical subvariety and U is the dimension of the unipotent subvariety of $\mathrm{Jac}(\mathcal{C}_p)$.

This has already been calculated in this section, so

$$\mathcal{N}_{\mathbb{Q}}^{T} = 2^4 \cdot 3^5 \cdot 13^2 \cdot 17^2.$$

An upper bound for the conductor of C. As described in Section 3.9 an upper bound for the conductor of C can be given by the formula

$$\begin{aligned}
\mathcal{N}_{\mathbb{Q}} &\leqslant 2^{m_2} 3^{m_3} 13^2 17^2 \\
m_p &= 2g + (pd_p + (p-1)\lambda_p(d_p)) \\
d_p &= \lfloor \frac{2g}{p-1} \rfloor \\
\lambda_p(n) &= \sum_{i=0}^{s} i r_i p^i \text{ where} \\
n &= \sum_{i=0}^{s} r_i p^i
\end{aligned}$$

is the p-adic expansion of n, with $0 \leqslant r_i \leqslant p-1$. By using this formula we get the following upper bound for the conductor

$$2^4 \cdot 3^5 \cdot 13^2 \cdot 17^2 \leqslant \mathcal{N}_{\mathbb{Q}} \leqslant 2^{28} 3^{21} 13^2 17^2.$$

Determine the conductor by numerical calculations. Since there is only a finite number of choices, it is now possible to calculate the conductor through numerical calculations. That is, assuming that the L-function of C satisfies a functional equation, the computer can check the functional equation for each possible conductor whether the functional equation is satisfied or not.

While in theory that seems a reasonable attempt, in practice it is quite hard to do. The reason for this failure of feasibility is due to the amount of Euler factors that need to be calculated. For a curve C of genus g the computation of the Euler factor includes counting points in $C(\mathbb{F}_{p^n})$ for $n \leqslant g$ which is quite a tedious task, even for computers, and with growing conductor the number of required factors to achieve the same level of precision grows. For the curve in this example the genus of 3 is quite small but the conductor is bigger than in most previously considered examples. Even after one month of work by a computer to calculate the Euler factors it was not possible to test whether all potential conductors satisfy the functional equation. But since there was only one conductor which satisfied the functional equation among the tested conductors it is reasonable to assume that this is the conductor of the curve. Therefore, the conductor of the curve is probably

$$\mathcal{N}_{\mathbb{Q}} = 2^6 \cdot 3^5 \cdot 13^2 \cdot 17^2.$$

Calculating the global root number.

The only practical method to find the global root number is to actually test the functional equation. This is not too hard since it is known that $W_C = \pm 1$. The numerical data for this example suggest that the sign of the functional equation is

$$W_C = 1.$$

Remark 3.12.1. The root number and the conductor exponent were found by a numerical experiment with Magma. For this experiment the first 960643 coefficients were used. The accuracy of the computation in dependency of the set precision as calculated by ComputeL is displayed in Table 3.12.5. Magma offers two functions to check the functional equation. The new function "CFENew" offers much betters results than the old function "CheckFunctionalEquation". The precision was bound by 23 due to the number of coefficients used.

Conclusion

The values of the invariants needed have been calculated by the computer (cf. Section 6.3). We now collect these result in one of the main results of this thesis.

Theorem 3.12.2.

1. The local Euler factors up to a certain prime P depending on the preset precision. A list of local Euler factors up to $P = 97$ is contained in Table 3.12.6, p. 69.
2. The conductor that enters the functional equation

$$\mathrm{N}_{\mathbb{Q}} = \mathrm{Nm}(\mathcal{N}_{\mathbb{Q}}) = 2^6 \cdot 3^5 \cdot 13^2 \cdot 17^2.$$

3. The global root number

$$W_C = 1.$$

The numerical calculations with ComputeL yields

$$\mathrm{L}(C, \mathbb{Q}, 2) \approx 1.04321034530598890940.$$

The functional equation Equation 2.5.7) then determines the value of $\mathrm{L}^*(C, 0)$ as

$$\begin{aligned} \mathrm{L}^*(C, \mathbb{Q}, 0) &= \mathrm{L}^*(C, \mathbb{Q}, 2) \\ &= \frac{\mathrm{Nm}(\mathcal{N}_{\mathbb{Q}})}{(2\pi)^6} \mathrm{L}(C, \mathbb{Q}, 2) \\ &= \frac{\mathrm{N}_{\mathbb{Q}}}{(2\pi)^6} \mathrm{L}(C, \mathbb{Q}, 2) \\ &\approx 12878.446259. \end{aligned}$$

□

Precision	*Accuracy with CheckFunctionalEquation*	*Accuracy with CFENew*
1	8.0E2	0.00
2	8.0	0.00
3	1.00	0.000
4	0.06250	6.104E-5
5	0.0039062	0.00000
6	0.00292969	0.000000
7	0.0001220703	5.960464E-8
8	2.6702881E-5	0.00000000
9	2.38418579E-6	1.86264515E-9
10	1.192092896E-7	0.0000000000
11	7.4505805969E-9	1.4551915228E-11
12	9.31322574615E-10	9.09494701773E-13
13	2.910383045673E-10	2.842170943040E-13
14	2.1827872842550E-11	1.4210854715202E-14
15	5.91171556152403E-12	0.000000000000000
16	5.684341886080801E-14	0.0000000000000000
17	4.26325641456060011E-14	6.93889390390722284E-18
18	1.154631945610162780E-14	1.734723475976807094E-18
19	3.0531133177191804860E-16	0.0000000000000000000
20	1.04083408558608425660E-17	2.71050543121376108500E-20
21	Not enough coefficients	6.776263578034402712550E-21
22	Not enough coefficients	4.2351647362715016953420E-22
23	Not enough coefficients	2.64697796016968855958850E-23

Table 3.12.5: Accuracy of the functional equation test

p	$\mathrm{L}_p(C,T)$
2	$2T^2+1$
3	$1-T$
5	$125T^6-15T^4-3T^2+1$
7	$343T^6+49T^5+35T^4-2T^3+5T^2+T+1$
11	$1331T^6-99T^4-9T^2+1$
13	$13T^4-31T^3+24T^2-7T+1$
17	$289T^4-2T^2+1$
19	$6859T^6+361T^5-133T^4-26T^3-7T^2+T+1$
23	$12167T^6+897T^4+39T^2+1$
29	$24389T^6+957T^4+33T^2+1$
31	$29791T^6-4805T^5+1643T^4-326T^3+53T^2-5T+1$
37	$50653T^6-12321T^5+999T^4-38T^3+27T^2-9T+1$
41	$68921T^6+1353T^4+33T^2+1$
43	$79507T^6+12943T^5-301T^4-422T^3-7T^2+7T+1$
47	$103823T^6+2115T^4+45T^2+1$
53	$148877T^6-1113T^4-21T^2+1$
59	$205379T^6+6549T^4+111T^2+1$
61	$226981T^6-55815T^5+915T^4+718T^3+15T^2-15T+1$
67	$300763T^6-22445T^5-2077T^4+850T^3-31T^2-5T+1$
71	$357911T^6+3621T^4+51T^2+1$
73	$389017T^6+31974T^5+219T^4+412T^3+3T^2+6T+1$
79	$493039T^6-124820T^5+20303T^4-2408T^3+257T^2-20T+1$
83	$571787T^6+7221T^4+87T^2+1$
89	$704969T^6+1335T^4+15T^2+1$
97	$912673T^6-141135T^5+1455T^4+1150T^3+15T^2-15T+1$

Table 3.12.6: Local Euler factors $\mathrm{L}_p(C,T)$ for all $p<100$

4 K-Theory of Algebraic Curves

After the definition of the L-function in the previous chapter this chapter covers basic algebraic K-theory for algebraic curves. Both theories are combined in the Beilinson conjectures which are covered at the end of this chapter.

4.1 The Second Tame K-Group of Curves

In Chapter 1 we gave the definitions for K_1 and K_2 of number fields.

It turns out that it is complicated to define the higher K-groups for number fields, or even any K-group for curves or schemes.

In the case where F is a field, there is the following famous theorem by Matsumoto.

Theorem 4.1.1 (Matsumoto [33, Theorem 11.1])**.** The abelian group $\mathrm{K}_2(F)$ has a presentation, in terms of generators and relations, as follows:
The generators are $\{a, b\}$, where $a, b \in F^*$, they are subject only to the following relations and their consequences:

1. $$\{a, 1-a\} = 1 \text{ for } a \neq 0, 1$$
2. $$\{a_1 a_2, b\} = \{a_1, b\}\{a_2, b\}$$
3. $$\{a, b_1 b_2\} = \{a, b_1\}\{a, b_2\}$$

□

For the remaining chapter let K be a number field of degree $d = [K : \mathbb{Q}]$ and let C be a (non-singular, projective, geometrically irreducible) curve defined over K.

For every $n \in \mathbb{N}$ there exists a K-group $\mathrm{K}_n(C)$, but in this thesis we take a look at only a certain quotient group of $\mathrm{K}_2(C)$, which we call $\mathrm{K}_2^T(C)$ in accordance with [19] [1]. The 'T' stands for 'tame' quotient group.

[1] Usually denoted by $\mathrm{H}^0(C, \underline{\mathcal{K}})_2$

Definition 4.1.2 ([19] p. 243)**.** We define $\mathrm{K}_2^T(C)$, the second tame K-group of C, to be

$$\mathrm{K}_2^T(C) = \ker\left(\mathrm{K}_2(F) \xrightarrow{T} \bigoplus_{x \in C(\overline{\mathbb{Q}})} \overline{\mathbb{Q}}^* \right), \tag{4.1.1}$$

where $F = K(C)$ is the function field of C and where the x-component of the map T is the $t$ame symbol at x, defined by

$$T_x : \{a, b\} \mapsto (-1)^{\mathrm{ord}_x(a)\,\mathrm{ord}_x(b)} \frac{a^{\mathrm{ord}_x(b)}}{b^{\mathrm{ord}_x(a)}}(x) \,. \tag{4.1.2}$$

Lemma 4.1.3. The tame symbol T_x is a map on $\mathrm{K}_2(F)$ and for each $x \in C(\overline{\mathbb{Q}})$ the image is in $\overline{\mathbb{Q}}^*$.

Proof. Since for each $x \in C(\overline{\mathbb{Q}})$ the order of $\frac{a^{\mathrm{ord}_x(b)}}{b^{\mathrm{ord}_x(a)}}$ is

$$\begin{aligned} \mathrm{ord}\left(\frac{a^{\mathrm{ord}_x(b)}}{b^{\mathrm{ord}_x(a)}}\right) &= \mathrm{ord}(a^{\mathrm{ord}_x(b)}) - \mathrm{ord}(b^{\mathrm{ord}_x(a)}) && (4.1.3)\\ &= \mathrm{ord}(a)\,\mathrm{ord}_x(b) - \mathrm{ord}(b)\,\mathrm{ord}_x(a) && (4.1.4)\\ &= 0 && (4.1.5) \end{aligned}$$

Thus, $\frac{a^{\mathrm{ord}_x(b)}}{b^{\mathrm{ord}_x(a)}}$ has order zero at x and therefore it is defined and non-zero.

Furthermore, it is clear that T_x is a map on $F^* \otimes_{\mathbb{Z}} F^*$. To finish the proof we have to show that T_x is trivial on the symbols $\{a, 1-a\}$ for $a \neq 0, 1$. We prove that for all x, depending on the order of a at x. Since $T_x(a, b) = T_x(b, a)^{-1}$ we can assume that $\mathrm{ord}_x(a) \geqslant \mathrm{ord}_x(1-a)$.

1. Let $x \in C(\overline{\mathbb{Q}})$ such that $\mathrm{ord}_x(a) > 0$ then $\mathrm{ord}_x(1-a) = 0, (1-a)(x) = 1$ and

$$\begin{aligned} T_x(\{a, 1-a\}) &= (-1)^{\mathrm{ord}_x(a)\,\mathrm{ord}_x(1-a)} \frac{a^{\mathrm{ord}_x(1-a)}}{(1-a)^{\mathrm{ord}_x(a)}}(x) \\ &= (-1)^{\mathrm{ord}_x(a)\,\mathrm{ord}_x(1-a)} \frac{a^{\mathrm{ord}_x(1-a)}}{(1-a)^{\mathrm{ord}_x(a)}}(x) \\ &= \frac{1}{(1-a)^{\mathrm{ord}_x(a)}}(x) \\ &= 1 \end{aligned}$$

2. Let $x \in C(\overline{\mathbb{Q}})$ such that $\mathrm{ord}_x(a) = 0$ and $a(x) \neq 1$ then $\mathrm{ord}_x(1-a) = 0$ and

$$\begin{aligned} T_x(\{a, 1-a\}) &= (-1)^{\mathrm{ord}_x(a)\,\mathrm{ord}_x(1-a)} \frac{a^{\mathrm{ord}_x(1-a)}}{(1-a)^{\mathrm{ord}_x(a)}}(x) \\ &= (-1)^{\mathrm{ord}_x(a)\,\mathrm{ord}_x(1-a)} \frac{a^{\mathrm{ord}_x(1-a)}}{(1-a)^{\mathrm{ord}_x(a)}}(x) \\ &= 1 \end{aligned}$$

3. Let $x \in C(\overline{\mathbb{Q}})$ such that $\mathrm{ord}_x(a) < 0$ then $\mathrm{ord}_x(1-a) = \mathrm{ord}_x(a) < 0$ and

$$\begin{aligned}
T_x(\{a, 1-a\}) &= (-1)^{\mathrm{ord}_x(a)\,\mathrm{ord}_x(1-a)} \frac{a^{\mathrm{ord}_x(1-a)}}{(1-a)^{\mathrm{ord}_x(a)}}(x) \\
&= (-1)^{\mathrm{ord}_x(a)\,\mathrm{ord}_x(a)} \frac{a^{\mathrm{ord}_x(a)}}{(1-a)^{\mathrm{ord}_x(a)}}(x) \\
&= (-1)^{\mathrm{ord}_x(a)\,\mathrm{ord}_x(a)} \frac{a^{\mathrm{ord}_x(a)}}{(\frac{a-1}{a})^{\mathrm{ord}_x(a)}}(x) \\
&= (-1)^{\mathrm{ord}_x(a)\,\mathrm{ord}_x(a)} \left(\frac{a(a-1)}{a}\right)^{\mathrm{ord}_x(a)}(x) \\
&= (-1)^{\mathrm{ord}_x(a)\,\mathrm{ord}_x(a)} (a-1)^{\mathrm{ord}_x(a)}(x) \\
&= (-1)^{\mathrm{ord}_x(a)(\mathrm{ord}_x(a)+1)} \\
&= 1
\end{aligned}$$

□

There is a product formula for elements of $\mathrm{K}_2(K(C))$ due to Weil.

Theorem 4.1.4. [5, VI Theorem 8.2] Let α be an element of $K_2(K(C))$, then

$$\prod_{x \in C(\overline{\mathbb{Q}})} T_x(\alpha) = 1.$$

□

4.2 Constructing Elements of K_2 from Torsion Divisors

In the last section we defined $\mathrm{K}_2(C, \mathcal{O}_K)$. In this section we look at ways to generate elements in $\mathrm{K}_2(C, \mathcal{O}_K)$.

This section is completely taken from Dokchitser, de Jeu and Zagier [19] chapter 4 and it also coincides with [29]. This section explains the preliminaries for the next chapter and is included as a reference. No work of the author has been done in this subsection.

What does it mean that the tame symbol is trivial? Let $\{f, g\} \in K_2(K(C))$ be a symbol and $P \in C$ be a point of C.

1. If $P \notin \mathrm{div}(f) \cup \mathrm{div}(g)$, then the tame symbol is automatically trivial, since $\mathrm{ord}_P(f) = \mathrm{ord}_P(g) = 0$.
2. If $P \in \mathrm{div}(f) \cup \mathrm{div}(g)$, but $P \notin \mathrm{div}(f) \cap div(g)$, e.g. $P \notin \mathrm{div}(g)$ then the tame symbol is trivial, if by definition $g^{\mathrm{ord}_P(f)} = 1$. This means, that if f and g have disjoint support, then f needs to be one (or a root of unity), for every pole and zero of g and vice versa.

3. Only if $P \in \operatorname{div}(f) \cap \operatorname{div}(g)$ we need the full definition.

Therefore, to satisfy these conditions it is natural to look for functions with only very few zeroes and poles. The simplest case is that both functions have only one (multiple) zero and one (multiple) pole. If, additionally, one of these points belongs to the support of both functions then it turns out that a renormalization is enough to make the tame symbol trivial. Thus, we look for triplets of points such that their pairwise differences are torsion divisors. For each such triplet we get three elements of $\mathrm{K}_2^T(C)$. This construction is known as an explicit version of Bloch's trick.

Construction 4.2.1 ([19] Construction 4.1)**.** Let C/K be a curve. Let P_1, P_2, and $P_3 \in C(K)$ be distinct triplet of points and f_1, f_2, and f_3 be rational functions with

$$\operatorname{div}(f_i) = m_i(P_{i+1}) - m_i(P_{i-1}), \qquad i \in \mathbb{Z}/3\mathbb{Z}\,,$$

where m_i is the order of $(P_{i+1}) - (P_{i-1})$ in the divisor group $\operatorname{Pic}^0(C)$. For this triplet we define three elements of $\mathrm{K}_2(K(C))$ by setting

$$S_i = \left\{ \frac{f_{i+1}}{f_{i+1}(P_{i+1})}, \frac{f_{i-1}}{f_{i-1}(P_{i-1})} \right\}, \qquad i \in \mathbb{Z}/3\mathbb{Z}\,.$$

The symbols S_i are uniquely defined by the triplet, because the functions are unique up to constants.

Lemma 4.2.2 ([19] Lemma 4.2)**.** The S_i are elements of $\mathrm{K}_2^T(C)$. □

The construction yields three elements for every triplet of points, which would make it possible that only few triplets are necessary to check the Beilinson conjectures. This is not the case as the following facts show.

Proposition 4.2.3. We keep the notation of Construction 4.2.1.

1. ([19] Proposition 4.3). There is a unique element $\{P_1, P_2, P_3\}$ of $\mathrm{K}_2^T(C)$/torsion such that in this group

$$S_i = \frac{\operatorname{lcm}(m_1, m_2, m_3)}{m_i} \{P_1, P_2, P_3\}, \qquad i = 1, 2, 3\,.$$

2. ([19] Proposition 4.3). The element $\{P_1, P_2, P_3\}$ is unchanged under even permutations and changes sign under odd permutations of the points.
3. ([19] Proposition 4.6). Let P_1, P_2, P_3, P_4 be four distinct points in $C(K)$ such that all $(P_i) - (P_j)$ are torsion divisors. Then, the four elements

$$\{P_1, \ldots, \widehat{P}_i, \ldots, P_4\} \qquad (1 \leqslant i \leqslant 4)$$

are linearly dependent. More precisely, if m_{ij} is the order of $(P_i) - (P_j)$, then

$$\sum_{i=1}^{4} c_i \{P_1, \ldots, \hat{P}_i, \ldots, P_4\} = 0$$

holds in $\mathrm{K}_2^T(C)$ with

$$c_i = \gcd(m_{ij}, m_{ik}, m_{il}) \quad (\{i,j,k,l\} = \{1,2,3,4\}).$$

4. ([19] Corollary 4.13). Let $P_1, \ldots, P_n \in C(K)$ be points such that all $(P_i) - (P_j)$ are torsion. Then, the subspace of $K_2^T(C) \otimes K$ generated by all elements $\{P_i, P_j, P_k\}$ is already generated by those of the form $\{P_1, P_i, P_j\}$.
5. ([19] Proposition 4.15). Let $S \subseteq C(\overline{\mathbb{Q}})$ and $P_0 \in S$ be such that $(P) - (P_0)$ is a torsion divisor for all P in S. Let V be the subspace of $K_2^T(C_{\overline{\mathbb{Q}}}) \otimes K$ generated by all elements $\{P, Q, P_0\}$ with $P, Q \in S$ and W be the subspace of $K_2(\overline{\mathbb{Q}}(C)) \otimes K$ generated by all symbols $\{f, g\}$ with $\operatorname{div}(f)$ and $\operatorname{div}(g)$ supported in S. Then,

$$W \cap \mathrm{K}_2^T(C_{\overline{\mathbb{Q}}}) \otimes K = V.$$

$\square$

This collection of propositions tells us a lot about the elements that we can create if we have n points $P_1, \cdots P_n$, such that $P_i - P_j$ is torsion for $i \neq j$. Part 1 of Theorem 4.2.3 states that for any family (P_i, P_j, P_k) of three elements we get exactly one element $\{P_i, P_j, P_k\}$ of $\mathrm{K}_2^T(C)$/torsion. Part 2 tells us that these elements at most change sign if we permute the P_i, P_j and P_k. That is, we can get at most $\binom{n}{3}$ linearly independent elements. Part 3 and its corollary Part 4 give us even more dependencies, such that we can get at most $\binom{n-1}{2}$ linearly independent elements in $\mathrm{K}_2^T(C)$. At last, Part 5 states that all elements with functions, such that their poles and zeroes are contained in $P_1, \cdots, P_n$, are linear combinations of the elements of Construction 4.2.1.

Corollary 4.2.4 ([19] p. 348)**.** If $P_1, \cdots P_n$ are points on C, such that $P_i - P_j$ is torsion for $i \neq j$, then there are at most $\binom{n-1}{2}$ elements of $\mathrm{K}_2^T(C)$/torsion that can be constructed by applying Construction 4.2.1 to $P_1, \cdots P_n$. $\square$

4.3 The Regulator Pairing

In this chapter we define the regulator pairing for $\mathrm{K}_2^T(C)$. The general regulator of the K-groups of C (see [41]) was defined by Beilinson, who was generalizing work by Bloch. We follow the description in [19] to describe the regulator for $\mathrm{K}_2^T(C)$ in elementary terms.

First, we prove that there exists a pairing from $H_1(X, \mathbb{Z})^- \times \mathrm{K}_2^T(C)$/torsion to $\mathbb{R}$.

