The arithmetic of maximal curves, the Hesse pencil and the Mestre curve

Ane Anema

This research is financially supported by