Theorem 4.3.1. There exists a pairing

$$\langle \cdot, \cdot \rangle : H_1(X, \mathbb{Z})^- \times \mathrm{K}_2^T(C)/\text{torsion} \to \mathbb{R} \tag{4.3.1}$$

called the $r$egulator pairing defined by

$$\langle \gamma, (a, b) \rangle = \int_\gamma (\log|a| d\arg b - \log|b| d\arg a)$$

for $\gamma \in H_1(X, \mathbb{Z})^-$ and $(a, b) \in \mathrm{K}_2^T(C)/\text{torsion}$.

Proof. We define η as a map from $F^* \times F^*$ to the group of almost everywhere defined 1-forms on the Riemann surface $X = C(K)$ which consists of d connected components X_σ, one for each embedding $\sigma : K \to \mathbb{C}$, each of genus g.

The map is defined on the connected component X_σ as

$$\eta_\sigma(a, b) = \log|a_\sigma| d \arg b_\sigma - \log|b_\sigma| d \arg a_\sigma,$$

where $\arg z$ is the argument of z. The subscripts indicate that we consider the functions on the Riemann surface obtained by applying σ to the coefficients involved in a and b.

For simplicity we drop the subscripts in the following, since the meaning is clear.

Lemma 4.3.2. The map η is well-defined, and $\eta(a, b)$ is a smooth and closed 1-form on the complement of the set of zeroes and poles of a and b.

Proof. The map η is well defined since the argument arg is defined up to multiples of 2π, but these multiples map to zero under the derivative d.

The image $\eta(a, b)$ is a smooth (even real-analytic) 1-form on the complement of the set of zeroes and poles of a and b, because it is a composition of smooth 1-forms.

The image $\eta(a, b)$ is closed, since $\log z = \log|z| + i \arg z$ and therefore

$$\begin{aligned} d\eta(a, b) &= d(\log|a| d \arg b - \log|b| d \arg a) \\ &= d \log|a| d \arg b - d \log|b| d \arg a \\ &= \operatorname{Im}(d \log a \wedge d \log b) \\ &= 0 \end{aligned}$$

□

Moreover, η even induces a map on $F^* \otimes_{\mathbb{Z}} F^*$ that we also denote by η.

Lemma 4.3.3. The map η induces a map

$$\eta : F^* \otimes_{\mathbb{Z}} F^* \to \text{group of almost everywhere defined 1-forms.}$$

Proof. Let $a, a_1, a_2, b, b_1, b_2 \in F^*$. By definition

$$\eta(a_1 a_2, b) = \eta(a_1, b) + \eta(a_2, b) \quad \text{and } \eta(a, b_1 b_2) = \eta(a, b_1) + \eta(a, b_2).$$

□

For any smooth closed 1-form ω defined on the complement of a finite set $S \subset X$ and any smooth oriented loop γ in $X \backslash S$, we have a pairing

$$(\gamma, \omega) = \frac{1}{2\pi} \int_\gamma \omega$$

which only depends on the homology class of γ in $X \backslash S$. As γ moves across a point x in S, the value of (γ, ω) increases by (C_x, ω), where C_x denotes a small circle around x.

Lemma 4.3.4 ([19] p. 343)**.** If $\alpha = \sum_i a_i \otimes b_i \in F^* \otimes_{\mathbb{Z}} F^*$ such that $\mathrm{T}_x(\alpha) = 1$ for all $x \in X$, then

$$(\cdot, \eta(\alpha)) : H_1(X, \mathbb{Z}) \to \mathbb{R}$$

is a well-defined map. □

We can now prove that we have a pairing on $H_1(X, \mathbb{Z}) \times \mathrm{K}_2^T(C)$.

Lemma 4.3.5. There exists a pairing

$$\langle \cdot, \cdot \rangle : H_1(X, \mathbb{Z}) \times \mathrm{K}_2^T(C) \to \mathbb{R}$$

given by

$$\langle \gamma, \alpha \rangle = (\gamma, \eta(\alpha)).$$

Proof. To prove the lemma, we have to show that

$$\eta(\alpha) = 0$$

for all $\alpha = a \otimes (1 - a)$.

Let $\alpha = a \otimes (1 - a)$. Then

$$\begin{aligned} \eta(\alpha) &= \log|a| d \arg(1 - a) - \log|(1 - a)| d \arg a \\ &= dD(a) \\ &= 0 \end{aligned}$$

where $D(z)$ is the Bloch-Wigner dilogarithm function (see [19] p. 343). □

Now, we are almost ready to prove the Theorem 4.3.1 using the following lemma.

Lemma 4.3.6. If $\gamma \in H_1(X, \mathbb{Z})^+$, the invariant part under complex conjugation, then

$$\langle \gamma, \alpha \rangle = 0 \text{ for any } \alpha \in \mathrm{K}_2^T(C).$$

Proof. Let c denote the complex conjugation on X, then

$$\begin{aligned} c^*(\eta(\alpha)) &= \log|c^*(a)| d \arg c^*(b) - \log|c^*(b)| d \arg c^*(a) \\ &= \log|a|(-d \arg b) - \log|b|(-d \arg a) \\ &= -\log|a| d \arg b + \log|b| d \arg a \\ &= -\eta(\alpha) \end{aligned}$$

for any $\alpha \in \mathrm{K}_2^T(C)$.

Let $\gamma \in H_1^+(X, \mathbb{Z})$, then

$$\langle \gamma, \alpha \rangle = \frac{1}{2\pi} \int_\gamma \eta(\alpha) = \frac{1}{2\pi} \int_{c \circ \gamma} \eta(\alpha) = \frac{1}{2\pi} \int_\gamma c^*(\eta(\alpha)) = -\frac{1}{2\pi} \int_\gamma \eta(\alpha) = -\langle \gamma, \alpha \rangle,$$

for all $\alpha \in \mathrm{K}_2^T(C)$.

Thus,

$$\langle \gamma, \alpha \rangle = 0 \text{ for any } \alpha \in \mathrm{K}_2^T(C)$$

for all $\gamma \in H_1(X, \mathbb{Z})^+$. □

By the last lemma we have a pairing on $H_1(X, \mathbb{Z})/H_1(X, \mathbb{Z})^+$.

This gives us a pairing

$$\langle \cdot, \cdot \rangle : H_1(X, \mathbb{Z})^- \times \mathrm{K}_2^T(C) \to \mathbb{R}.$$

Since the pairing is bilinear and the image is in $\mathbb{R}$, we get a pairing

$$\langle \cdot, \cdot \rangle : H_1(X, \mathbb{Z})^- \times \mathrm{K}_2^T(C)/\text{torsion} \to \mathbb{R}.$$

This proves Theorem 4.3.1.

□

4.4 The Beilinson Conjectures

The conjecture originally stated by Beilinson is equivalent to the statement that the pairing in Theorem 4.3.1 is non-degenerate, that the rank of $\mathrm{K}_2^T(C)$/torsion is equal to dg and that the absolute value of the determinant of the matrix of this pairing with respect to bases of $H_1(X, \mathbb{Z})^-$ and $\mathrm{K}_2^T(C)$/torsion is in rational relation to the special value of the L-function $\mathrm{L}(C, s)$. Note that $H_1(X, \mathbb{Z})^-$ is always of rank dg, since X consists of d irreducible components X_i, each corresponding to one embedding of K in $\mathbb{C}$.

However, Bloch and Grayson [7] discovered that this conjecture is wrong. They showed that $\mathrm{K}_2^T(C)$/torsion can have rank larger than 1 for elliptic curves. They refined the conjecture in the following way.

Instead of considering the curve over the number field K one should consider the curve over the ring of integers $\mathcal{O}_K$. This is similar to Chapter 1.4, where Theorem 1.4.1 used $\mathrm{K}_0(\mathcal{O}_K)$ and $\mathrm{K}_1(\mathcal{O}_K)$. Over this ring there exists a regular proper model of C, i.e. a regular, proper, irreducible two-dimensional scheme $\mathcal{C}$ over $\mathcal{O}_K$ such that the generic fiber $\mathcal{C}_K$ is isomorphic to C.

Let $\mathcal{C}$ be a regular proper model of C. For more information on regular proper models see [30].

For each prime $\mathfrak{p}$ of $\mathcal{O}_K$, $\mathcal{C}_p$ denotes the fiber of $\mathcal{C}$ over $\mathbb{F}_{\mathfrak{p}}$. For each irreducible component $\mathcal{D}$ of the curve $\mathcal{C}_p$, let $\mathbb{F}_{\mathfrak{p}}(\mathcal{D})$ denote its field of rational functions over $\mathbb{F}_p$.

Definition 4.4.1 ([19] p. 343)**.** We refine the definition of $\mathrm{K}_2^T(C)$ (formula (4.1.1) on page 72) by setting

$$\mathrm{K}_2^T(\mathcal{C}) = \ker\left(\mathrm{K}_2^T(C) \xrightarrow{T} \bigoplus_{\mathfrak{p},\mathcal{D}\subseteq\mathcal{C}_{\mathfrak{p}}} \mathbb{F}_{\mathfrak{p}}(\mathcal{D})\right), \tag{4.4.1}$$

where the map to $\mathbb{F}_{\mathfrak{p}}(\mathcal{D})$ is given as follows. The order of vanishing along $\mathcal{D}$ gives rise to a discrete valuation, v_d, on $\mathbb{F}_{\mathfrak{p}}(\mathcal{D})$. The component for $\mathcal{D}$ of the map T is given by the corresponding tame symbol

$$T_{\mathcal{D}} : \{a, b\} \mapsto (-1)^{v_{\mathcal{D}}(a)v_{\mathcal{D}}(b)} \frac{a^{v_{\mathcal{D}}(b)}}{b^{v_{\mathcal{D}}(a)}}(\mathcal{D}) . \tag{4.4.2}$$

in analogy with (4.1.2) on page 72. Finally we define

$$\mathrm{K}_2(C, \mathcal{O}_K) = \mathrm{K}_2^T(\mathcal{C})/\text{torsion}.$$

Remark 4.4.2 ([19] p. 344)**.**

- The group $\mathrm{K}_2(C, \mathcal{O}_K)$ is a subgroup of $\mathrm{K}_2^T(C)$/torsion.
- The defined group is independent of the regular proper model $\mathcal{C}$ of C. [41, p. 13].

We can now restrict the pairing (4.3.1) of page 75 to

$$\langle\cdot,\cdot\rangle : H_1(X, \mathbb{Z})^- \times \mathrm{K}_2(C, \mathcal{O}_K) \to \mathbb{R}. \tag{4.4.3}$$

Bloch and Grayson [7] refined the Beilinson conjecture in the following way.

Conjecture 4.4.3 ([19] Conjecture 3.11)**.** Let K be a number field of degree $d = [K : \mathbb{Q}]$. Let C be a non-singular, projective, geometrically irreducible curve of genus g defined over K, and let $X = C(\mathbb{C})$. Then:

1. the group $\mathrm{K}_2(C, \mathcal{O}_K)$ is a free abelian group of rank dg and the pairing (4.4.3) is non-degenerate;
2. let R_C denote the absolute value of the determinant of this pairing with respect to $\mathbb{Z}$-bases of $H_1(X, \mathbb{Z})^-$ and $\mathrm{K}_2(C, \mathcal{O}_K)$, and let $\Lambda(C, 0)$ be defined as in Section 3.2; then $\Lambda(C, 0) = Q\,\mathrm{R}_C$ for some non-zero rational number Q.

Remark 4.4.4 ([19] Remark 3.12)**.** The value of $\Lambda(C, 0)$ is not guaranteed by Theorem 3.2.4, but only conjectured by the Hasse-Weil conjectures (Conjecture 2.5.7). These conjectures also hypothesize the functional equation of $\mathrm{L}(C, s)$ and by the functional equation $\Lambda(C, 0)$ is rationally equivalent to $\pi^{-2g}\,\mathrm{L}(C, 2)$. Therefore, the Beilinson conjectures can be formulated using the value $\Lambda(C, 2)$.

Remark 4.4.5 ([19] Remark 3.12)**.** The Beilinson conjectures are difficult to check, even in simple cases, because generating enough elements in $\mathrm{K}_2(C, \mathcal{O}_K)$ is nearly impossible. Not even tensoring with $\mathbb{Q}$ offers any advantage. The only known ways to generate elements are ad hoc measures or explicit versions of Bloch's trick.

Ad hoc measure have been used by Young [54] for elliptic curves over $\mathbb{Q}$ and certain real quadratic number fields. Kimura [26] generated enough elements for the genus two curve $y^2 - y = x^5$ by using ad hoc elements of a corresponding Fermat curve. Otsubo [36] uses one ad hoc element found by Ross [40] and the projection into certain motivic subspaces.

Dokchitser, de Jeu and Zagier used an explicit version of Bloch's trick that we also explain and use in this thesis.

For superelliptic curves, as investigated in this thesis, the situation becomes even more intractable. Using the same methods as [19] yields only enough elements to numerically check the Beilinson conjecture in one case. It was never possible to find more than enough elements to check for linear dependencies, except for one example, where the Jacobian splits into elliptic and hyperelliptic curves, thus the example reduces to the cases considered in [7] and [19].

5 Towards Beilinsons Conjectures for Superelliptic Curves

After the previous chapters covered the general theory to state the Beilinson conjectures the next chapters contain the theory to check them. This chapter works out concrete examples to check the Beilinson conjecture, which will be worked out in detail in the end of this thesis.

To be able to test Conjecture 4.4.3 we need sufficiently many elements of $\mathrm{K}_2(C, \mathcal{O}_K)$ to calculate the regulator. So, far there does not exist an algorithm to produce enough elements for a general algebraic curve. Beilinson himself produced elements for modular curves that have their support in the cusps of that curve. These elements where enough to determine the regulator and allowed him to prove his conjecture for modular curves.

Otherwise there are only ad hoc methods that use a more or less explicit version of Bloch's trick, which we explain in this chapter. Otsubo [36] uses one ad hoc element found by Ross [40] for Fermat curves and certain motivic subspaces. He shows that the projections of this elements in these subspaces are again elements of $\mathrm{K}_2(C)$ for the Fermat curves. This gives him enough elements to prove the Beilinson conjectures for the Fermat curve X_N if $N = 3, 4, 5, 6, 7$. That leaves us with the question of how we can construct elements that are in $\mathrm{K}_2^T(C)$, that is, such the tame symbol at every point of C is trivial?

We follow [19] in the construction of elements from torsion points on the Jacobian. Since they state everything only for hyperelliptic curves over $\mathbb{Q}$, but we need it for superelliptic curves over general number fields, we generalize everything to superelliptic curves over an arbitrary number field K. Thus, the constructions, lemmas and propositions of the first two sections of this chapter are taken directly from [19] and the author has only adapted them to the new setting. The corresponding source in [19] is noted for each statement quoted. Since this does not change the proofs in most cases we only work out the proofs of statements where something different happens and refer to [19] in most cases. The proofs, which are worked out in this thesis, are the work of the author. Some work has been done independently by Liu and Tang in the short exposition [29]. Their work states and proves Proposition 5.2.4 and a special case of Theorem 5.4.1. For simplicity we refer to [29] for the proof of Proposition 5.2.4, because no new insight can be gained by the full exposition of this proof.

In this chapter a curve is a non-singular, projective, geometrically irreducible curve over a number field.

5.1 Torsion Divisors on Superelliptic Curves

This section follows [19] chapter 5, and makes the obvious generalizations to superelliptic curves. The work has been done independently in [29] beginning of chapter 3.

Notation 5.1.1. Let K be a number field. We now consider a superelliptic curve C/K, that is a curve

$$y^m = t(x) = c_n x^n + c_{n-1}x^{n-1} + \ldots + n_1 x + c_0, \qquad c_n \neq 0,\ m,n \geqslant 3,\ (m,n) = 1, \quad (5.1.1)$$

where the polynomial $t(x)$ has coefficients in K and no multiple roots. This equation can be seen in two ways. On the one hand it defines an m-cover of $\mathbb{P}^1$ and on the other hand is defines a singular curve in $\mathbb{P}^2$ whose normalization is C. In the normalization there exists exactly one point $\infty = \infty_C$ at infinity. The m-cover ϕ is defined as follows:

$$\phi : C \to \mathbb{P}^1, \quad (x,y) \to x.$$

The ramification points of ϕ are given by the point at infinity and the roots of $t(x)$.

If we want to use Construction 4.2.1 to generate elements of $\mathrm{K}_2^T(C)$ it is necessary to have a source of points P and Q such that $(P) - (Q)$ is a torsion divisor. To simplify the search for such points Dokchitser, de Jeu and Zagier use the following notation.

Notation 5.1.2 ([19] p. 349)**.** Let $c \in \mathbb{N}$ be a positive integer. An (c-)torsion point is a point $P \in C$ such that the divisor $(P) - (\infty)$ is an c-torsion divisor.

If we have two torsion points P and Q, then obviously $(P) - (Q)$ is a torsion divisor and thus, we can use P and Q to generate an element of $\mathrm{K}_2^T(C)$ using Construction 4.2.1.

Our goal is to construct many torsion points P_i such that we get enough elements $\{\infty, P_i, P_j\} \in \mathrm{K}_2^T(C)$ by using Proposition 4.2.3 1.

The first set of torsion points can be constructed directly from the equation (5.1.1)

Example 5.1.3 ([19] Example 5.2)**.** Using the same notation as before, any non-trivial difference $(P) - (Q)$ for P and Q among ∞ and T_α is m-torsion:

$$m(T_\alpha) - m(T_\beta) = \operatorname{div}\left(\frac{x-\alpha}{x-\beta}\right), \qquad m(T_\alpha) - m(\infty) = \operatorname{div}(x-\alpha)\,.$$

So the T_α are m-torsion points, though not necessarily defined over $\mathbb{Q}$.

As in [19] the calculation

$$\left\{\frac{x-\beta}{\alpha-\beta}, \frac{\beta-\alpha}{x-\alpha}\right\} = \left\{\frac{x-\alpha}{\beta-\alpha}, \frac{x-\beta}{\alpha-\beta}\right\} = \left\{\frac{x-\alpha}{\beta-\alpha}, 1 - \frac{x-\alpha}{\beta-\alpha}\right\} = 0 \qquad (5.1.2)$$

shows that m-torsion points alone are not sufficient to construct non-trivial elements of $\mathrm{K}_2^T(C)$.

The big problem is how one can find more torsion points on C. We can use a similar trick as in examples 5.3 and 5.6 [19] to produce n-torsion points if we make more assumptions on the equation of C.

Example 5.1.4 (n-torsion)**.** We assume that the equation of the superelliptic curve (5.1.1) has the form

$$y^m = t(x) = c_n x^n + (b_r x^r + b_{r-1}x^{r-1} + \cdots + b_1 x + b_0)^m = c_n x^n + f(x)^n \qquad (5.1.3)$$

where $rm < n$ and $c_n \neq 0$. The substitution $y \mapsto y + \sum b_i x^i$ transforms this equation to

$$y^m + \sum_{i=1}^{m-1} \binom{m}{i} (b_n x^n + \ldots + b_1 x + b_0)^i y^{m-i} = \prod_{i=1}^{m} (y - \pi_i f(x)) = cx^n, \qquad (5.1.4)$$

where $\pi_i = \zeta_m^i - 1$ and ζ_m a primitive m-th root of unity. The points $\{\mathcal{O}_i\}_{0 \leqslant i < m} = \{(0, \pi_i b_0)\}_{0 \leqslant i < m}$ (corresponding to $(0, \zeta_m^i b_0)$ on the curve (5.1.3)) lie on this curve and the functions $y - \pi_i f(x)$ have divisor $n\,((0, \pi_i)) - n(\infty)$. So the points $\{(0, \pi_i b_0)\}_{0 \leqslant i < m}$ are n-torsion points, but except $\mathcal{O}_0 = (0, 0)$ they are not defined over $\mathbb{Q}$.

These n-torsion points allow us to construct elements of $\mathrm{K}_2^T(C)$ using Proposition 4.2.3 1 either by pairing n-torsion points or pairing n- and m-torsion points.

5.2 Distinguished Elements of K_2 for Superelliptic Curves

In this section we construct explicit elements for a superelliptic curve and study the linear dependencies between different elements. The section follows [19] chapter 6 and makes the necessary generalization to superelliptic curves. Especially the proof of Proposition 5.2.6 requires new insights. Furthermore, the author was even able to prove a new relation for $\mathrm{K}_2^T(C)$ in Proposition 5.2.6. The proof of Proposition 5.2.4 has been done independently from Liu and Tang [29] and the author.

Following Example 5.1.4 we consider curves that have the form

$$\prod_{i=1}^{m} (y - \pi_i f(x)) = cx^n \qquad (5.2.1)$$

with $c \neq 0$, $m \geqslant 3$, $(m, n) = 1$, and $\deg(f)m < n$ in such way that the m-torsion polynomial $t(x) = cx^n + f(x)^n$ has no multiples zeroes. By Section 4.2 we get one element $\{\infty, P_i, P_j\}$ for each pair of torsion points P_i, P_j.

In this section we keep the notation of Example 5.1.3 and Example 5.1.4, that is

$$T_\alpha = (\alpha, f(\alpha)) \text{ and } \mathcal{O}_i = (0, \pi_i f(0))$$

where $\pi_i = \zeta_m^i - 1$ and ζ_m is a primitive m-th root of unity.

Theorem 5.2.1. Let L be a field that contains all m-th roots of unity and all zeroes of the polynomial $t(x)$. The possible distinguished elements of $\mathrm{K}_2^T(C_{\overline{\mathbb{Q}}})$ are given by

1. $$\{\infty, T_\alpha, T_\beta\} = 0.$$
   That is, if two m-torsion points get paired, the resulting element vanishes.
2. $$\{\infty, \mathcal{O}_i, T_\alpha\} = \left\{ \frac{y - \pi_i f(x)}{-f(\alpha)}, \frac{x-\alpha}{-\alpha} \right\}.$$
3. $$\{\infty, \mathcal{O}_i, \mathcal{O}_j\} = c_{i,j} \left(\frac{y - \pi_i f(x)}{\pi_j f(0) - \pi_i f(0)}, \frac{y - \pi_j f(x)}{\pi_i f(0) - \pi_j f(0)} \right).$$

Proof. The calculation (5.1.2) proves part 1. The theorem follows directly from 4.2.3, Part 1. The only part left to prove is to determine the order of the divisors $(T_\alpha) - (T_\beta)$, $(\mathcal{O}_i) - (T_\alpha)$ and $(\mathcal{O}_i) - (\mathcal{O}_j)$. Since $(m, n) = 1$, the order of $(\mathcal{O}_i) - (T_\alpha)$ has to be mn, but the order of $(T_\alpha) - (T_\beta)$ or $(\mathcal{O}_i) - (\mathcal{O}_j)$ can be any divisor of m or n, respectively. Therefore we set $c_{i,j} = \frac{n}{\mathrm{ord}((\mathcal{O}_i)-(\mathcal{O}_j))}$, which proves the theorem.

□

Theorem 5.2.1 only gives explicit elements if the field L contains all m-th roots of unity and a zero of the polynomial $t(x)$.

This might not be the case in most circumstances. But even if not all roots are rational we can still construct one element in $\mathrm{K}_2^T(C)$ for each rational factor.

Theorem 5.2.2. Let C/K be a superelliptic curve of the form (5.2.1) on page 83. For each irreducible factor $u(x)$ of $t(x)$ and $w(x)$ of $(x + 1)^m - 1$ over K there exists an element

$$\left\{ \frac{\left(w\left(\frac{y}{f(x)}\right) f(x)^{\deg(w(x))} \right)^m}{cx^n}, \frac{u(x)}{u(0)} \right\} \in \mathrm{K}_2^T(C).$$

Proof. To prove the theorem we have to use some of the relations in $\mathrm{K}_2^T(C)$ to be able to combine the added elements. From now on we always write elements in $\mathrm{K}_2^T(C_{\overline{\mathbb{Q}}})$ for their classes in $\mathrm{K}_2^T(C_{\overline{\mathbb{Q}}})$/torsion. Let

$$\begin{aligned}
M &= \sum_{\substack{u(\alpha)=0 \\ w(\pi_i)=0}} m\{\infty, \mathcal{O}_i, T_\alpha\} \\
&= \sum_{\substack{u(\alpha)=0 \\ w(\pi_i)=0}} m \left\{ \frac{y - \pi_i f(x)}{-f(\alpha)}, \frac{x-\alpha}{-\alpha} \right\} \\
&= \sum_{\substack{u(\alpha)=0 \\ w(\pi_i)=0}} \left\{ \frac{(y - \pi_i f(x))^m}{(-f(\alpha))^m}, \frac{x-\alpha}{-\alpha} \right\}.
\end{aligned}$$

By the definition of the curve, we have $f(\alpha)^m = c\alpha^n$, so

$$
\begin{aligned}
&= \sum_{\substack{u(\alpha)=0\\ w(\pi_i)=0}} \left\{ \frac{(y-\pi_i f(x))^m}{c\alpha^n}, \frac{x-\alpha}{-\alpha} \right\} \\
&= \sum_{\substack{u(\alpha)=0\\ w(\pi_i)=0}} \left\{ \frac{(y-\pi_i f(x))^m}{c\alpha^n}, \frac{x-\alpha}{-\alpha} \right\} - n\left\{ \frac{x}{\alpha}, 1-\frac{x}{\alpha} \right\} \\
&= \sum_{\substack{u(\alpha)=0\\ w(\pi_i)=0}} \left\{ \frac{(y-\pi_i f(x))^m}{cx^n}, \frac{x-\alpha}{-\alpha} \right\}.
\end{aligned}
$$

This is the most important step, because now it is possible to simplify the sum into one element.

$$
\begin{aligned}
&= \sum_{w(\pi_i)=0} \left\{ \frac{(y-\pi_i f(x))^m}{cx^n}, \frac{u(x)}{u(0)} \right\} \\
&= \left\{ \frac{\prod_{w(\pi_i)=0}(y-\pi_i f(x))^m}{cx^n}, \frac{u(x)}{u(0)} \right\} \\
&= \left\{ \frac{\left(w\left(\frac{y}{f(x)}\right) f(x)^{\deg(w(x))} \right)^m}{cx^n}, \frac{u(x)}{u(0)} \right\} \in \mathrm{K}_2^T(C).
\end{aligned}
$$

$\square$

Construction 5.2.3. Let C/K be given by (5.2.1). Let $u_1, \ldots, u_\ell$ be the irreducible factors in $K[x]$ (up to multiplication by K^*) of the m-torsion polynomial $t(x) = cx^n + f(x)^m$ and let $w_1, \ldots, w_k$ be the irreducible factors (up to multiplication by K^*) of the polynomial $(x+1)^m - 1$. To each of them we can associate an element of $\mathrm{K}_2^T(C)/\text{torsion}$ by Theorem 5.2.2,

$$
M_{ij} = \text{ class of } \left\{ \frac{\left(w_i\left(\frac{y}{f(x)}\right) f(x)^{\deg(w_i(x))} \right)^m}{cx^n}, \frac{u_j(x)}{u_j(0)} \right\} \quad 1 \leqslant i \leqslant k,\ 1 \leqslant j \leqslant \ell.
$$

Extension by linearity gives a map

$$
\begin{aligned}
\mathbb{Z}^k \times \mathbb{Z}^\ell &\longrightarrow \mathrm{K}_2^{\mathrm{T}}(\mathrm{C}, \mathrm{K})/\text{torsion} \\
(n_1, \ldots, n_k, m_1, \ldots, m_\ell) &\longmapsto \sum_{i,j} n_i m_j M_{i,j}
\end{aligned}
$$

In addition to the symmetric properties, the tetrahedron relation of Proposition 4.2.3 and the vanishing of m-torsion elements of Theorem 5.2.1 the elements satisfy the following relations:

Proposition 5.2.4. The constructed elements satisfy the relation

$$\sum_i \{\infty, \mathcal{O}_i, T_\alpha\} = 0 \quad \text{for any linear factor } \alpha \text{ of } t(x).$$

Furthermore, for any fixed i there exists a non-trivial linear relation of the elements $\{\infty, \mathcal{O}_i, \mathcal{O}_j\}$ and $\{\infty, \mathcal{O}_i, T_\alpha\}$, where $0 \leqslant j < m$ and $0 \leqslant \alpha < n$.

Proof. The proof is analogous to the proof of Proposition 6.3 in [19]. The proof has been written down by Liu/Tang in [29]. □

Remark 5.2.5. If we set $c_{ij} = n$ in Theorem 5.2.1 part 3, then

$$\{\infty, \mathcal{O}_i, \mathcal{O}_j\}^* = n\left(\frac{y - \pi_i f(x)}{\pi_j f(0) - \pi_i f(0)}, \frac{y - \pi_j f(x)}{\pi_i f(0) - \pi_j f(0)}\right).$$

This is in general a multiple of the element $\{\infty, \mathcal{O}_i, \mathcal{O}_j\}$. Then, the linear relation of Proposition 5.2.4 takes the form

$$\sum_j m\{\infty, \mathcal{O}_i, \mathcal{O}_j\}^* = \sum_\alpha n\{\infty, \mathcal{O}_i, T_\alpha\}.$$

If $m = 3$, Proposition 5.2.4 can be extended to the following proposition.

Proposition 5.2.6. Let $m = 3$, ζ_3 a primitive cube root of unity, $\mathbb{Q}[\zeta_3] \subset K$ and V be the $\mathbb{Q}$-subspace of $\mathrm{K}_2^T(C)$ generated by the elements of the form $\{P_i, P_j, P_k\}$ where P_i, P_j and P_k run through the points $\infty, \mathcal{O}_i$ and T_α. Then V is already generated by the elements of the form $\{\infty, \mathcal{O}_i, T_\alpha\}$ for $0 \leqslant i < 2$ and $\alpha \in \overline{\mathbb{Q}}$ a root of $t(x)$. More precisely, the elements $\{\infty, \mathcal{O}_i, \mathcal{O}_j\}$ satisfy the additional relation

$$\{\infty, \mathcal{O}_0, \mathcal{O}_1\} + \{\infty, \mathcal{O}_1, \mathcal{O}_2\} + \{\infty, \mathcal{O}_2, \mathcal{O}_0\} = 0.$$

Proof. Let $m = 3$. By the tetrahedron relation of Proposition 4.2.3 Part 3, we have

$$n(\{\infty, \mathcal{O}_0, \mathcal{O}_1\} + \{\infty, \mathcal{O}_1, \mathcal{O}_2\} + \{\infty, \mathcal{O}_2, \mathcal{O}_0\} - \{\mathcal{O}_0, \mathcal{O}_1, \mathcal{O}_2\}) = 0$$

where n is the order of any $(\mathcal{O}_i) - (\mathcal{O}_j)$. Therefore, it is enough to show that the element

$$\{\mathcal{O}_0, \mathcal{O}_1, \mathcal{O}_2\} = \left\{\frac{y - \pi_1 f(x)}{\pi_2 f(0) - \pi_1 f(0)}, \frac{y - \pi_2 f(x)}{\pi_1 f(0) - \pi_2 f(0)}\right\} = 0.$$

The most important fact is that

$$(\zeta_3 + 1)(y - \pi_2 f(x)) = y + \zeta_3(y - \pi_1 f(x)).$$

Indeed,

$$(\zeta_3 + 1)(y - \pi_2 f(x)) = \zeta_3 y + y - (\zeta_3 - 1 + 1 - \zeta_3^2) f(x) = y + \zeta_3(y - \pi_1 f(x)).$$

It follows that

$$\begin{aligned}
\{\mathcal{O}_0, \mathcal{O}_1, \mathcal{O}_2\} &= \left\{ \frac{y}{(\zeta_3+1)f(0)(y-\pi_2 f(x))}, \frac{y-\pi_1 f(x)}{-\zeta_3 f(0)(y-\pi_2 f(x))} \right\} \\
&= \left\{ \frac{y}{(\zeta_3+1)f(0)(y-\pi_2 f(x))}, \frac{\zeta_3(y-\pi_1 f(x))}{(\zeta_3+1)f(0)(y-\pi_2 f(x))} \right\} \\
&= \left\{ \frac{y}{(\zeta_3+1)f(0)(y-\pi_2 f(x))}, \frac{y+\zeta_3(y-\pi_1 f(x))-y}{(\zeta_3+1)f(0)(y-\pi_2 f(x))} \right\} \\
&= \left\{ \frac{y}{(\zeta_3+1)f(0)(y-\pi_2 f(x))}, \frac{(\zeta_3+1)(y-\pi_2 f(x))-y}{(\zeta_3+1)f(0)(y-\pi_2 f(x))} \right\} \\
&= \left\{ \frac{y}{(\zeta_3+1)(y-\pi_2 f(x))}, 1-\frac{y}{(\zeta_3+1)(y-\pi_2 f(x))} \right\} = 0.
\end{aligned}$$

To finish the proof we have to show that any element of the form $\{\infty, \mathcal{O}_i, \mathcal{O}_j\}$ can be expressed in terms of an element of the form $\{\infty, \mathcal{O}_i, T_\alpha\}$ for $0 \leqslant i < 2$ and $\alpha \in \overline{\mathbb{Q}}$ a root of $t(x)$. The relations of Proposition 5.2.4 give $n+2$ independent relations. Together with the relation of this proposition there exist $n+3$ independent relations, such that the vector space generated by all $3n+3$ elements is already generated by the $2q$ given elements. $\square$

Remark 5.2.7. Over an extension L of K there always exist the elements $\{\infty, \mathcal{O}_i, \mathcal{O}_j\}$. These elements seem to be a good addition to the elements of Construction 5.2.3, but the last relations state that for the case $m = 3$ these elements are always linearly dependent on the elements of Construction 5.2.3. In Section 5.3 we call m-torsion polynomials "good", if they factor into "enoug" factors, such that using the construction above yields enough elements with no known linear relation, such that it is reasonable to check the Beilinson conjectures numerically. It turns out (Theorem 5.3.1) that only in the case $m = 3$ good polynomials can be found. For that reason the elements $\{\infty, \mathcal{O}_i, \mathcal{O}_j\}$ are not interesting for our studies.

5.3 Constructing Good Polynomials

Let m and n be positive integers relatively prime to each other. Let K be a number field of degree d. The superelliptic curve over K defined by

$$C : y^m = \sum_{i=0}^{n} a_i x^i = t(x)$$

with $a_n \neq 0$ has genus $g = g(C) = \frac{1}{2}(m-1)(n-1)$.

The goal is to use Construction 4.2.1 to produce examples of superelliptic curves C with as many distinguished elements of $\mathrm{K}_2^T(C)$ as possible. For C to have enough elements to check the Beilinson conjectures it needs at least gd elements.

Therefore, we want to construct polynomials of the form

$$t(x) = cx^n + (\sum_{i=0}^{l} a_i x^i)^m$$

with $c \neq 0$ and $lm \leqslant n$, such that $t(x)$ has enough factors over K. We refer to polynomials of this form, with enough factors over K, such that we can check Beilinson conjectures, as “good” polynomials.

Dokchitser, De Jeu and Zagier [19] found multiple classes of good examples for hyperelliptic curves over $\mathbb{Q}$. The following theorem states that for general superelliptic curves using Construction 4.2.1 there are only a few examples where it is possible to find enough elements in $\mathrm{K}_2^T(C)$ to check the Beilinson conjectures.

In order to find a curve whose Jacobian does not have a factor which comes from a hyperelliptic curve, we need to choose m to be odd. Since for any $m = m_1 m_2$ the Jacobian has a factor that comes from a superelliptic curve of the form

$$C_1 : y^{m_1} = t(x).$$

We thus restrict our self to m prime and for better understanding we write p instead of m in the following.

Theorem 5.3.1. Let C be a superelliptic curve over K

$$C : y^p = \sum_{i=0}^{n} a_i x^i = t(x)$$

with p an odd prime, $n \geqslant 3$ and $(p, n) = 1$. Using Construction 4.2.1 it is only possible to find good polynomials if $p = 3$ and $K = \mathbb{Q}$ or $K = \mathbb{Q}[\zeta_3]$, where ζ_3 is a primitive third root of unity. Furthermore, in both cases there need to be at least $n - 1$ linear factors.

Proof. Let k be the number of rational factors of $t(x)$ in K. We prove the theorem by checking different classes of conditions:

1. Let $p = 3$ and $K = \mathbb{Q}$. Then $d = 1$. Since the polynomial $(x + 1)^3 - 1$ only has two rational factors, the Construction 4.2.1 gives k elements. To be able to check the Beilinson conjectures there need to be at least $g(C) = (n - 1)$ elements. To get enough elements in $\mathrm{K}_2^T(C)$ it is necessary that there are at least $n - 1$ factors of the polynomial $t(x)$, i.e. there can be at most one factor of degree 2.
2. Let $p = 3$ and $K = \mathbb{Q}[\zeta_3]$. Then $d = 2$. Since the polynomial $(x + 1)^3 - 1$ splits, it has three factors and the Construction 4.2.1 gives $2k$ elements. To be able to check the Beilinson conjectures there need to be at least $dg(C) = 2(n - 1)$ elements. To get enough elements in $\mathrm{K}_2^T(C)$ it is necessary that there are at least $n - 1$ factors of the polynomial $t(x)$.

3. Let $p = 3$ and $d = 2$, but $K \not\supseteq \mathbb{Q}[\zeta_3]$. Since the polynomial $(x+1)^3 - 1$ does not split, there are only two factors and the Construction 4.2.1 gives k elements. To be able to check the Beilinson conjectures there would need to be at least $dg(C) = 2(n-1)$ elements. To get enough elements in $\mathrm{K}_2^T(C)$ it would be necessary to have at least $2(n-1)$ factors of $t(x)$, which is impossible since $2(n-1)$ is bigger than the degree of $t(x)$.
4. Let $p = 3$ and $d > 2$. Even if the polynomial $(x+1)^3 - 1$ splits, Construction 4.2.1 gives at most $2k$ elements. To be able to check the Beilinson conjectures, there would need to be at least $dg(C) = d(n-1)$ elements. To get enough elements in $\mathrm{K}_2^T(C)$ it would be necessary to have at least $d/2(n-1)$ factors of $t(x)$, which is impossible since $d/2(n-1)$ is bigger than the degree of $t(x)$.
5. Let $p \geqslant 5$ and $d < p-1$. Since the polynomial $(x+1)^3 - 1$ splits into at most $d+1$ factors, the Construction 4.2.1 gives dk elements. To be able to check the Beilinson conjectures there would need to be at least $dg(C) = d\frac{(p-1)(n-1)}{2} > 2d(n-1)$ elements. To get enough elements in $\mathrm{K}_2^T(C)$ it would be necessary to have at least $2(n-1)$ factors of $t(x)$, which is impossible since $2(n-1)$ is bigger than the degree of $t(x)$.
6. Let $p \geqslant 5$ and $d \leqslant p-1$. Even if the polynomial $(x+1)^3 - 1$ splits, Construction 4.2.1 gives at most $(p-1)k$ elements. To be able to check the Beilinson conjectures there would need to be at least $dg(C) = \frac{d(p-1)(n-1)}{2} > 2(p-1)(n-1)$ elements. To get enough elements in $\mathrm{K}_2^T(C)$ it would be necessary to have at least $2(n-1)$ factors of $t(x)$, which is impossible since $2(n-1)$ is bigger than the degree of $t(x)$.

$\square$

Theorem 5.3.1 reduces our options to find good curves using Construction 4.2.1. The problem comes down to not having enough variables to force the polynomial $t(x)$ to have enough factors. We give two classes of examples, one over $\mathbb{Q}$ and one over $\mathbb{Q}[\zeta_3]$.

Proposition 5.3.2. Let $a_1, a_2 \in \mathbb{Q}$ be two rational numbers that are not equal. Let $b = b_1 + b_2 i \in \mathbb{C}$ with

$$b_1 = -\frac{1}{2}(a_1 + a_2) \text{ and } b_2 = \sqrt{\frac{1}{2}(a_1^2 + a_2^2 + 2b_1^2)}.$$

The curve

$$C_{a_1,a_2}: \quad y^3 = x^4 + (-(a_1^{-1} + a_2^{-1} + b^{-1} + \bar{b}^{-1})x + (a_1 a_2 b\bar{b})^{-1})^3$$

is rational over $\mathbb{Q}$ and Construction 5.2.3 yields six elements in $\mathrm{K}_2^T(C)$.

Proof. Let K be any field and $t(x) = x^4 + (c_1 x + c_0)^3 \in K[x]$. Every root of $t(x)$ in K is of the form r^3 for some $r \in \overline{K}$, so if $t(x)$ factors completely over K it is necessary that

$$t(x) = x^4 + (c_1 x + c_0)^3 = \prod_{i=1}^{4}(x - r_i^3), \;\; r_i \in K.$$

Assume that the r_i^3 are pairwise distinct and non-zero (otherwise $t(x)$ has a double root). Since all roots are of the form r^3 we can look at the polynomial $t(x^3)$. The two formulas for $t(x)$ give two factorizations of $t(x^3)$, and hence

$$(x^4+c_1x^3+c_0)(x^4+\zeta_3(c_1x^3+c_0))(x^4+\zeta_3^2(c_1x^3+c_0)) = \prod_{i=1}^4(x-r_i^3)\prod_{i=1}^4(x-\zeta_3 r_i^3)\prod_{i=1}^4(x-\zeta_3^2 r_i^3).$$

Call the three factors $q(x), \zeta_3 q(\zeta_3^2 x)$ and $\zeta_3^2 q(\zeta_3 x)$ respectively. Clearly in every triple $\zeta_3^\ell r_i,\ i \in \{1,2,3\}$ one of the numbers is a root of $q(x)$ and the others are a root of the other two polynomials. By changing the factor of some of the r_i, if necessary, we can assume that all of them are roots of $q(x)$. The polynomial $q(x)$ has no linear or quadratic term. Newton's formulas imply that the numbers $s_i = r_i^{-1}$ satisfy the two relations

$$\sum_{i=1}^4 s_i = 0 \text{ and } \sum_{i=1}^4 s_i^2 = 0. \tag{5.3.1}$$

Conversely, any 4-tuple $\{s_i\}$ of non-zero K-rationals satisfying the equation above, such that $s_i \neq \zeta_3^\ell s_j$ for any $i \neq j$ and $\ell \in \{0,1,2\}$ give rise to $t(x) = \prod(x - s_i^{-3})$ of the desired form.

The equations above are impossible to satisfy in $\mathbb{Q}$ due to the fact that all squares are positive. However, since it is possible to have one rational factor of degree 2 we can look for matches in an imaginary quadratic number field.

By taking any two different rational numbers a_1 and a_2, we define a complex number $b = b_1 + ib_2$ with $b \in L$, where L is an imaginary quadratic number field, by setting

$$b_1 = -\frac{1}{2}(a_1 + a_2) \text{ and } b_2 = \sqrt{\frac{1}{2}(a_1^2 + a_2^2 + 2b_1^2)}.$$

The numbers a_1, a_2, b and $\bar{b}$ satisfy the relations (5.3.1) and thus give rise to the curve

$$\begin{aligned} y^3 &= (x - a_1^{-3})(x - a_2^{-3})(x - b^{-3})(x - \bar{b}^{-3}) \\ &= (x - a_1^{-3})(x - a_2^{-3})(x^2 - (b^{-3} + \bar{b}^{-3})x + (b\bar{b})^{-3}) \\ &= x^4 + (-(a_1^{-1} + a_2^{-1} + b^{-1} + \bar{b}^{-1}) + (a_1a_2b\bar{b})^{-1})^3. \end{aligned}$$

The coefficients are given by

$$c_1 = -(a_1^{-1} + a_2^{-1} + b^{-1} + \bar{b}^{-1}) \text{ and } c_0 = (a_1a_2b\bar{b})^{-1}.$$

So, for any two numbers $a_1, a_2 \in \mathbb{Q}$, such that $a_1 \neq a_2$, we get a polynomial $t(x)$ that factors over $\mathbb{Q}$ in three factors, such that by Construction 5.2.3 we get six elements in $\mathrm{K}_2^T(C_{a_1,a_2})$.

$\square$

Remark 5.3.3. Proposition 5.3.2 guarantees that there exist six elements in $\mathrm{K}_2^T(C)$. This sounds more than enough to test the Beilinson conjecture, but by the relations of Proposition 5.2.4 and Proposition 5.2.6, at most three of these elements are linearly independent. This is the minimal number of elements needed to test the Beilinson conjecture.

Remark 5.3.4. Since we are interested in curves with integer coefficients, we take the least common denominator $c = \mathrm{lcd}(c_0, c_1)$ of c_0 and c_1 and use the transformation $x \mapsto cx$. This leads to the new equations of the curve C_{a_1,a_2}:

$$C_{a_1,a_2}: \quad y^3 = c'x^4 + (c_1'x + c_0'),$$

where $c' = c^3$, $c_1' = c_1 c$ and $c_0' = c_0 c$. Now c', c_1' and c_0' are integers.

We give two concrete examples, that we will look at later.

Example 5.3.5.

1. Let $a_1 = 1$ and $a_2 = -1$. Thus, $b = i$ and $c' = 1, c_1' = 0$ and $c_0' = -1$. Therefore,

$$t(x) = (x-1)(x+1)(x-i)(x+i) = x^4 - 1$$

   and

$$C_{1,-1}: \quad y^3 = x^4 - 1.$$

2. Let $a_1 = 1$ and $a_2 = 3$. Thus, $b = (-2+3i)$ and $c' = 39^3, c_1' = -40$ and $c_0' = 1$. Therefore,

$$\begin{aligned} t(x) &= 59319(x-1)(x-3^{-3})(x-(-2-3i)^{-3})(x-(-2+3i)^{-3}) \\ &= 59319x^4 + (-40x+1)^3 \end{aligned}$$

   and

$$C_{1,3}: y^3 = 59319x^4 + (-40x+1)^3.$$

Remark 5.3.6. To find new examples for the Beilinson conjectures it is necessary that the Jacobians of the treated curves are absolutely irreducible. The Jacobian of example 1. is known to split into three elliptic CM curves over $\mathbb{Q}(\sqrt{3})$ [27, Proposition 5.1]. The Jacobian of example 2. has not been studied in such detail. All we know is that the Jacobian of the curve is irreducible over $\mathbb{Q}$, because the characteristic polynomial of the Frobenius at $p = 37$ (see Table 3.12.6) is irreducible over $\mathbb{Q}$.

Proposition 5.3.7. Let $K = \mathbb{Q}(\zeta_3)$, where ζ_3 is a primitive third root of unity. Let $a_1, a_2 \in K$ such that $a_1(1-\zeta_3) \neq a_2$. Let

$$c_1 = -(a_1 + (1-\zeta_3)a_2) \text{ and } c_0 = a_1 a_2.$$

The curve

$$C: \quad y^3 = -x^6 + (x^2 + c_1 x + c_0)^3$$

is rational over K and Construction 5.2.3 yields twelve elements in $\mathrm{K}_2^T(C)$.

Proof. Let $K = \mathbb{Q}[\zeta_3]$ and

$$t(x) = -x^6 + (x^2 + c_1 x + c_0)^3.$$

The polynomial factors over K as

$$t(x) = -x^6 + (x^2 + c_1 x + c_0)^3 = (c_1 x + c_0)((1 - \zeta_3)x^2 + c_1 x + c_0)((1 - \zeta_3^2)x^2 + c_1 x + c_0).$$

So, $t(x)$ has at least three rational factors. We can now choose c_1 and c_0 in such a way that at least one of the factors of degree two splits over K.

Let $a_1, a_2 \in K$ such that $a_1(1 - \zeta_3) \neq a_2$. If we set

$$\begin{aligned} c_1 &= -((1 - \zeta_3)a_1 + a_2), \text{ and} \\ c_0 &= a_1 a_2, \end{aligned}$$

then

$$(x - a_1)((1 - \zeta_3)x - a_2) = (1 - \zeta_3)x^2 + c_1 x + c_0.$$

So, for any two elements $a_1, a_2 \in K$, such that $a_1(1 - \zeta_3) \neq a_2$, we get a polynomial $t(x)$ that factors over K into at least four factors. By Construction 5.2.3 we get at least eight elements into $\mathrm{K}_2^{\mathrm{T}}(\mathrm{C}, \mathrm{K})$.

□

Remark 5.3.8. Proposition 5.3.7 guarantees that there exist twelve elements in $\mathrm{K}_2^T(C)$. This sounds more than enough to test the Beilinson conjecture, but by the relations of Proposition 5.2.4 and Proposition 5.2.6, at most eight of these elements are linearly independent. This is the minimal number of elements needed to test the Beilinson conjecture.

We give two concrete examples that we will look at later.

Example 5.3.9.

1. Let $a_1 = -\zeta_3 - 1$ and $a_2 = \zeta_3$, then $c_0 = 1$ and $c_1 = 2$, therefore,

$$C: \quad y^3 = -x^6 + (x^2 + 2x + 1)^3 = -x^6 + (x + 1)^6.$$

   Furthermore, the other quadratic factor also splits and

$$(1 - \zeta_3^2)x^2 + 2x + 1 = ((-\zeta_3 - 1)x - 1)((1 - \zeta_3^2)x - 1).$$

2. Let $a_1 = a_2 = 1$, then $c_0 = 1$ and $c_1 = -2 + \zeta_3$, therefore,

$$C: y^3 = -x^6 + (x^2 + (-2 + \zeta_3)x + 1)^3.$$

5.4 Integrality of the Elements

Even though Construction 5.2.3 gives us a method to produce elements in $\mathrm{K}_2^T(C)/\text{torsion}$, it is still not possible to compute regulators and test the Beilinson conjectures. This is because the elements in the conjecture need to be integral.

Let p be a prime. Let C be a curve of the form

$$C: \quad y^p + \sum_{i=1}^{p-1} \binom{p}{i} (b_k x^k + \ldots + b_1 x + b_0)^i y^{p-i} = cx^n \tag{5.4.1}$$

with $c \neq 0,\ (p,n) = 1, \deg(f)p < n$, and

$$f(x) = c_k x^k + \ldots + c_0.$$

The p-torsion polynomial is given by the following formula

$$t(x) = -cx^n + (c_k x^k + \ldots + c_0)^p. \tag{5.4.2}$$

$$\tag{5.4.3}$$

Let $u_1, \ldots, u_\ell$ be the irreducible factors in $K[x]$ (up to multiplication by K^*) of the polynomial $(x+1)^p - 1$ and let $w_1, \ldots, w_k$ be the irreducible factors in $K[x]$ (up to multiplication by K^*) of the p-torsion polynomial $t(x) = cx^n + f(x)^p$. By Construction 5.2.3 we get ℓk elements M_{ij} in $K_2^T(C)/\text{torsion}$.

For curves of the form (5.4.1) with $c = 1$, Liu and Tang (cf. [29] chapter 4) proved the integrality of some elements over $\mathbb{Q}$.

We hereby prove the integrality under the necessary conditions for a multiple of all of the elements M_{ij} over any number field K.

Theorem 5.4.1. Let K be a number field. Let C/K be a curve of the form (5.4.1), where c and $b_0, \ldots b_k \in \mathcal{O}_K$ are integers.

The class of M_{ij} in $\mathrm{K}_2^T(C)/\text{torsion}$ is in $\mathrm{K}_2(C, \mathcal{O}_K)$, if $\frac{u_j}{u_j(0)} \equiv 1 \mod \mathfrak{p}$ for all $\mathfrak{p}|c,\ \mathfrak{p} \nmid p$.

Proof. Let $\mathcal{C}/\mathcal{O}_K$ be a regular model of C over K that is constructed by repeatedly blowing up singularities. Such a regular model exists [30, Theorem 3.44]. A constructive algorithm to produce such a regular model is a result of Hironaka, contained in his appendix to [15, pages 102 and 105]. Let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal and $\mathcal{C}_\mathfrak{p}$ the fiber over $\mathfrak{p}$ and $F_\mathfrak{p}$ be the fiber over $\mathfrak{p}$ in the arithmetic surface defined by the equation(5.4.1). Let $\mathcal{D}$ be any irreducible component of $\mathcal{C}_\mathfrak{p}$. Since $\mathcal{C}_\mathfrak{p}$ was constructed by repeatedly blowing up singularities the projection of $\mathcal{D}$ on $F_\mathfrak{p}$ is either an irreducible component of $F_\mathfrak{p}$ or a singular point of $F_\mathfrak{p}$.

We prove the theorem by showing the result for $\mathrm{K}_2^T(C_{\overline{\mathbb{Q}}})$, i.e. that every $M'_{k\ell} \in \mathrm{K}_2^T(C_{\overline{\mathbb{Q}}})$, $1 \leqslant k \leqslant p, \quad 1 \leqslant \ell \leqslant n$ with the given restriction is also an element in $\mathrm{K}_2(C, \mathcal{O}_K)$. The theorem then follows by adding these elements up.

Over $\overline{\mathbb{Q}}$ the left hand side of the curve C can be factored as

$$C: \quad \prod_{i=1}^{p}(y - \pi_i f(x)) = cx^n. \tag{5.4.4}$$

Let the element $M'_{k\ell} = (f_k, g_\ell)$ be given by

$$f_k = \frac{(y - \pi_k f(x))^p}{cx^n} \qquad g_\ell = \frac{u_\ell(x)}{u(0)}.$$

1. Let $\mathfrak{p} \mid p$ and $\mathfrak{p} \mid c$ be a prime ideal and $\mathcal{D}$ be an irreducible component that maps onto an irreducible component D of $F_{\mathfrak{p}}$.

   The functions f_i and g_j do not vanish identically on D and, thus, also not on $\mathcal{D}$. Therefore, $v_{\mathcal{D}}(f_i) = v_{\mathcal{D}}(g_j) = 0$ and $T_{\mathcal{D}}(M_{ij}) = 1$.

2. Let $\mathfrak{p} \nmid pc$ be a prime ideal and $\mathcal{D}$ be an irreducible component that maps onto a singular point of $F_{\mathfrak{p}}$.

   We first look at the point at infinity. Setting $y = \frac{\tilde{y}^n}{\tilde{x}^m}$ and $x = \frac{1}{\tilde{x}^n}$, with $mp - nq = 1$, leads to

   $$\prod_{i=1}^{p}(\tilde{y}^n - \pi_i \tilde{x}^m f(\frac{1}{\tilde{x}^n})) + c\tilde{x} = 0,$$

   which shows that the point at infinity $(\tilde{x}, \tilde{y}) = (0,0)$ is non-singular.

   Let $P = (a, b)$ be a finite singular point. Since $\mathfrak{p} \nmid p$ and

   $$\frac{d}{dy}\prod_{i}(y - \pi_i f(x)) = \frac{d}{dy}((y + f(x))^p - f(x)^p) = p(y + f(x))^{p-1}$$

   it follows that $b + f(a) = 0$ and $b^p = ca^n$. Therefore,

   $$\begin{aligned} f_k(P) &= \frac{(b - \pi_k f(a))^p}{ca^n} \\ &= \frac{(b + \pi_k b)^p}{ca^q n} \\ &= \frac{\left(\zeta_p^k b\right)^p}{ca^n} \\ &= \frac{(b)^p}{ca^n} \\ &= 1 \end{aligned}$$

   implying $T_{\mathcal{D}}(M_{i,j}) = 1$.

3. Let $\mathfrak{p} \mid p$ and $\mathfrak{p} \mid c$ be a prime ideal. We claim that f_i is constant and equal to 1 on $F_\mathfrak{p}$ and, thus, $T_\mathcal{D}(M_{ij}) = 1$ for all $\mathcal{D}$ in $\mathcal{C}_\mathfrak{p}$.

   The fiber $F_\mathfrak{p}$ consists of one component with multiplicity bigger than 1:
$$D : y = 0.$$

   Since
$$\begin{aligned} f_i &= \frac{(y - \pi_i f(x))^p}{cx^d} \\ &= \frac{\prod_{i=1}^p (y - \pi_i f(x)) + \sum_{n=1}^{p-1}(-\binom{p}{n} + (-\pi_i)^n) y^{p-n} f(x)^n + (-\pi_i f(x))^p}{cx^d} \\ &= \frac{\prod_{i=1}^p (y - \pi_i f(x))}{cx^d} + \frac{\sum_{n=1}^{p-1}(-\binom{p}{n} + (-\pi_i)^n) y^{p-n} f(x)^n + (-\pi_i f(x))^p}{cx^d} \\ &= 1 + \frac{\sum_{n=1}^{p-1}(-\binom{p}{n} + (-\pi_i)^n) y^{p-n} f(x)^n + (-\pi_i f(x))^p}{cx^d} \\ &= 1 + \frac{\sum_{n=1}^{p-1}(-\binom{p}{n} + (-\pi_i)^n) y^{p-n} f(x)^n + (-\pi_i f(x))^p}{\prod_{i=1}^p (y - \pi_i f(x))} \end{aligned}$$
   in K and since $\mathfrak{p} \mid \binom{p}{n}$ for all $1 \leqslant n < p$ and $\mathfrak{p} \mid \pi_i$, the function
$$\frac{\sum_{n=1}^{p-1}(-\binom{p}{n} + (-\pi_i)^n) y^{p-n} f(x)^n + (-\pi_i f(x))^p}{\prod_{i=1}^p (y - \pi_i f(x))}$$
   is constant and equal to 0 on all of $\mathbb{P}^2_{\mathbb{F}_\mathfrak{p}}$ and therefore f_i is constant and equal to 1 on every irreducible component D of $F_\mathfrak{p}$, thus $T_\mathcal{D}(M_{ij}) = 1$.
4. Let $\mathfrak{p} \mid p$ but $\mathfrak{p} \nmid c$ and let $\mathcal{D}$ be an irreducible component that maps onto an irreducible component D of $F_\mathfrak{p}$.

   The functions f_i and g_j do not vanish identically on D and, thus, also not on $\mathcal{D}$. Therefore, $v_\mathcal{D}(f_i) = v_\mathcal{D}(g_j) = 0$ and $T_\mathcal{D}(M_{ij}) = 1$.
5. Let $\mathfrak{p} \mid p$ but $\mathfrak{p} \nmid c$, then since $\pi_i = 0$ for all i we have $y_0^p = x_0^n$. Let $\mathcal{D}$ be a component that maps to a singular point of $F_\mathfrak{p}$. Since $y_0^p = x_0^n$ it follows that $T_\mathcal{D}(M_{i,j}) = 1$.
6. Let $\mathfrak{p} \mid c$ and $\mathfrak{p} \nmid p$ be a prime ideal. Since $g_j(x) \equiv 1 \mod \mathfrak{p}$ it follows that $T_\mathcal{D}(M_{ij}) = 1$.

This rounds up all possible cases and hereby proves the theorem. □

5.5 Concrete Examples for the Beilinson Conjectures

This chapter has restricted possible examples of superelliptic curves that are not hyperelliptic to two classes. The first class of examples was presented in Proposition 5.3.2

and the second class in Proposition 5.3.7. We consider both classes of examples in this section and try to find concrete examples to test the Beilinson conjectures. By Theorem 5.4.1 we know that for all elements to be integral it is necessary that either c is a power of 3 or for any additional factor $p \neq 3$ of c all factors of the 3-torsion polynomial need to be constant and equal to 1 modulo p.

We start by studying the integrality of the elements of the curves C_{a_1,a_2} of Proposition 5.3.2.

Let $a_1, a_2 \in \mathbb{Q}$ be two rational numbers that are not equal. Let $b = b_1 + b_2 i \in \mathbb{C}$ with

$$b_1 = -\frac{1}{2}(a_1 + a_2) \text{ and } b_2 = \sqrt{\frac{1}{2}(a_1^2 + a_2^2 + 2b_1^2)}.$$

The curve C_{a_1,a_2} Proposition 5.3.2 is given by

$$\begin{aligned} C_{a_1,a_2}: \quad y^3 &= t(x) = x^4 + (c_1 x + c_0)^3 \\ &= x^4 + (-(a_1^{-1} + a_2^{-1} + b^{-1} + \bar{b}^{-1})x + (a_1 a_2 b \bar{b})^{-1})^3. \end{aligned}$$

Writing c_0 and c_1 in terms of a_1 and a_2 we get

$$\begin{aligned} c_0 &= \left(a_1 a_2 \frac{(a_1+a_2)^2}{4} \frac{3a_1^2 + 2a_1 a_2 + 3a_2^2}{4} \right)^{-1} \\ c_1 &= -c_0 \left(a_2 \left(\frac{(a_1+a_2)^2}{4} + \frac{3a_1^2 + 2a_1 a_2 + 3a_2^2}{4} \right) \right) \\ &\quad - c_0 \left(a_1 \left(\frac{(a_1+a_2)^2}{4} + \frac{3a_1^2 + 2a_1 a_2 + 3a_2^2}{4} \right) \right) \\ &\quad + c_0 \left(a_1 a_2 \left(a_1 + a_2 \right) \right). \end{aligned}$$

We are interested in polynomials $t(x)$ with integer coefficients and constant coefficient 1 (see Remark 5.3.4), because otherwise we have obviously at least one factor that is not integral. For this reason it is necessary that $c_0^{-1} \in \mathbb{Z}$ and $c_0^{-1} c_1 \in \mathbb{Z}$.

For this to be true it is necessary that

$$\begin{aligned} a_1 + a_2 &\in 2\mathbb{Z} \text{ and} \\ 3a_1^2 + 2a_1 a_2 + 3a_2^2 &\in 4\mathbb{Z}. \end{aligned}$$

We assume from now on that these conditions are satisfied and, thus, that $c_0^{-1} \in \mathbb{Z}$ and $c_0^{-1} c_1 \in \mathbb{Z}$. With the transformation $y \mapsto c_0^{-1} y$ we get a new model of the curve, which is given by

$$C_{a_1,a_2}: \quad y^3 = cx^4 + (c_1' x + 1)^3,$$

where $c = c_0^3$ and $c_1' = c_1 c_0$.

We check for integrality in dependence of the fact whether c is a power of 3 or not.

1. Let c be a power of 3. Let a_1^3x-1, a_2^3x-1 and $(b_1^2+b_2^2)^3x^2-2(b_1^3-3b_1b_2^2)x+1$ be the three rational factors of $t(x)$. Since $c=(a_1a_2(b_1^2+b_2^2))^3$, a_1 and a_2 need to be powers of 3. Since $b_1=-\frac{1}{2}(a_1+a_2)$ and $b_2=\pm\sqrt{\frac{1}{2}(a_1^2+a_2^2+2b_1^2)}$, it follows that
$$b_1^2+b_2^2=\frac{1}{4}(a_1+a_2)^2+\frac{1}{2}(a_1^2+a_2^2+\frac{1}{2}(a_1+a_2)^2)=\frac{1}{2}(a_1^2+a_2^2+(a_1+a_2)^2)$$
If a_1 and a_2 are powers of 3, then $\frac{1}{2}(a_1^2+a_2^2+(a_1+a_2)^2)$ can only be a power of 3 if $a_1=\pm a_2$: Let $a_1=3^{e_1}$ and $a_2=\pm 3^{e_2}$ and without restriction $e_1<e_2$. Then $\frac{1}{2}(a_1^2+a_2^2+(a_1+a_2)^2)=3^{2e_1}\frac{1}{2}(1+3^{2e_2-2e_1}+(1+3^{e_2-e_1})^2)$ cannot be a power of 3, because $\frac{1}{2}(1+3^{2e_2-2e_1}+(1\pm 3^{e_2-e_1})^2)$ is congruent 1 modulo 3 and not equal to 1.
   Since a_1 and a_2 cannot be equal, because otherwise the polynomial $t(x)$ would have multiple roots, it follows that $a_1=-a_2$. In this case $b_1=0$ and $b_2=\pm a_1$ and thus
$$t(x)=-a_1^12x^4+1.$$
   Let $v_1=a_1x+1, v_2=a_2x+1$ and $v_3=c^2x^2+1$ and $M_j=\{\frac{y^3}{cx^4},\frac{v_j(x)}{v_j(0)}\}$. We claim that the elements M_j satisfy the additional relation
$$M_1+M_2+M_3=0$$
   and thus there only exist two linear independent elements in $\mathrm{K}_2(C,\mathcal{O}_K)$ and we cannot check the Beilinson conjectures.
   Indeed,
$$\begin{aligned}M_1+M_2+M_3&=\{\frac{y^3}{cx^4},cx^4+1\}\\&=\{y^3,cx^4+1\}-\{cx^4,cx^4+1\}\\&=\{cx^4+1,cx^4+1\}-\{cx^4,cx^4+1\}\\&=0,\end{aligned}$$
   where the elements are zero by the basic relations of the K_2 group.
2. Let $p\neq 3$ be another prime factor of c. For all possible elements to be integral, it is necessary that all irreducible factors of $\frac{t(x)}{t(0)}$ are constant and equal to 1 modulo p.
   Let $C/\mathbb{Q}$ be the curve
$$C:\quad y^3=cx^4+(c_1x+1)^3,$$
   with $c,c_1\in\mathbb{Q}$ and $cc_1\neq 0$. Let $p_1,\dots p_n$ be the prime factors of c except 3. Then the transformation $x\mapsto\prod_{i=1}^n p_ix$ yields the curve
$$C:\quad y^3=c'x^4+(c_1'x+1)^3,$$
   with $c'=\prod_{i=1}^n p_i^4c$ and $c_1'=\prod_{i=1}^n p_ic_1$. This transformation yields a model of the curve such that $c'\equiv c_1'\equiv 0 \mod p_i$ for all $1\leqslant i\leqslant n$.

Let $v_1, \dots, v_3$ be the irreducible factors of the 3-torsion polynomial $t(x) = c'x^4 + (c'_1 x + 1)^3$, then the element M_{ij} is integral because $\frac{v_j(x)}{v_j(0)} = 1$ for all $1 \leqslant j \leqslant n$.

It is therefore reasonable to check Beilinsons conjectures for this class of curves, since a priori no relation is known between those elements.

The previous calculations prove the following theorem:

Theorem 5.5.1. Let $a_1, a_2 \in \mathbb{Z}$ satisfy the relations

$$\begin{aligned} a_1 + a_2 &\in 2\mathbb{Z}, \\ 3a_1^2 + 2a_1a_2 + 3a_2^2 &\in 4\mathbb{Z}, \text{ and} \\ \left(a_1a_2\frac{(a_1+a_2)^2}{4}\frac{3a_1^2+2a_1a_2+3a_2^2}{4}\right) &\neq 3^n \text{ for any } n \in \mathbb{Z}. \end{aligned}$$

For each pair a_1 and a_2 we can construct a curve C_{a_1,a_2} for which we can generate sufficiently enough elements for $\mathrm{K}_2(C, \mathcal{O}_K)$ and for which a priori no relations are known.

The curve is given by the equation

$$C_{a_1,a_2}: \quad y^3 = cx^4 + (c_1x+1)^3,$$

where

$$\begin{aligned} c &= \left(a_1a_2\frac{(a_1+a_2)^2}{4}\frac{3a_1^2+2a_1a_2+3a_2^2}{4}\right)^3 \\ c_1 &= -\left(a_2\left(\frac{(a_1+a_2)^2}{4} + \frac{3a_1^2+2a_1a_2+3a_2^2}{4}\right)\right) \\ &\quad -\left(a_1\left(\frac{(a_1+a_2)^2}{4} + \frac{3a_1^2+2a_1a_2+3a_2^2}{4}\right)\right) \\ &\quad + \left(a_1a_2\left(a_1+a_2\right)\right) \end{aligned}$$

For this class of curves it is therefore reasonable to check the Beilinsons conjectures numerically. □

Remark 5.5.2. This class is not empty. One element of this class is the curve C given by the equation of Example 5.3.5

$$C_{1,3}: \quad y^3 = 59319x^4 + (-40x+1)^3.$$

Remark 5.5.3. For the second class of examples, presented in Example 5.3.9, it is not reasonable to numerically check the Beilinson conjectures.

By Theorem 5.4.1 we get as many possible linear independent elements as twice the number of K-rationals factors ($K = \mathbb{Q}[\zeta_3]$) of the 3-torsion polynomial.

1. Let C/K be the curve

$$C: \quad y^3 = -x^6 + (x^2+2x+1)^3 = -x^6 + (x+1)^6.$$

The 3-torsion polynomial splits into 5 K-rational factors, so there exist 10 elements that do not satisfy any known relation. However, this curve is isomorphic to the curve $y^3 = x^6 - 1$, and is thus a quotient of the Fermat curve $y^6 = x^6 - 1$. Hence, the Jacobian is a product of four elliptic curves with complex multiplication (see [55] example 7.3 and [36] remark 4.18). Since for curves with complex multiplication the Beilinson conjectures were proven by Bloch [8], the Beilinson conjectures are already proven for this curve.

2. Let C be another curve of Example 5.3.9. If we force the 3-torsion polynomial $t(x)$ to have four rational factors, then we get eight possibly linearly independent elements in $\mathrm{K}_2^T(C)$.

   Liu and de Jeu [unpublished] found out that there exists a relation among the elements of this example, such that n K-rational factors yield at most $n-1$ linear independent elements of $\mathrm{K}_2(\mathrm{C}; \mathcal{O}_\mathrm{K})$.

   In detail: There exists a map f from $C: \quad y^3 = -x^6 + (f(x))^3$ to the Fermat curve $u^3 + v^3 = 1, \quad (x, y) \mapsto (-\frac{y}{x^2}, \frac{f(x)}{x^2})$. The six elements

   $$\begin{aligned} a_1 &= \{\tfrac{y-f(x)^3}{x^6}, f(x) - x^2\}, & b_1 &= \{\tfrac{y-\zeta_3 f(x)^3}{x^6}, f(x) - x^2\}, \\ a_2 &= \{\tfrac{y-f(x)^3}{x^6}, f(x) - \zeta_3 x^2\}, & b_2 &= \{\tfrac{y-\zeta_3 f(x)^3}{x^6}, f(x) - \zeta_3 x^2\}, \\ a_3 &= \{\tfrac{y-f(x)^3}{x^6}, f(x) - \zeta_3^2 x^2\}, & b_3 &= \{\tfrac{y-\zeta_3^2 f(x)^3}{x^6}, f(x) - \zeta_3^2 x^2\} \end{aligned}$$

   are in $\mathrm{K}_2(\mathrm{C}; \mathcal{O}_\mathrm{K})$, but $a_1 - a_2, a_1 - a_3, b_1 - b_2, b_1 - b_3$ come from K_2 of the Fermat curve of genus 1. For example $a_1 - a_2 = \{\frac{(y-f(x))^3}{x^6}, \frac{(f(x)-x^2)}{(f(x)-\zeta_3 x^2)} = f^*\{-(u+v)^3, \frac{v-1}{v-\zeta_3}\}$ is the pullback of an element in K_2 of the Fermat curve. Hence, there are at most two independent elements of these, such that we get at most four linear independent elements in $\mathrm{K}_2(\mathrm{C}; \mathcal{O}_\mathrm{K})$.

   Thus, we only get enough elements if the polynomials $f(x) - \zeta_3 x^2$ and $f(x) - \zeta_3^2 x^2$ split at the same time. The only example the author could find is the curve mentioned above given by the equation

   $$C: \quad y^3 = -x^6 + (x+1)^6.$$

   This curve was already covered in case 1 and is unsuited for testing the Beilinson conjectures.

Let us consider again the examples of Example 5.3.9. The first example is a case 1 curve, which is thus not relevant for testing the Beilinson conjectures. The second example is a special case of 2. Since there exists another linear dependency between the eight known elements, this example is also not suited for testing the Beilinson conjectures.

In summary, there is only one known class of examples for non-hyperelliptic superelliptic curves to test the Beilinson conjectures.

5.6 Elements in $\mathrm{K}_2(C, \mathcal{O}_K)$ for the Curve $y^3 = 59319x^4 + (-40x + 1)^3$

In this thesis we numerically check the Beilinson conjecture for the curve $C = C_{1,3}$. As explained in Section 5.5 (Theorem 5.5.1) the curve is of special interest because it is reasonable to check the Beilinson conjecture numerically.

Let C be the curve of (3.10.1) on page 58.

Since the right hand side of (3.10.1) factors in the following way

$$C : y^3 = (x - 1)(27x - 1)(2197x^2 - 92x + 1).$$

There are nine elements of $\mathrm{K}_2^T(C)$ that can be constructed using Construction 5.2.3.

If we call $T_1 = (x - 1)$, $T_2 = (27x - 1)$ and $T_3 = 2197x^2 - 92x + 1$, these elements are

$$\{\infty, \mathcal{O}_i, T_k\} \text{ for } 0 \leqslant i, k < 3.$$

For three of these elements, namely

$$\{\infty, \mathcal{O}_1, T_k\} \text{ for } 0 \leqslant k < 3,$$

no relation is known.

Making these elements explicit yields:

Lemma 5.6.1. The elements of $\mathrm{K}_2^T(C)$ are given by the following formulas:

$$\begin{aligned}
\{\infty, \mathcal{O}, T_1\} &= \left\{ \frac{(y - (-40x + 1))^3}{59319x^4}, 1 - x \right\} \\
\{\infty, \mathcal{O}, T_2\} &= \left\{ \frac{(y - (-40x + 1))^3}{59319x^4}, 1 - 27x \right\} \\
\{\infty, \mathcal{O}, T_3\} &= \left\{ \frac{(y - (-40x + 1))^3}{59319x^4}, 2197x^2 - 92x + 1 \right\}
\end{aligned}$$

Proof. The lemma follows directly from Theorem 5.2.2. □

By Theorem 5.5.1 it is known that these elements are integral.

Since C is of genus 3 and there are 3 elements of $\mathrm{K}_2(C, \mathcal{O}_K)$, there is a chance to test the Beilinson conjectures. We will be able to test the conjecture, if these three elements are linearly independent.

5.7 Computing the Beilinson Regulator

In this chapter we work out all necessary tools to calculate the Beilinson regulator.

Let K be a number field. Let C/K be a superelliptic curve defined by the equation

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

where f is a geometrically irreducible polynomial of degree m and $gcd(p, m) = 1$ and coefficients in $\mathbb{Z}$. Let $X = C(\mathbb{C})$ be the associated Riemann surface. Let the leading coefficient of $f(x)$ be positive. This can always be achieved by replacing x with $-x$ if necessary.

The curve C can be interpreted as a p-cover of $\mathbb{P}^1_{\mathbb{C}}$ by the map

$$\phi : X \to \mathbb{P}^1_{\mathbb{C}}, \quad (x, y) \mapsto x, \tag{5.7.1}$$

which has $m + 1$ ramification points $P_1, \ldots, P_m$ and $P_{m+1} = \infty$. The points $P_1, \ldots, P_m$ are the zeroes of the polynomials f. Let $P_i' = (P_i, 0)$, be the points on X, such that $\phi(P_i') = P_i$.

In the hyperelliptic case (cf. [19]) there exists a basis of $H_1(X, \mathbb{Z})$ consisting of liftings of simple loops in $\mathbb{P}^1_{\mathbb{C}}$ around P_i and P_{i+1} for all finite ramification points.

This is not possible for superelliptic curves such that $p > 2$, since these paths would not even be closed in X anymore and therefore are not even contained in $H_1(X, \mathbb{Z})$. The details why they are not closed are explained at the beginning of Section 5.9. Therefore, different paths in $P^1_{\mathbb{C}}$ have to be chosen.

To choose these loops it is first necessary to understand the Riemann surface X in more detail. Section 5.8 elaborates the structure of the Riemann surface for a curve over $\mathbb{Q}$, where there only exists one embedding and the Riemann surface is, thus, irreducible.

Afterwards, in Section 5.9 the structure of the group $H_1(X, \mathbb{Z})$ is determined in this setting.

Using the basis of $H_1(X, \mathbb{Z})$ from Section 5.9 we construct a basis of a subgroup of finite index of $H_1^-(X, \mathbb{Z})$ in Section 5.10.

Section 5.11 contains a brief overview how to simplify the actual computation on a computer.

5.8 The Riemann Surface X for Superelliptic Curves $C/\mathbb{Q}$

This chapter introduces a graphical notation for better understanding of the Riemann surface X for a curve $C/\mathbb{Q}$.

In this chapter $K = \mathbb{Q}$. Let $A \subset \mathbb{C} \subset \mathbb{P}^1_{\mathbb{C}}$ be the set

$$A = \{z \in \mathbb{C} | f(z) \neq 0\}.$$

As in [19] the constructed charts of the Riemann surface does not include charts that contain the branch points of the map ϕ. But any lift of a point $P \in A$ under the map ϕ of equation (5.7.1) is contained in at least one of the charts that is constructed. This is enough for this setting since the chosen loops never cross trough a branch point.

The charts we use are glued along the lifts of the real line.

Therefore, let

$$A^c = \{z \in \mathbb{C} | f(z) \notin \mathbb{R}\} \subset \mathbb{C} \subset P^1_{\mathbb{C}}.$$

To be able to glue charts together, the charts have to be defined in such way that they overlap each other. Thus, it is necessary to define two kinds of charts A^+ and A^-, which overlap on nonempty intersections.

Let $A^+ \subset \mathbb{C} \subset \mathbb{P}^1_{\mathbb{C}}$ and $A^- \subset \mathbb{C} \subset \mathbb{P}^1_{\mathbb{C}}$ be the open sets defined by

$$\begin{aligned} A^+ &= \left\{z \in \mathbb{C} | f(z) \notin \mathbb{R}^-_0\right\} \text{ and} \\ A^- &= \left\{z \in \mathbb{C} | f(z) \notin \mathbb{R}^+_0\right\}. \end{aligned}$$

Example 5.8.1. Let $C/\mathbb{Q}$ be the superelliptic curve

$$y^3 = f(x) = x^4 + x^3 - 2x^2 + 2x + 4.$$

The zero set of $f(x)$ is the set

$$\{-2, -1, 1 + i, 1 - i\}.$$

The set A is illustrated in Figure 5.8.1 on page 102. The zeroes are drawn as huge circles, so they can be identified more easily.

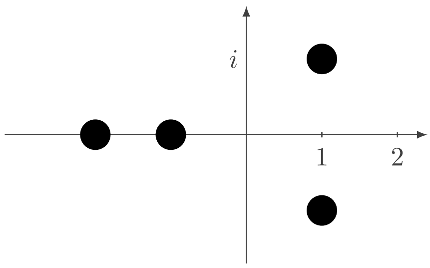


Figure 5.8.1: The set A of the curve $y^3 = x^4 + x^3 - 2x^2 + 2x + 4$

Since the axes clutter up the image they are left out in all further figures.

In this example the sets A^c, A^+ and A^- can be illustrated as in Figure 5.8.2 on page 103, Figure 5.8.3 on page 104 and Figure 5.8.4 on page 105. Note that in these pictures the black circles and lines illustrate the parts of $\mathbb{C}$ that are not contained in the set.

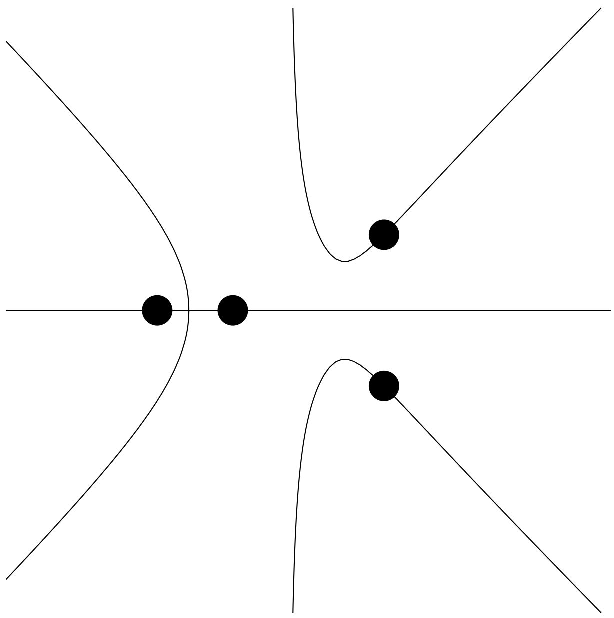


Figure 5.8.2: The set A^c of the curve $y^3 = x^4 + x^3 - 2x^2 + 2x + 4$

By construction $A^+ \cup A^- = A$ and $A^+ \cap A^- = A^c$.

Different lifts of A^+ and A^- are glued together in such a way that they give a cover of the whole Riemann surface, except at the branch points, the lifts of the zeroes P_i. Let ζ_p be a fixed pth-root of unity $\zeta_p = \exp\left(\frac{2\pi i}{p}\right)$. ζ_p is the first primitive pth-root of unity going counter-clockwise around the unit circle starting at 1.

The cover consists of special lifts of the sets A^- and A^+. Define

$$\begin{aligned} A_i^+ &= \left\{(x,y) \in X | x \in A^+ \text{ and } y = \zeta_p^i \sqrt[p]{f(x)}, \quad \frac{-\pi}{p} < \arg\left(\sqrt[p]{f(x)}\right) < \frac{\pi}{p}\right\} \text{ and} \\ A_i^- &= \left\{(x,y) \in X | x \in A^- \text{ and } y = \zeta_p^i \sqrt[p]{f(x)}, \quad 0 < \arg\left(\sqrt[p]{f(x)}\right) < \frac{2\pi}{p}\right\}. \end{aligned}$$

Remark 5.8.2. The definition implies

$$\begin{aligned} A_i^+ \cap A_i^- &= \left\{(x,y) \in X | x \in A^c \text{ and } y = \zeta_p^i \sqrt[p]{f(x)}, \quad 0 < \arg\left(\sqrt[p]{f(x)}\right) < \frac{\pi}{p}\right\} \\ A_{i-1}^- \cap A_i^+ &= \left\{(x,y) \in X | x \in A^c \text{ and } y = \zeta_p^i \sqrt[p]{f(x)}, \quad \frac{-\pi}{p} < \arg\left(\sqrt[p]{f(x)}\right) < 0\right\} \end{aligned}$$

and that all other intersections are empty.

The following lemmas give closer information how the Riemann surface is glued together.

Lemma 5.8.3. Let $C/\mathbb{Q}$ be a superelliptic curve, then

$$\bigcup_{0 \leqslant i \leqslant p} \left(A_i^+ \cup A_i^-\right) = X \backslash \bigcup_{1 \leqslant j \leqslant m+1} P_j'.$$

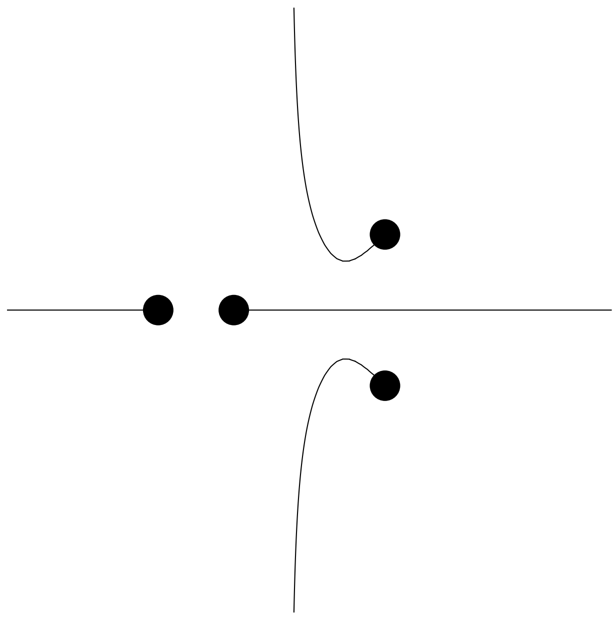


Figure 5.8.3: The set A^+ of the curve $y^3 = x^4 + x^3 - 2x^2 + 2x + 4$

Proof. It is clear that $\bigcup_{0\leqslant i\leqslant p}\left(A_i^+ \cup A_i^-\right) \subset X \backslash \bigcup_{1\leqslant j\leqslant m+1} P_j'$. We still need to prove that $\bigcup_{0\leqslant i\leqslant p}\left(A_i^+ \cup A_i^-\right) \supset X \backslash \bigcup_{1\leqslant j\leqslant m+1} P_j'$. Let $(x,y) \in X \backslash \bigcup_{1\leqslant j\leqslant m+1} P_j'$, so that $y \neq 0$. Therefore there exists an $i \in \{0,\cdots,p-1\}$ such that $y = \zeta_p^i \sqrt[p]{f(x)}$. Thus, the point (x,y) is either in A_i^+ or in A_i^-. □

The previous lemma shows that the given charts cover the whole Riemann surface, except the branch points. We are now going to investigate how these charts are glued together.

Lemma 5.8.4. Let $C/\mathbb{Q}$ be a superelliptic curve given by

$$C: \quad y^p = f(x)$$

and P a zero of $f(x)$. Let γ be a lift of a loop $\phi(x)$ in $\mathbb{P}^1_{\mathbb{C}}$ that circles clockwise p times around P such that no other zero of $f(x)$ is contained in the interior of that circle.

Let Q be a point on the loop $\phi(\gamma)$ and let Q_i be the lift of Q in A_i^+ or/and A_i^-, whichever is possible, for every $0 \leqslant i < p-1$. Then the Q_i are organized along γ either in increasing or decreasing order, depending on the sign of the leading coefficient of $f(x)$.

In detail: The numbers increase, if and only if the leading coefficient of $f(x)$ is negative.

Proof. For simplicity we prove this result for $Q_i \in A_i^-$. The proof for $Q_i \in A_i^+$ is similar.

If we follow along γ we leave A_i^- at some point and the question is, which chart covers the Riemann surface next.

By Remark 5.8.2 it is clear that the only two choices are A_i^+ or A_{i+1}^+. Since γ circles clockwise it is A_i^+ if the sign of the leading coefficient of $f(x)$ is positive and it is A_{i+1}^+ if the sign of the leading coefficient is negative.

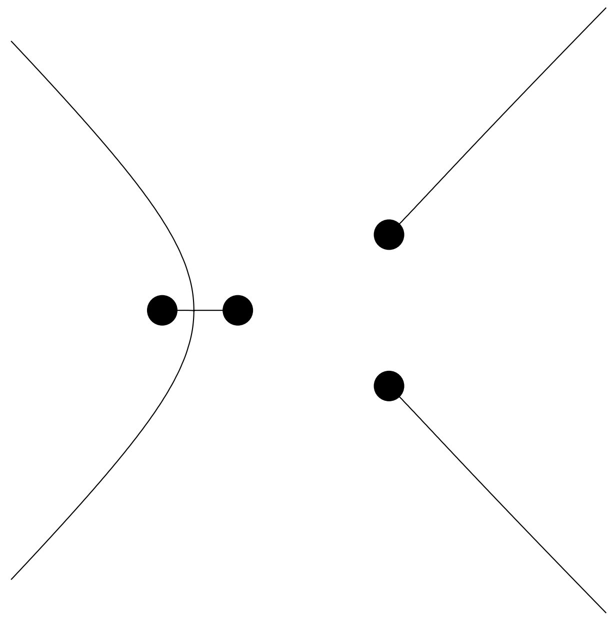


Figure 5.8.4: The set A^- of the curve $y^3 = x^4 + x^3 - 2x^2 + 2x + 4$

Again, by Remark 5.8.2 we know that if we follow along γ the next chart is A^-_{i-1}, resp. A^-_{i+1}. The next lift of Q is thus Q_{i-1}, resp. Q_{i+1}.

$\square$

5.9 First Homology Group of Superelliptic Curves $C/\mathbb{Q}$

The knowledge about X that has been gathered in Section 5.8 is used to construct a basis of $\mathrm{H}_1(X, \mathbb{Z})$.

Lifts of simple loops around roots do not work for non-hyperelliptic superelliptic curves, since a loop around two roots that starts in $A_i^{\pm}$ ends in the simplest case in $A_{i\pm2}^{\pm} \neq A_i^{\pm}$, since $p \geqslant 3$, so that this kind of loop is not closed any more on X. Therefore, other loops have to be chosen.

Lemma 5.9.1. Let $\gamma_{i,j}$ be a loop in $\mathbb{P}^1_{\mathbb{C}}$ that is an eight exactly around P_i and $P_j, i \neq j$. That is, $\gamma_{i,j}$ consist of a first clockwise loop around P_i and of a second counterclockwise loop around P_j, while no other P_k for $k \neq i$ (resp. $k \neq j$) is included in the interior of the first (resp. second) loop. Then it follows:

Any lift of $\gamma_{i,j}$ to X is a closed loop in X.

Proof. This lemma follows directly from Lemma 5.8.4. $\square$

This leaves several choices for choosing the paths. To give more detailed information on the first homology group the paths have to be more specific. Let us start by ordering the zeroes of $f(x)$.

Definition 5.9.2. In this thesis we consider the ramification points $P_1, \ldots, P_m$ ordered in the following way:

$$P_i = \begin{cases} \text{real for } 1 \leqslant i \leqslant r \text{ and} \\ \text{complex for } r < i \leqslant m. \end{cases}$$

Let P_{r+2i} and P_{r+2i+1} be complex conjugates and $\mathrm{Im}(P_{r+2i}) > 0$ for $0 \leqslant i \leqslant \frac{m-r}{2}$.

Furthermore, $P_i < P_j$ for all $i < j \leqslant r$ and either $\mathrm{Re}(P_{r+2k}) < \mathrm{Re}(P_{r+2\ell})$ for all $k < \ell \leqslant \frac{m-r}{2}$ or $\mathrm{Re}(P_{r+2k}) = \mathrm{Re}(P_{r+2\ell})$ and $\mathrm{Im}(P_{r+2k}) < \mathrm{Im}(P_{r+2\ell})$ for $k < \ell \leqslant \frac{m-r}{2}$.

If all ramification points are complex, we define $P_r = P_0 = 0$.

Using this ordering we can define a set of paths. This definition pins down the exact element of $\mathrm{H}_1(X, \mathbb{Z})$ we are using.

We start with defining paths in $\mathbb{P}^1_{\mathbb{C}}$.

To make some general definitions we first state two auxiliary definitions.

1. Let o_{min} be the minimal imaginary part of all ramification points with positive imaginary parts
$$o_{min} = \min_i(\mathrm{Im}\, P_{r+2i+1})$$
where $i \in \{0, \ldots, \frac{m-r}{2} - 1\}$.
2. The minimal positive distance between the coordinates of two torsion points is defined as d_{min}:
$$d_{min} = \min_{i \neq j} \left\{ \min_{\mathrm{Re}(P_i) \neq \mathrm{Re}(P_j)} |\mathrm{Re}(P_i) - \mathrm{Re}(P_j)|, \min_{\mathrm{Im}(P_i) \neq \mathrm{Im}(P_j)} |\mathrm{Im}(P_i) - \mathrm{Im}(P_j)| \right\}.$$

Definition 5.9.3. Let γ_j be an eight-path around P_j and P_{j+1} (one of the $\gamma_{j,j+1}$ of Lemma 5.9.1), defined in the following way:

1. The radius of all circles is
$$d = \min\left\{\frac{d}{4}, \frac{o_{min}}{4}\right\}.$$
2. The circle around P_j is given by
$$\alpha_j : [0,1] \to \mathbb{R}, x \mapsto P_j + d(\exp(-2i\pi x) + 1/2).$$
The circle around P_{j+1} is given by
$$\beta_j : [0,1] \to \mathbb{R}, x \mapsto P_{j+1} + d(\exp(2i\pi x) - 1/2).$$
3. For $1 \leqslant j < r$ the two circles are connected by $\delta_j : [0,1] \to \mathbb{R}, x \mapsto (P_j + 3d/2) + x(P_j - P_{j+1} - 3d)\}$.

4. For $j = r$ the two circles are connected by

$$\delta_r : [0,1] \to \mathbb{R},$$
$$x \mapsto \begin{cases} P_r + \frac{3d}{2} + 3xi(\frac{d}{4} + \frac{rd}{2m}), & \text{if } 0 \leqslant x \leqslant \frac{1}{3} \\ P_r + \frac{3d}{2} + (\frac{d}{4} + \frac{rd}{2m})i + (3x-1)(\operatorname{Re}(P_{r+1}) - P_r - 3d), & \text{if } \frac{1}{3} < x \leqslant \frac{2}{3} \\ \operatorname{Re}(P_{r+1}) - \frac{3d}{2} + (\frac{d}{4} + \frac{rd}{2m})i + (3x-2)(\operatorname{Im}(P_{r+1}) - (\frac{d}{4} + \frac{rd}{2m})i), & \text{otherwise.} \end{cases}$$

5. For $r < j < m-1$ let $s = \operatorname{sign}(\operatorname{Im}(P_j))$. The two circles are connected by

$$\delta_j : [0,1] \to \mathbb{R},$$
$$x \mapsto \begin{cases} P_j + \frac{3d}{2} + 8x\frac{jd}{2m}, & \text{if } 0 \leqslant x \leqslant \frac{1}{8} \\ P_j + \frac{3d}{2} + \frac{jd}{2m} + (8x-1)(-\operatorname{Im}(P_j)i + (\frac{d}{4} + \frac{jd}{2m})si), & \text{if } \frac{1}{8} < x \leqslant \frac{2}{8} \\ \operatorname{Re}(P_j) + \frac{3d}{2} + \frac{jd}{2m} + (\frac{d}{4} + \frac{jd}{2m})si + (8x-2)(P_r - \operatorname{Re}(P_j) + \frac{d}{2}), & \text{if } \frac{2}{8} < x \leqslant \frac{3}{8} \\ P_r + 2d + \frac{jd}{2m} + (\frac{d}{4} + \frac{jd}{2m}))si - (8x-3)(\frac{d}{2} + \frac{jd}{m})si, & \text{if } \frac{3}{8} < x \leqslant \frac{4}{8} \\ P_r + 2d + \frac{jd}{2m} - (\frac{d}{4} + \frac{jd}{2m}))si + (8x-4)(\operatorname{Re}(P_{j+1}) - P_r - \frac{d}{2}), & \text{if } \frac{4}{8} < x \leqslant \frac{5}{8} \\ \operatorname{Re}(P_{j+1}) + \frac{3d}{2} + \frac{jd}{2m} - (\frac{d}{4} + \frac{jd}{2m}))si & \\ +(8x-5)(\operatorname{Im}(P_{j+1})i + (\frac{-5d}{4} + \frac{jd}{2m})si), & \text{if } \frac{5}{8} < x \leqslant \frac{6}{8} \\ P_{j+1} + \frac{3d}{2} + \frac{jd}{2m} - \frac{3d}{2}si - (8x-6)(3d + \frac{jd}{2m}), & \text{if } \frac{6}{8} < x \leqslant \frac{7}{8} \\ P_{j+1} - \frac{3d}{2} - \frac{3d}{2}si + (8x-7)\frac{3d}{2}si, & \text{otherwise.} \end{cases}$$

6. The path γ_j is given by
$$\gamma_j = \alpha_j * \delta_j * \beta_j * \delta_j^{-1}.$$

We fix a p-root of unity ζ_p to be $\exp(2i\pi/p)$ and therefore fix the lifts $\gamma_1^k, 0 \leqslant k < p$ to be lift of γ_1 that contains the point $(P_j + \frac{\sqrt{3}d}{2}i, \zeta_p^k \sqrt[p]{f(P_j + \frac{\sqrt{3}d}{2}i)})$, with $\frac{-\pi}{p} < \arg\left(\sqrt[p]{f(x)}\right) \leqslant \frac{\pi}{p}$.

The rest of the $\gamma_i^k, 1 < i \leqslant m-1, \quad 0 \leqslant k < p$ are fixed as follows.

Let $(\gamma_i^k, \gamma_\ell^m)$ be the intersection pairing of γ_i^k and γ_ℓ^m.

Each path γ_i intersects with the path $\gamma_{i+1}, \quad 1 < i \leqslant m-2$ in two points, and their intersection numbers are $+1$ and -1.

These intersection points lift to X and we fix γ_i^k for $1 < i \leqslant m-1, \quad 0 \leqslant k < p$ such that
$$(\gamma_i^k, \gamma_{i+1}^k) = 1. \tag{5.9.1}$$

This conditions determines all γ_i^k, for $1 < i \leqslant m-1, \quad 0 \leqslant k < p$.

Remark 5.9.4. The exact definition of the paths used is necessary to uniquely describe the paths. For the calculations only the class in $\mathrm{H}_1(X,\mathbb{Z})$ is relevant for the correct result. Thus, in the following we rather use paths in the same class in $\mathrm{H}_1(X,\mathbb{Z})$ that are easy to draw and calculate.

Example 5.9.5. Let $C/\mathbb{Q}$ be the curve of Example 5.8.1. In Figure 5.9.1 on page 108 the loop γ_1^0 is shown. The A_i^-'s next to the curve give information about the chart that this part of the loop is contained in.

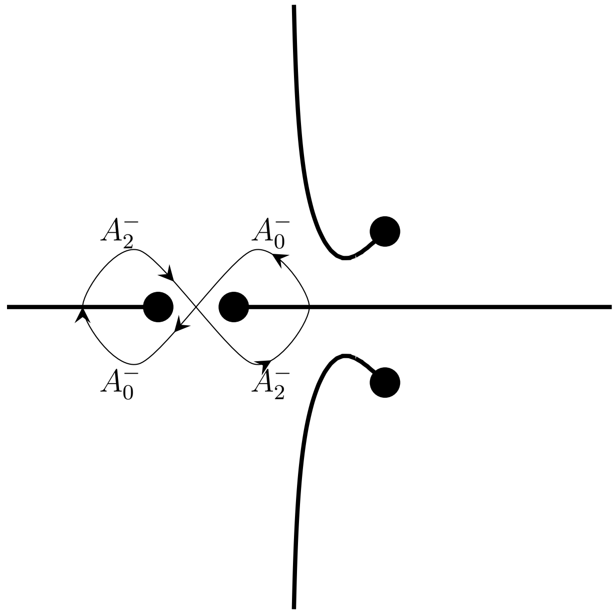


Figure 5.9.1: The path γ_1^0 on X

We denote the class of γ_i^k in $\mathrm{H}_1(X,\mathbb{Z})$ by $\left[\gamma_i^k\right]$.

Theorem 5.9.6. For $p = 3$ and $m = 4$ the set

$$B = \left\{\left[\gamma_i^k\right] | 1 \leqslant i \leqslant m-1,\ 0 \leqslant k \leqslant p-2\right\}$$

is a basis of $\mathrm{H}_1(X,\mathbb{Z})$.

Proof. We start the proof for general p and m, but at the end we have to show that the intersection matrix of the elements has determinant ± 1. Since we do that only for $p = 3$ and $m = 4$ the theorem follows.

First, we prove that the set B contains $2g$ elements and then we prove that they form a basis by showing that the determinant of the corresponding intersection matrix is equal to 1.

The set B contains $(m-1)(p-1)$ elements. The genus of X is given by $\frac{(m-1)(p-1)}{2}$. It thus follows that

$$|B| = (m-1)(p-1) = 2 \cdot \frac{(m-1)(p-1)}{2} = 2g.$$

We now calculate the intersection numbers. By definition (see equation (5.9.1) on page 107) we have

$$(\gamma_i^k, \gamma_{i+1}^k) = 1.$$

Since the leading coefficient of $f(x)$ is positive, we have

$$\begin{aligned}(\gamma_i^k, \gamma_{i+1}^{k-1}) &= -1,\\ (\gamma_i^k, \gamma_i^{k+1}) &= -1,\end{aligned}$$

and all other intersections are zero.

If we consider the intersection matrix to the set B ordered in the following way

$$\{\gamma_1^0, \gamma_2^0, \dots \gamma_{m-1}^0, \gamma_1^1, \dots \gamma_{m-1}^1, \gamma_1^{p-2}, \dots \gamma_{m-1}^{p-2}\},$$

then the intersection matrix M is given by a $2g \times 2g$-matrix, which consists of the blocks C, given by

$$C = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0\\ -1 & 0 & 1 & 0 & \dots & 0\\ 0 & \ddots & \ddots & \ddots & 0 & \vdots\\ 0 & 0 & \ddots & \ddots & \ddots & 0\\ \vdots & 0 & 0 & -1 & 0 & 1\\ 0 & \dots & \dots & 0 & -1 & 0 \end{pmatrix}$$

which is a $m-1 \times m-1$ -block that has 1 on the line above the diagonal and -1 on the line below the diagonal, and D, given by

$$D = \begin{pmatrix} 1 & 0 & 0 & 0 & \dots & 0\\ -1 & 1 & 0 & 0 & \dots & 0\\ 0 & \ddots & \ddots & \ddots & 0 & \vdots\\ 0 & 0 & \ddots & \ddots & \ddots & 0\\ \vdots & 0 & 0 & -1 & 1 & 0\\ 0 & \dots & \dots & \dots & 0, -1 & 1 \end{pmatrix}$$

which is a $m-1 \times m-1$ -block that has 1 one the diagonal and -1 on the line below the diagonal.

The intersection matrix M is thus given by

$$M = \begin{pmatrix} C & D & 0 & 0 & \dots & 0\\ -D^T & C & D & 0 & \dots & 0\\ 0 & \ddots & \ddots & \ddots & 0 & \vdots\\ 0 & 0 & \ddots & \ddots & \ddots & 0\\ \vdots & 0 & 0 & -D^T & C & D\\ 0 & \dots & \dots & \dots & 0, -D^T & C \end{pmatrix}$$

which is a $2g \times 2g = (m-1)(p-1) \times (m-1)(p-1)$-matrix that has A one the diagonal, B on the line above the diagonal, and $-B^T$ on the line below the diagonal.

To prove the theorem we have to calculate the determinant of the matrix M for the special case $p = 3$ and $m = 4$. It follows that

$$\det(M) = \det \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ -1 & 0 & 1 & -1 & 1 & 0 \\ 0 & -1 & 0 & 0 & -1 & 1 \\ -1 & 1 & 0 & 0 & 1 & 0 \\ 0 & -1 & 1 & -1 & 0 & 1 \\ 0 & 0 & -1 & 0 & -1 & 0 \end{pmatrix} = 1.$$

The theorem follows from the fact that the intersection pairing is non-degenerate for compact Riemann surfaces.

This follows from the fact that the intersection pairing is a skew-symmetric bilinear form on the homology and that it is non-zero on the canonical basis [20, section III.1].

□

Remark 5.9.7. Let $C/\mathbb{Q}$ be the curve of Example 5.8.1. The elements of the set

$$\{[\gamma_1^0], [\gamma_1^1], [\gamma_2^0], [\gamma_2^1], [\gamma_3^0], [\gamma_3^1]\}$$

form a basis of $H_1(X, \mathbb{Z})$. □

Remark 5.9.8. In this chapter we have put a lot of effort in naming and fixing lifts γ_i^k to be able to prove that they form a basis. For calculations it is not necessary to calculate the intersection numbers and select exactly the same cycles as in Theorem 5.9.6. Since the different lifts of one path satisfy the equation

$$\sum_{k=0}^{p-1} \gamma_i^k = 0,$$

for all $1 \leqslant i \leqslant m - 1$, any set of $p - 1$ different cycles of γ_i^k is a basis to the module generated by

$$\{[\gamma_i^k] \mid 0 \leqslant k \leqslant p - 2\}$$

for any fixed i.

5.10 On $\mathrm{H}_1^-(X, \mathbb{Z})$ of Superelliptic Curves $C/\mathbb{Q}$

The previous section described a basis for $\mathrm{H}_1(X, \mathbb{Z})$, but for Beilinson's conjectures we are interested in a basis for $\mathrm{H}_1^-(X, \mathbb{Z})$, the antiinvariant part of $\mathrm{H}_1(C, \mathbb{Z})$ under the action of complex conjugation on $\mathrm{H}_1(X, \mathbb{Z})$. The chosen basis does not allow a splitting into invariant and antiinvariant parts. Considering the curve of Example 5.8.1, in the last section we proved (Remark 5.9.7) that the set

$$\{[\gamma_1^0], [\gamma_1^1], [\gamma_2^0], [\gamma_2^1], [\gamma_3^0], [\gamma_3^1]\}$$

is a basis of $\mathrm{H}_1(X, \mathbb{Z})$. Of this set only one lift of γ_1 is antiinvariant and one lift of γ_3 is invariant. All other cycles contain invariant and antiinvariant parts.

In this chapter we use a standard method producing a basis for a subgroup of $\mathrm{H}_1^-(X, \mathbb{Z})$ by mapping each element of the base of $\mathrm{H}_1(C, \mathbb{Z})$ to the difference of itself and its complex conjugate, and thus generating an antiinvariant element. Afterwards, we compare the images of the constructed and original element and simplify the numerical calculations.

Lemma 5.10.1. Let B be the basis of $\mathrm{H}_1^-(X, \mathbb{Z})$ described in the last section. Let $\mathfrak{B}$ be the set

$$\mathfrak{B} = \{\gamma - c^*(\gamma) | \gamma \in B\},$$

where c^* denotes the action of the complex conjugation c on the Riemann surface $\mathrm{H}_1(X, \mathbb{Z})$.

Let $\mathfrak{B}'$ be a maximal subset of linearly independent elements of $\mathfrak{B}$.

The set $\mathfrak{B}'$ is a basis for a subset H of finite index of $\mathrm{H}_1^-(X, \mathbb{Z})$ the index is smaller than 2^{dg}.

Proof. The set H is clearly contained in $\mathrm{H}_1^-(X, \mathbb{Z})$, since all elements of $\mathfrak{B}$ are antiinvariant. On the other hand, B is a basis of $\mathrm{H}_1(C, \mathbb{Z})$, therefore $\mathrm{rank}(H) = \mathrm{rank}(\mathrm{H}_1^-(X, \mathbb{Z}))$. By the construction it is even clear that for all $\gamma \in \mathrm{H}_1^-(X, \mathbb{Z}), 2\gamma$ is contained in H. $\square$

By the definition of the regulator pairing we have for all $(a, b) \in \mathrm{K}_2^T(C)/\text{torsion}$

$$\begin{aligned}
\langle \gamma - c^*(\gamma), (a, b) \rangle &= \langle \gamma, (a, b) \rangle - \langle c^*(\gamma), (a, b) \rangle \\
&= \langle \gamma, (a, b) \rangle + \langle \gamma, (a, b) \rangle \\
&= 2\langle \gamma, (a, b) \rangle.
\end{aligned}$$

So the image under the regulator pairing of the constructed element $\gamma - c^*(\gamma)$ is twice the image of the original element γ.

Remark 5.10.2. For the numerical calculations we calculate the images of the original Base B. The determinants of the different possible square submatrices (of maximal rank) are either zero, if the cycles are linearly dependent modulo $\mathrm{H}_1^+(X, \mathbb{Z})$, or rational non-zero multiples of each other. We set the absolute value of the minimal non-zero determinant to be the regulator R' for our calculations. This regulator is a rational multiple of the regulator defined in Conjecture 4.4.3. Since the Beilinson conjectures hypothesize equality only up to a rational factor, this does not inflict our results.

5.11 Numerical Calculations of the Regulator

With the information from Section 5.9 it is now possible to calculate the regulator of a superelliptic curve.

However, plots of these paths tend to be rather unenlightening (see Figure 5.11.1 on page 112). Hence, we continue to picture homologous paths as in Figure 5.9.1 on page 108 for expository purposes.

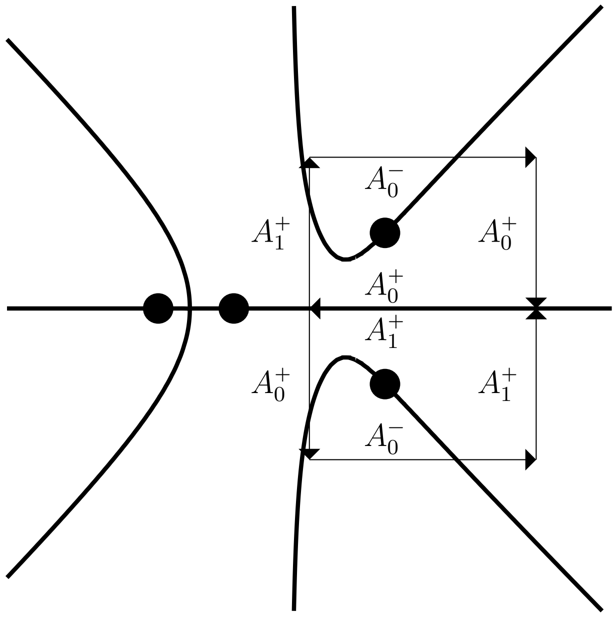


Figure 5.11.1: The path γ_3^1 on X as calculated by the computer

For the compute calculations we calculate the paring for γ for each element of the basis of Theorem 5.9.6. Afterwards, we determine the minimal non-zero absolute value of the determinant as described in Remark 5.10.2.

The sources for the computer programs used for the numerical calculations are contained in Chapter 6.

5.12 Computing the Beilinson Regulator of the Curve $y^3 = 59319x^4 + (-40x+1)^3$

The last section described three concrete elements $\mathrm{K}_2(C, \mathcal{O}_K)$. In this section we are going to calculate the Beilinson Regulator of the curve C. To do this, we have to use the zeroes of the p-torsion polynomial of C to construct elements in $\mathrm{H}_1(X, \mathbb{Z})$. Pairing these elements with the elements of $\mathrm{K}_2(C, \mathcal{O}_K)$ gives us the Regulator matrix, from which we can deduce the Beilinson Regulator.

The elements described in the last section are

$$\{\infty, \mathcal{O}, T_i\} \text{ for } 0 \leqslant i < 3 \tag{5.12.1}$$

which do not satisfy any of the known relations of Section 4.2 and Section 5.2.

By Lemma 5.6.1 these elements are explicitly given by the formula

$$\{\infty, \mathcal{O}, T_\alpha\} = \left\{ \frac{(y-(-40x+1)^3}{59319x^4}, \frac{\alpha(x)}{\alpha(0)} \right\}$$

with $\alpha(x) \in \{x-1, 27x-1, 2197x^2 - 92x + 1\}$.

This section describes all the necessary computations that have to be done to calculate the Beilinson Regulator of the curve

$$C : y^3 = t(x) = 59319x^4 + (-40x+1)^3 = 59319x^4 + f(x)^3.$$

To calculate the Beilinson Regulator, it is necessary to determine the charts that have to be used for the calculation (see Section 5.9). This is done by taking one cube root of $t(x)$ and moving to a new chart whenever $t(x)$ is a real number. To do so the path has to stay away from the zeroes of $t(x)$ (other charts would be needed here) and the poles of the functions of the element. The poles are only the points $(0,1), (0,\zeta_3), (0,\zeta_3^2)$ and the point at infinity, where ζ_3 is any primitive cube root of unity. So the zeroes of $t(x)$ have to be determined. The polynomial $t(x)$ factors over $\mathbb{Q}$ as

$$t(x) = (x-1)(27x-1)(2197x^2 - 92x + 1).$$

The zeroes of $t(x)$ are therefore

$$P_1 = 1 \qquad P_2 = 3^{-3}$$
$$P_3 = (-2+3i)^{-3} \qquad P_4 = (-2-3i)^{-3}.$$

Now the path can be defined as described in Section 5.11. The calculated paths on $C(\mathcal{C})$ are lifts of the following paths in $\mathbb{P}^1_{\mathbb{C}}$:

$$\gamma_1 : [0,1] \to \mathbb{P}^1_{\mathbb{C}}, \gamma_1(t) = \begin{cases} 0.03 + i + 0.47(8t) & \text{for } 0 \leqslant t \leqslant \frac{1}{8} \\ 0.5 + i - 2i(8t-1) & \text{for } \frac{1}{8} \leqslant t \leqslant \frac{2}{8} \\ 0.5 - i + 1(8t-2) & \text{for } \frac{2}{8} \leqslant t \leqslant \frac{3}{8} \\ 1.5 - i + 2i(8t-3) & \text{for } \frac{3}{8} \leqslant t \leqslant \frac{4}{8} \\ 1.5 + i - 1(8t-4) & \text{for } \frac{4}{8} \leqslant t \leqslant \frac{5}{8} \\ 0.5 + i - 2i(8t-5) & \text{for } \frac{5}{8} \leqslant t \leqslant \frac{6}{8} \\ 0.5 - i - 0.47(8t-6) & \text{for } \frac{6}{8} \leqslant t \leqslant \frac{7}{8} \\ 0.03 - i + 2i(8t-7) & \text{for } \frac{7}{8} \leqslant t \leqslant 1 \end{cases}$$

$$\gamma_2 : [0,1] \to \mathbb{P}^1_{\mathbb{C}}, \gamma_2(t) = \begin{cases} 1.5 + i - 1i(8t) & \text{for } 0 \leqslant t \leqslant \frac{1}{8} \\ 1.5 - i - 1(8t-1) & \text{for } \frac{1}{8} \leqslant t \leqslant \frac{2}{8} \\ 0.5 - i + 2i(8t-2) & \text{for } \frac{2}{8} \leqslant t \leqslant \frac{3}{8} \\ 0.5 + i - 0.49(8t-3) & \text{for } \frac{3}{8} \leqslant t \leqslant \frac{4}{8} \\ 0.01 + i - i(8t-4) & \text{for } \frac{4}{8} \leqslant t \leqslant \frac{5}{8} \\ 0.01 + 0.02(8t-5) & \text{for } \frac{5}{8} \leqslant t \leqslant \frac{6}{8} \\ 0.03 + i(8t-6) & \text{for } \frac{6}{8} \leqslant t \leqslant \frac{7}{8} \\ 0.03 + i + 1.47(8t-7) & \text{for } \frac{7}{8} \leqslant t \leqslant 1 \end{cases}$$

$$\gamma_3 : [0,1] \to \mathbb{P}^1_{\mathbb{C}}, \gamma_3(t) = \begin{cases} 0.01 + i(12t-5) & \text{for } 0 \leqslant t \leqslant \frac{1}{12} \\ 0.01 + i + 1.49(12t-6) & \text{for } \frac{1}{12} \leqslant t \leqslant \frac{2}{12} \\ 1.5 + i - 2i(12t-7) & \text{for } \frac{2}{12} \leqslant t \leqslant \frac{3}{12} \\ 1.5 - i - 1.47(12t-8) & \text{for } \frac{3}{12} \leqslant t \leqslant \frac{4}{12} \\ 0.03 - i + i(12t-9) & \text{for } \frac{4}{12} \leqslant t \leqslant \frac{5}{12} \\ 0.03 - 0.02(12t-10) & \text{for } \frac{5}{12} \leqslant t \leqslant \frac{6}{12} \\ 0.01 - i(12t-11) & \text{for } \frac{6}{12} \leqslant t \leqslant \frac{7}{12} \\ 0.01 - i + 1.49(12t) & \text{for } \frac{7}{12} \leqslant t \leqslant \frac{8}{12} \\ 1.5 - i + 2i(12t-1) & \text{for } \frac{8}{12} \leqslant t \leqslant \frac{9}{12} \\ 1.5 + i - 1.47(12t-2) & \text{for } \frac{9}{12} \leqslant t \leqslant \frac{10}{12} \\ 0.03 + i - i(12t-3) & \text{for } \frac{10}{12} \leqslant t \leqslant \frac{11}{12} \\ 0.03 - 0.02(12t-4) & \text{for } \frac{11}{12} \leqslant t \leqslant 1 \end{cases}$$

To determine the correct lift, the subset $M \subset \mathbb{P}^1_{\mathbb{C}}$ that has a real image under $t(x)$ has to be determined. This set can be visualized to sufficient accuracy by producing implicit plots of the imaginary part $\mathrm{Im}(t(z))$ of $t(z)$ for complex $z \in \mathbb{C}$. Figure 5.12.1 on page 115 shows the zero set of $\mathrm{Im}(t(z))$. The dots are the zeroes of $t(x)$. On the right side is the zero 1 and on the left side the three other zeroes agglomerate. Figure 5.12.2 on page 115 and Figure 5.12.3 on page 116 show implicit plots of those zeroes of $\mathrm{Im}(t(z))$ where $\mathrm{Re}(t(z))$ is negative, resp. positive. To distinguish the left three zeroes a more detailed plot is necessary. Figure 5.12.4 on page 116 shows the zeroes of $\mathrm{Im}(t(z))$ in the neighborhood of the three zeroes $\frac{1}{27}, \frac{46}{2197} + \frac{9}{2197}i$ and $\frac{46}{2197} - \frac{9}{2197}i$ of $t(z)$.

Using this data the lifts of the path can be split into parts that are contained in one chart. This data can be found in the sources for the computer calculations in Chapter 6.

This is everything that is needed to calculate the regulator pairing. The images of the elements under the regulator pairing are given in Table 5.12.5 on page 115.

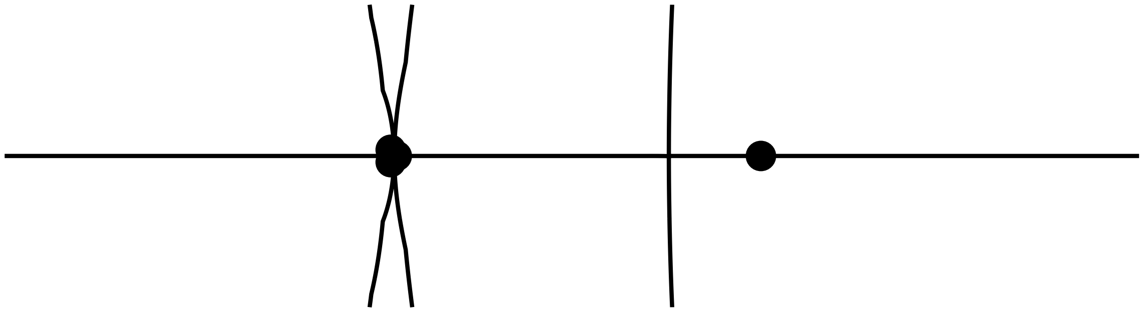


Figure 5.12.1: The zeroes of $\mathrm{Im}(t(x))$

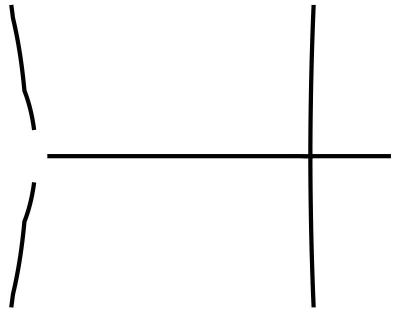


Figure 5.12.2: The zeroes of $\mathrm{Im}(t(x))$ where $\mathrm{Re}(t(x))$ is negative

The Table 5.12.5 on page 115 shows all values of the regulator pairing for a basis that was constructed in Section 5.10.

Following Remark 5.10.2 we find the minimal absolute value of the determinant of the possible square submatrices (of maximal rank).

A minimal absolute value of the determinant is taken for the cycles γ_1^1, γ_2^1 and γ_3^1. Let $M_{\gamma_1^1,\gamma_2^1,\gamma_3^1}$ be the matrix constructed from the paths γ_1^1, γ_2^1 and γ_3^1. The value of the corresponding determinant is

$$\det(M_{\gamma_1^1,\gamma_2^1,\gamma_3^1}) \approx -9563.1.$$

Taking the absolute value of the determinant of the matrix yields one of the main results of this thesis.

element	γ_1^0	γ_1^1	γ_2^0	γ_2^1	γ_3^0	γ_3^1
$\{\infty, \mathcal{O}_1, T_1\}$	11.845	−5.922	−11.858	6.449	18.307	−18.307
$\{\infty, \mathcal{O}_1, T_2\}$	−23.333	11.667	11.581	32.415	20.834	−20.834
$\{\infty, \mathcal{O}_1, T_3\}$	−21.350	10.675	44.752	35.913	−8.839	8.839

Table 5.12.5: Results of the numerical integration of the symbols along the given paths in H_1

Figure 5.12.3: The zeroes of $\mathrm{Im}(t(x))$ where $\mathrm{Re}(t(x))$ is positive

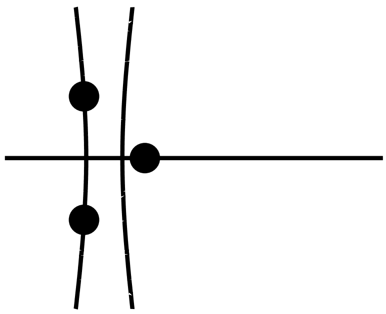


Figure 5.12.4: The zeroes of $\mathrm{Im}(t(x))$ in the neighborhood of $\frac{1}{27}$.

Theorem 5.12.1. The Regulator of C is up to a rational factor approximately

$$\mathrm{R}(C) \approx 9563.1.$$

□

Remark 5.12.2.

1. Since we are not using a basis of $\mathrm{H}_1^-(X, \mathbb{Z})$, but only of a submodule of finite index, the calculated Regulator is only a rational multiple of the original Regulator, which uses a basis of $\mathrm{H}_1^-(X, \mathbb{Z})$. This is not important for this thesis, since the Beilinson conjectures hypothesize the equality of the Regulator and the special value of the L-function only up to a rational number.
2. The precision of the calculation is really low. This comes from the fact that the zeroes of the chosen curve are very close together. Numerical integration only works well for paths that are far away from ramification points. In this example it was necessary to integrate very close to the zeroes of the curve and, therefore, only low precision could be acquired. The author tried to find other examples with higher numerical precision but, as explained in Section 5.3, these examples would require new methods to generate elements in $\mathrm{K}_2(C, \mathcal{O}_K)$.

   Furthermore, the considered example is in this perspective the best example from the class of examples given in Section 5.5, because for all other examples the three clustered ramification points would even be closer to each other.

The information of Theorem 5.12.1 and Theorem 3.12.2 can be combined into the following theorem, which gives numerical evidence for parts of the Beilinson conjectures.

Theorem 5.12.3. The following part of the Beilinson conjectures can be confirmed for the curve C: The group $\mathrm{K}_2(C, \mathcal{O}_K)$ is at least of rang 3.

The precision of the Regulator is only up to one decimal (see Remark 5.12.2); the result about the rational equivalency is not satisfying.

Remark 5.12.4. The quotient of $\mathrm{L}^*(C, Q, 0)$ by the Regulator is approximately

$$1.3.$$

6 Source Code for Computer Programs

This chapter contains simplified versions of all computer programs used in this thesis.

Remark 6.0.1. The calculations for this thesis were done in SageMath and Magma, using also PARI/GP and ComputeL. The reasons for the mix of system is the speed and possibility of doing the calculations. The author tested each calculation in each system in which it was possible. No system could provide all necessary calculations in a reasonable amount of time. For instance, while the calculation of regular models is not possible in SageMath, counting points over finite fields is extremely slow compared to Magma. On the other hand the numerical calculation of integrals in SageMath, provided by PARI/GP, is much faster than in Magma.

Remark 6.0.2. The sources in this chapter are simplified to ease understanding. The author removed the code for logging and parallel computing. Both are really important, since to archive a high precision very long calculations are necessary. With logging one can save results in case of server downtime, and through parallel computing one can take advantage of modern multi-core systems. Both methods were implemented by the author on shell-level. The programs presented in this chapter are sufficient for low precision calculations on a stable system. In tests done by the author each program finishes the calculations in under one day.

6.1 Invariants and Regular Model

The following Magma program calculates the basic invariants and the regular model for the curve C given by equation (3.10.1) on page 58.

```
//Creating the necessary objects
A3<X,Y,Z>:=ProjectiveSpace(Rationals(),2);
C:=Curve(A3,-59319*X^4 + 64000*X^3*Z - 4800*X^2*Z^2 + 120*X*Z^3
    + Y^3*Z - Z^4);
P<T>:=PolynomialRing(Rationals());

//Calulating the Genus
printf "The genus of the curve C is: ";
Genus(C);
```

```
//Calculating the Discriminant
disc:=Discriminant(Evaluate(DefiningPolynomial(C),[T,0,1]));
printf "The curve C has the discriminant: ";
disc;
discfact:=Factorisation(Round(disc));
printf "The discriminant factors as: ";
discfact;
print "";

//Calculating the fiber over 2
M2:=RegularModel(C,2);
cpts2 := Components(M2);
genera2 := [Genus(Curve(AffineSpace(Parent(Basis(cpt)[1])), cpt
    )) : cpt in cpts2];
printf "The fiber over 2 has %o components\n", #cpts2;
printf "The intersection Matrix is:\n";
IntersectionMatrix(M2);
printf "The components of the regular model over 2 have the
    genera: ";
genera2;
printf "The second component has positive genus and its
    LPolynomial is: ";
lpol2:=LPolynomial(Curve(AffineSpace(Parent(Basis(cpts2[2])[1])
    ), cpts2[2]));
Evaluate(lpol2,T);
print "";

//Calculating the fiber over 3
M2:=RegularModel(C,2);
M3:=RegularModel(C,3);
cpts3 := Components(M3);
genera3 := [Genus(Curve(AffineSpace(Parent(Basis(cpt)[1])), cpt
    )) : cpt in cpts3];
printf "The fiber over 3 has %o components\n", #cpts3;
printf "The intersection Matrix is:\n";
IntersectionMatrix(M3);
printf "The components of the regular model over 3 have the
    genera: ";
genera3;
printf "All component have genus 0.\n";
print "";

//Calculating the fiber over 13
```

```
M2:=RegularModel(C,2);
M13:=RegularModel(C,13);
cpts13 := Components(M13);
genera13 := [Genus(Curve(AffineSpace(Parent(Basis(cpt)[1])),
   cpt)) : cpt in cpts13];
printf "The fiber over 13 has %o components\n", #cpts13;
printf "The intersection Matrix is:\n";
IntersectionMatrix(M13);
printf "The components of the regular model over 13 have the 
   genera: ";
genera13;
printf "The fifth component has positive genus and its 
   LPolynomial is: ";
lpol13:=LPolynomial(Curve(AffineSpace(Parent(Basis(cpts13[5])
   [1])), cpts13[5]));
Evaluate(lpol13,T);
print "";

//Calculating the fiber over 17
M2:=RegularModel(C,2);
M17:=RegularModel(C,17);
cpts17 := Components(M17);
genera17 := [Genus(Curve(AffineSpace(Parent(Basis(cpt)[1])),
   cpt)) : cpt in cpts17];
printf "The fiber over 17 has %o components\n", #cpts13;
printf "The intersection Matrix is:\n";
IntersectionMatrix(M17);
printf "The components of the regular model over 17 have the 
   genera: ";
genera17;
printf "The first component has positive genus and its 
   LPolynomial is: ";
lpol17:=LPolynomial(Curve(AffineSpace(Parent(Basis(cpts17[1])
   [1])), cpts17[1]));
Evaluate(lpol17,T);
print "";
```

Listing 6.1.1: Code to calculate invariants and the regular model of the curve $C_{1,3}$

6.2 Calculating Points over Finite Fields

The following Magma program calculates points over finite fields for the primes of good reduction of the curve C given by equation (3.10.1) on page 58.

```
//Setting the start and end value
StartNumber:=3;
EndNumber:=1000000;

//Defining the Curve
K:=Integers();
A<x,y>:=AffineSpace(K,2);
P:=CoordinateRing(A);
f:=y^3-59319*x^4-(-40*x+1)^3;
C:=Curve(A,f);
P<T>:=PolynomialRing(K,2);

//Counting points over finite fields.
CurrentPrime:=NextPrime(StartNumber);
pr1:=[];
pr2:=[];
pr3:=[];
//Up to the third root calculate the points up to F_p^3
while CurrentPrime lt Root(EndNumber,3) do
pr1:=Append(pr1,<CurrentPrime, #Points(BaseChange(C, GF(
    CurrentPrime)), GF(CurrentPrime,1))+1>);
pr2:=Append(pr2,<CurrentPrime, #Points(BaseChange(C, GF(
    CurrentPrime)), GF(CurrentPrime,2))+1>);
pr3:=Append(pr3,<CurrentPrime, #Points(BaseChange(C, GF(
    CurrentPrime)), GF(CurrentPrime,3))+1>);
CurrentPrime:=NextPrime(CurrentPrime);
end while;

//Up to the third root squared alculate the points up to F_p^2
while CurrentPrime lt Root(EndNumber^2,3) do
pr1:=Append(pr1,<CurrentPrime, #Points(BaseChange(C, GF(
    CurrentPrime)), GF(CurrentPrime,1))+1>);
pr2:=Append(pr2,<CurrentPrime, #Points(BaseChange(C, GF(
    CurrentPrime)), GF(CurrentPrime,2))+1>);
CurrentPrime:=NextPrime(CurrentPrime);
end while;

//Up to the upper limit alculate the points up to F_p
while CurrentPrime lt EndNumber do
```

```
pr1:=Append(pr1,<CurrentPrime, #Points(BaseChange(C, GF(
    CurrentPrime)), GF(CurrentPrime,1))+1>);
CurrentPrime:=NextPrime(CurrentPrime);
end while;
```

Listing 6.2.1: Code to calculate points over finite fields for the curve $C_{1,3}$

6.3 On Local L-Polynomials for Primes of Good Reduction and Conductors

The following Magma program calculates the L −polynomials for primes of good reduction for the curve C given by equation (3.10.1) on page 58. The program uses the results of the program of Section 6.2. The program further uses ComputeL to test the conductor and calculate the special value of the L −function at 2.

```
// Array contains the counted points for each prime
// prX contains a tuple <p, N> where
// p is a prime
// and N is the number of points of the curve C over the field
    with p^X elements
// Since it is takes more time to calculate points over larger
    fields:
// #pr4>#pr3>#pr2>#pr1,
pr1m := pmap<Integers() -> Integers() | pr1>;
pr2m := pmap<Integers() -> Integers() | pr2>;
pr3m := pmap<Integers() -> Integers() | pr3>;
pr:=[pr1,pr2,pr3];

//Definition of the polynomial ring
P<T>:=PolynomialRing(Integers());

//For the bad primes the local L-polynomial has already been
    calculated
EFmap:=[<2,2*T^2 + 1>, <3,1-T>, <13,(13*T^2-5*T+1)*(1-T)^2>,
    <17, 289*T^4-2*T^2+1>];

// For all primes, where points have been calculated up to p^3,
// the full local L-polynomial can be calculated.
for i:=1 to #(pr[3]) do
  p:=pr1[i][1];
  //There is one point at infinity
  b:=[p-pr1m(p)+1, p^2-pr2m(p)+1, p^3-pr3m(p)+1];
```

```
  a:=[];
  Append(~a,-b[1]);
  Append(~a,-1/2*(a[1]*b[1]+b[2]));
  Append(~a,-1/3*(a[2]*b[1]+a[1]*b[2]+b[3]));
  if p notin [2,3,13,17] then
    Append(~EFmap,<p,1 +  a[1] * T + a[2] * T^2 + a[3] * T^3 +
       p*a[2] * T^4 + p^2*a[1] * T^5 + p^3 * T^6>);
  end if;
end for;

// For all primes, where points have been calculated up to p^2,
// the local L-polynomial can be calculated up to T^2.
for i:=#(pr[3])+1 to #(pr[2]) do
  p:=pr1[i][1];
  //There is one point at infinity
  b:=[p-pr1m(p)+1, p^2-pr2m(p)+1];
  a:=[];
  Append(~a,-b[1]);
  Append(~a,-1/2*(a[1]*b[1]+b[2]));
  if p notin [2,3,13,17] then
    Append(~EFmap,<p,1 +  a[1] * T + a[2] * T^2>);
  end if;
end for;

// For all primes, where points have been calculated up to p,
// the local L-polynomial can be calculated up to T.
for i:=#(pr[2])+1 to #(pr[1]) do
  p:=pr1[i][1];
  //There is one point at infinity
  b:=[p-pr1m(p)+1];
  a:=[];
  Append(~a,-b[1]);
  if p notin [2,3,13,17] then
    Append(~EFmap,<p,1 +  a[1] * T>);
  end if;
end for;

// Creating a partial map from the data
EFm := pmap<Integers() -> P | EFmap>;

//Check the functional equation for a certain conductor, sign
   and precision
function CheckLseries(val2,val3,sig,prec)
  cond := 2^val2*3^val3*13^2*17^2;
```

```
  Ls := LSeries(2, [0,0,0,1,1,1], cond, 0: Sign := sig,
     Precision := prec);
  LSetCoefficients(Ls, func<p, d | EFm(p)>);
  return CheckFunctionalEquation(Ls);
end function;

//Check the functional equation for a certain conductor, sign
   and precision
function CalculateLseries(val2,val3,sig,prec,value)
  cond := 2^val2*3^val3*13^2*17^2;
  Ls := LSeries(2, [0,0,0,1,1,1], cond, 0: Sign := sig,
     Precision := prec);
  LSetCoefficients(Ls, func<p, d | EFm(p)>);
  return Evaluate(Ls,value);
end function;

//Check all possible values for the conductor.
function TestConductors()
print "Starting␣to␣test␣conductors.";
bre:=0;
for i:=4 to 50 do
  for j:=5 to 50 do
    try
      lser:=CheckLseries(i,j,1,10);
      if lser lt 10^0 then
        "CheckLseries(",i,",",j,",1)=",lser;
      end if;
    catch e
        "Not␣enough␣coefficients␣for␣CheckLseries(",i,",",j,"
           ,1).";
         bre:=1;
    end try;
    try
      lser:=CheckLseries(i,j,-1,10);
      if lser lt 10^0 then
        "CheckLseries(",i,",",j,",-1)=",lser;
      end if;
    catch e
        "Not␣enough␣coefficients␣for␣CheckLseries(",i,",",j,"
           ,-1).";
         bre:=1;
    end try;
    if bre eq 1 then
      bre:=0;
```

```
      break;
    end if;
  end for;
end for;
end function;


print "Checking the possible conductors as long as the 
   calculated coefficients permit.";
TestConductors();
print "The conductor 2^6 3^5 13^2 17^2 with sign +1 is a viable
    candidate.";
printf "Check the combination to a higher precision:";
CheckLseries(6,5,1,20);

printf "Using the combination, we calculate the special value 
   at 2:"
SpecialValue2:=CalculateLseries(6,5,1,20,2);
SpecialValue2;

printf "Using all information we can calculate the value at 0:"
   ;
R:=RealField(20);
SpecialValue0:=2^6*3^5*13^2*17^2/(2*Pi(R))^6*SpecialValue2;
SpecialValue0;
```

Listing 6.3.1: Code to calculate the L-Polynomials and test the conductor of $C_{1,3}$

6.4 Determining the Regulator

The following SageMath program uses PARI/GP to calculate the regulator for the curve C given by equation (3.10.1) on page 58.

```
#Definition of the curve
f1(x)=(-40*x+1)
f(x) = 59319*x^4+f1(x)^3

#Definition of the concrete elements of H_1(X,Z)
paths=[]
paths.append("gamma10")
paths.append([0.03+I, 0, 0.5+I, 5, 0.5 -I ,5, 1.5-I, 0, 1.5+
   I, 1, 0.5+I, 1, 0.5-I, 0, 0.03-I, 0])
```

```
paths.append("gamma20")
paths.append([0.5+I, 1, 1.5+I, 0, 1.5-I, 5, 0.5-I ,5, 0.5 + I,
   0, 0.01 + I, 1, 0.01+0.01*I, 2, 0.01, 2, 0.03, 2, 0.03+I,
   2])

paths.append("gamma30")
paths.append([0.01+I, 0, 0.5+I, 5,  1.5+I, 4,  1.5-I, 3, 0.5-I
   ,2,  0.03-I, 2,  0.03, 2, 0.01, 2, 0.01 -0.01*I, 3, 0.01-I,
   4, 0.5-I, 5,  1.5-I, 0,  1.5+I, 1, 0.5+I,2, 0.03+I, 2, 0.03,
    2, 0.01, 2, 0.01+0.01*I, 1])


Pt.<t>=PolynomialRing(QQ)

#Definition of the functions for the element of K_2(C,Z)
a1(x,y)=(y-f1(x))^3/(59319*x^4)
a=[a1]

b1(x,y)=x - 1
b2(x,y)=27*x - 1
b3(x,y)=2197*x^2 - 92*x + 1

b=[b1,b2,b3]

#Definition of the charts
z = CDF.zeta(3)
z6= z+1
sqrt30p(x) =     x^(1/3)
sqrt31p(x) = z*x^(1/3)
sqrt32p(x) = z^2*x^(1/3)
sqrt30n(x) =   z6* (-x)^(1/3)
sqrt31n(x) = z*z6*(-x)^(1/3)
sqrt32n(x) = z^2*z6*(-x)^(1/3)

#Sage needs a workaround to work in the expected way
def g0p(x): return sqrt30p(f(x))
def g1p(x): return sqrt31p(f(x))
def g2p(x): return sqrt32p(f(x))
def g0n(x): return sqrt30n(f(x))
def g1n(x): return sqrt31n(f(x))
def g2n(x): return sqrt32n(f(x))
g = [g0p,g0n,g1p,g1n,g2p,g2n]

#Calculating the derivatives
```

```
df(x)=derivative(f(x),x)
dx(x,y)=1
dy(x,y)=1/(3*y^2)*df(x)

#Function to calculate line of a path
def int(a,b,start,stop,branch):
    #Calculate all necessary invariants
    da(x,y)=derivative(a(x,y),x)*dx(x,y)+derivative(a(x,y),y)*
        dy(x,y)
    db(x,y)=derivative(b(x,y),x)*dx(x,y)+derivative(b(x,y),y)*
        dy(x,y)
    wx(x,y)=1/(2*I)*real(log(a(x,y)))*db(x,y)/b(x,y)-1/(2*I)*
        real(log(b(x,y)))*da(x,y)/a(x,y)
    wxq(X,Y)=conjugate(wx(X,Y))
    c1(t)=start+(stop-start)*t
    dc1(t)=derivative(c1(t),t)
    F(t) = wx(c1(t),g[branch](c1(t)))*dc1(t)+wxq(c1(t),g[branch
        ](c1(t)))*conjugate(dc1(t))
    #Calculate the integral with pari
    erg = gp("intnum(t=0,1,"+str(F(t)).replace("conjugate","
        conj")+")")
    return erg

#Function to calculate the pairing for an element (a,b) and a
   path path.
def regpath(a,b,path,branch):
  path=copy(path)
  #Check if the path makes sense
  for i in range(1,len(path)/2+2):
    if abs(CC(n(g[path[mod(2*i-1,len(path))]](path[mod(2*i,len(
        path))]) - g[path[mod(2*i+1,len(path))]](path[mod(2*i,
        len(path))])))) >10^(-10):
      print("Attention: Your path does not match up!")
      print("g["+str(path[mod(2*i-1,len(path))])+"]("+str(path[
          mod(2*i,len(path))])+") != g["+str(path[mod(2*i+1,len(
          path))])+"]("+str(path[mod(2*i,len(path))])+")")
  res = 0
  #calculate the pairing for the given path
  for i in range(1,len(path)/2+1):
    res +=  int(a,b, path[mod(2*i-2,len(path))], path[mod(2*i,
        len(path))], mod(path[mod(2*i-1,len(path))]+2*branch,6))
  #calculate the pairing for the complex conjugate path
  for i in range(1,len(path)/2+1):
    res -=  int(a,b, conjugate(path[mod(2*i-2,len(path))]),
```

```
        conjugate(path[mod(2*i,len(path))]), mod(6-path[mod(2*i
        -1,len(path))]+2*branch,6))
    return n(real(CC(res)))

#Function to calculate the paring for an element (a,b) and all
    existing paths
def image(a,b):
    res=[]
    for pathnr in range(0,len(paths)/2):
        res.append(regpath(a,b,paths[2*pathnr+1],0))
        res.append(regpath(a,b,paths[2*pathnr+1],1))
    return res

#Function to calculate the pariring for all elements of K_2 and
    all paths.
def fullmatrix():
    res=[]
    for i in range(0,3):
        res.append(image(a[0],b[i]))
    return matrix(res)

M=fullmatrix();

print "The matrix for all paths is:"
print M
print " Taking the second, fourth, and sixth column yields the
    matrix:"
M2=Matrix([M.column(1),M.column(3),M.column(5)]).transpose()
print M2
print "The determinant of this matrix is: " + str(abs(det(M2)))
```

Listing 6.4.1: Code to calculate the Regulator of the curve $C_{1,3}$

Listings

List of Figures

List of Tables

Bibliography

[1] J. L. Alperin and R. B. Bell. *Groups and representations*, volume 162 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.

[2] M. Artin and A. Grothendieck. *Cohomologie etale des schemas*, volume 2 of *Seminaire de geometrie algébrique*. Institut des hautes etudes scientifiques, Paris, 1964.

[3] K. Arzdorf. *Semistable reduction of cyclic covers of prime power degree*. PhD thesis, Leibniz Universität Hannover, 2012.

[4] K. Arzdorf and S. Wewers. Another proof of the semistable reduction theorem. Preprint, arXiv:1211.4624, 2012.

[5] H. Bass. *Algebraic K-theory*. W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[6] A. A. Beĭlinson. Higher regulators and values of L-functions. *Journal of Soviet Mathematics*, 30(2):2036–2070, 1985.

[7] S. Bloch and D. Grayson. K_2 and L-functions of elliptic curves: computer calculations. In *Applications of algebraic K-theory to algebraic geometry and number theory, Part I, II (Boulder, Colo., 1983)*, volume 55 of *Contemp. Math.*, pages 79–88. Amer. Math. Soc., Providence, RI, 1986.

[8] S. J. Bloch. *Higher regulators, algebraic K-theory, and zeta functions of elliptic curves*, volume 11 of *CRM Monograph Series*. American Mathematical Society, Providence, RI, 2000.

[9] A. Borel. Cohomologie de SL_n et valeurs de fonctions zeta aux points entiers. *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)*, 4(4):613–636, 1977.

[10] S. Bosch, W. Lütkebohmert, and M. Raynaud. *Néron models*, volume 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1990.

[11] I. I. Bouw and S. Wewers. Computing l-functions and semistable reduction of superelliptic curves. Preprint, arXiv:1211.4459, 2012.

[12] A. Brumer and K. Kramer. The conductor of an abelian variety. *Compositio Math.*, 92(2):227–248, 1994.

[13] M. Börner, I. Bouw, and S. Wewers. The functional equation for L-functions of hyperelliptic curves. Preprint, arXiv:1504.00508, 2015.

[14] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren, editors. *Handbook of elliptic and hyperelliptic curve cryptography*. Discrete Math-

ematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006.

[15] V. Cossart, J. Giraud, and U. Orbanz. *Resolution of surface singularities*, volume 1101 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1984.

[16] C. W. Curtis and I. Reiner. *Representation theory of finite groups and associative algebras*. Pure and Applied Mathematics, Vol. XI. Interscience Publishers, a division of John Wiley & Sons, New York-London, 1962.

[17] P. Deligne and D. Mumford. The irreducibility of the space of curves of given genus. *Inst. Hautes Études Sci. Publ. Math.*, (36):75–109, 1969.

[18] T. Dokchitser. Computing special values of motivic L-functions. *Experiment. Math.*, 13(2):137–149, 2004.

[19] T. Dokchitser, R. de Jeu, and D. Zagier. Numerical verification of Beilinson's conjecture for K_2 of hyperelliptic curves. *Compos. Math.*, 142(2):339–373, 2006.

[20] H. M. Farkas and I. Kra. *Riemann surfaces*, volume 71 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1992.

[21] J.-M. Fontaine and Y. Ouyang. *Theory of p-adic Galois Representations*. unpublished, 2012.

[22] A. Grothendieck. Modèles de néron et monodromie, in groupes de monodromie en géometrie algébrique, sga7 i. In A. Grothendieck, editor, *Groupes de monodromie en géometrie algébrique, SGA7 I*, volume 228 of *Lecture Notes in Mathematics*, pages 313–523. Springer, Berlin- Heidelberg-New York, 1972.

[23] A. Heller and I. Reiner. Grothendieck groups of integral group rings. *Illinois J. Math.*, 9:349–360, 1965.

[24] W. W. J. Hulsbergen. *Conjectures in arithmetic algebraic geometry*. Aspects of Mathematics, E18. Friedr. Vieweg & Sohn, Braunschweig, second edition, 1994.

[25] A. Jorza. The birch and swinnerton-dyer conjecture for abelian varieties over number fields. unpublished, 2005.

[26] K.-I. Kimura. K_2 of a Fermat quotient and the value of its L-function. *K-Theory*, 10(1):73–82, 1996.

[27] M. J. Klassen and E. F. Schaefer. Arithmetic and geometry of the curve $y^3+1=x^4$. *Acta Arith.*, 74(3):241–257, 1996.

[28] S. Lang. *Abelian varieties*. Interscience Tracts in Pure and Applied Mathematics. No. 7. Interscience Publishers, Inc., New York, 1959.

[29] H. Liu and G. Tang. On the K_2 group of a family of curves. *Journal of the Graduate School of the Chinese Academy of Sciences*, 26(2):152–157, 2009.

[30] Q. Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002.

[31] P. Lockhart, M. Rosen, and J. H. Silverman. An upper bound for the conductor of an abelian variety. *J. Algebraic Geom.*, 2(4):569–601, 1993.

[32] Y. I. Manin and A. A. Panchishkin. *Introduction to modern number theory*, volume 49 of *Encyclopaedia of Mathematical Sciences*. Springer-Verlag, Berlin, second edition, 2005.

[33] J. Milnor. *Introduction to algebraic K-theory*. Princeton University Press, Princeton, N.J., 1971.

[34] R. Miranda. *Algebraic curves and Riemann surfaces*, volume 5 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1995.

[35] J. Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999.

[36] N. Otsubo. On the regulator of Fermat motives and generalized hypergeometric functions. *J. Reine Angew. Math.*, 660:27–82, 2011.

[37] D. Quillen. Finite generation of the groups K_i of rings of algebraic integers. In *Algebraic K-theory, I: Higher K-theories (Proc. Conf., Battelle Memorial Inst., Seattle, Wash., 1972)*, pages 179–198. Lecture Notes in Math., Vol. 341. Springer, Berlin, 1973.

[38] J. Rosenberg. *Algebraic K-theory and its applications*, volume 147 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[39] M. Rosenlicht. Some basic theorems on algebraic groups. *Amer. J. Math.*, 78:401–443, 1956.

[40] R. Ross. K_2 of Fermat curves with divisorial support at infinity. *Compositio Math.*, 91(3):223–240, 1994.

[41] P. Schneider. Introduction to the Beĭlinson conjectures. In *Beĭlinson's conjectures on special values of L-functions*, volume 4 of *Perspect. Math.*, pages 1–35. Academic Press, Boston, MA, 1988.

[42] J.-P. Serre. *Abelian l-adic representations and elliptic curves*. McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute. W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[43] J.-P. Serre. Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures). In *Séminaire Delange-Pisot-Poitou: 1969/70, Théorie des Nombres, Fasc. 2, Exp. 19 bis*, page 15. Secrétariat mathématique, Paris, 1970.

[44] J.-P. Serre. *Linear representations of finite groups*. Springer-Verlag, New York, 1977.

[45] J.-P. Serre and J. Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492–517, 1968.

[46] A. Silverberg and Y. G. Zarhin. Étale cohomology and reduction of abelian varieties.

Bull. Soc. Math. France, 129(1):141–157, 2001.

[47] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[48] M. Stoll. Euler factors and tate's algorithm for genus 2 hyperelliptic curve. unpublished, 2009. Sage Googlegroup.

[49] Y. Taniyama. L-functions of number fields and zeta functions of abelian varieties. *J. Math. Soc. Japan*, 9:330–366, 1957.

[50] R. Taylor. Galois representations. *Ann. Fac. Sci. Toulouse Math. (6)*, 13(1):73–119, 2004.

[51] W. C. Waterhouse. *Introduction to affine group schemes*, volume 66 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979.

[52] C. Weibel. *The K-book: an introduction to algebraic K-theory*, volume 145 of *Graduate Studies in Math.* 2013.

[53] A. Weil. *Sur les courbes algébriques et les variétés qui s'en déduisent*. Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg **7** (1945). Hermann et Cie., Paris, 1948.

[54] M. Young. *K_2 and L-series of elliptic curves over real quadratic number fields.* PhD thesis, University of Durham, 1995.

[55] N. Yui. The L-series of Calabi-Yau orbifolds of CM type. In *Mirror symmetry. V*, volume 38 of *AMS/IP Stud. Adv. Math.*, pages 185–252. Amer. Math. Soc., Providence, RI, 2006.

Eidesstattliche Erklärung

Ich versichere hiermit an Eides statt, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Hilfsmittel und Quellen verwendet habe.

Vincenz Busch

Hamburg, den 21. September 2016

Lebenslauf

entfällt aus datenschutzrechtlichen Gründen.

Abstract

This thesis is concerned with numerical evidence for the Beilinson conjectures for algebraic curves. We focus on superelliptic curves over a number field K, which are curves of the form

$$y^m = t(x), \qquad m, \deg(t) \geqslant 3, \ (m, \deg(t)) = 1,$$

where the polynomial $t(x)$ has coefficients in K and no multiple roots. This aims to generalize a previous approach of de Jeu, Dokchitser and Zagier, who successfully considered the case of hyperelliptic curves. The Beilinson conjectures relate the analytic regulator with a special value of the algebraic L-series; this naturally separates the numerical verification into two separate sub-problems.

At first we show in detail how to determine all algebraic geometric invariants – including local L-factors at primes of bad reduction and the conductor – which are necessary to numerically calculate special values of the L-function of such curves by using the algorithms described and implemented by Tim Dokchitser. In these sections on L-series of curves new results on the explicit calculation of the local L-polynomials, especially at primes of bad reduction, are presented, using ideas of Michael Stoll on certain properties of ℓ-adic cohomology groups.

Furthermore, in the sections on the regulator we first construct elements in the second K-group of certain superelliptic curves using an approach which is analogous to the construction of de Jeu, Dokchitser and Zagier, based on Bloch's trick. Some new insights on new relations of such elements are obtained; unfortunately, these reduce the number of computationally accessible curves drastically. In summary, this construction can only lead to enough elements for $K = \mathbb{Q}$ and $K = \mathbb{Q}[\zeta_3]$, where ζ_3 is a third root of unity and even in these cases the polynomial $t(x)$ has to factor into $\deg(t)-1$ factors. Nevertheless, we are still able to give one class of examples for which it is possible to numerically test the Beilinson conjecture, but this class of examples does not contain examples with small coefficients.

We are then able to bring both worlds together in this one class of examples. For one particular curve we numerically calculate the Beilinson regulator and numerically check Beilinson's conjecture. For this we explain how to calculate the regulator pairing for arbitrary superelliptic curves using numerical integration algorithms, but not with the same level of detail we dedicate to the L-functions. Due to the nature of the examples considered, all zeroes of the polynomial t lie closely together. This forces us to integrate close to the zeroes, which makes it impossible to compute the integrals to high precision.

Zusammenfassung

Diese Doktorarbeit beschäftigt sich mit numerischen Belegen zu Belinson Vermutungen algebraischer Kurven. Der Fokus liegt auf superelliptischen Kurven über einem Zahlkörper K. Dies sind Kurven der Form

$$y^m = t(x), \qquad m, \deg(t) \geqslant 3, \ (m, \deg(t)) = 1,$$

in denen das Polynom $t(x)$ Koeffizienten in K und keine mehrfache Nullstellen besitzt. Die Arbeit zielt darauf ab, einen vorangegangenen Ansatz von de Jeu, Dokchitser und Zagier zu verallgemeinern, welche sich erfolgreich mit dem Fall der hyperelliptischen Kurven beschäftigt haben. Die Beilinson Vermutungen vergleichen den analytischen Regulator mit einem speziellen Wert der algebraischen L-Serie. Diese Tatsache unterteilt die numerische Verifikation in zwei verschiedene untergeordnete Problemfelder.

Zuerst wird eingehend gezeigt, wie man alle algebraischen geometrischen Invarianten bestimmt - einschließlich der lokalen L-Faktoren an Primzahlen von schlechter Reduktion und dem Führer - welche notwendig sind um spezielle Werte der L-Funktion solcher Kurven numerisch zu berechnen. Die Berechnung benutzt die von Tim Dokchitser beschriebenen und implementierten Algorithmen. In diesen Teilen der Arbeit über L-Serien von Kurven werden neue Ergebnisse über die expliziten Berechnungen von lokalen L-Polynomen präsentiert, insbesondere bei Primzahlen von schlechter Reduktion, indem Ideen von Michael Stoll über bestimmte Eigenschaften von ℓ-adischen Kohomologiegruppen verwendet werden.

Darüber hinaus werden im Kapitel über den Regulator zunächst Elemente in der zweiten K-Gruppe bestimmter superelliptischer Kurven konstruiert, indem ein Ansatz verwendet wird, der sich analog zu de Jeus, Dokchitser und Zagiers Konstruktion verhält und auf Blocks Trick beruht. Einige neue Erkenntnisse über die neuen Beziehungen solcher Elemente werden gewonnen, allerdings reduziert sich dadurch die Anzahl der durch den Computer überprüfbaren Kurven drastisch. Zusammengefasst bedeutet dies, dass diese Konstruktion nur zu genügend Elementen führt für $K = \mathbb{Q}$ und $K = \mathbb{Q}[\zeta_3]$ wo ζ_3 eine dritte Einheitswurzel ist und sogar in diesen Fällen muss das Polynom $t(x)$ in $\deg(t) - 1$ Faktoren zerfallen. Ungeachtet dessen wird in der Doktorarbeit eine Klasse von Beispielen gezeigt, für welche es möglich ist die Beilinson Vermutung numerisch zu testen, allerdings beinhaltet diese Klasse von Beispielen keine Beispiele mit kleinen Koeffizienten.

In dieser Arbeit werden beide Welten in einer Klasse von Beispielen miteinander vereint. Für eine bestimmte Kurve wurde der Beilinson Regulator numerisch berechnet und getestet. Dafür wird erklärt, wie die Regulator Paarung für beliebige superelliptische Kurven mit Hilfe von numerischen Integrationsalgorithmen berechnet werden kann. Dies wird allerdings nicht genau so detailliert dargestellt wie die L-Funktionen. Aufgrund der Beschaffenheit der verwendeten Beispiele liegen alle Nullstellen des Polynoms (t) dicht beieinander. Diese Tatsache zwingt dazu nah entlang der Nullstellen zu integrieren was es unmöglich macht die Integrale in einer hohen Präzision zu berechnen.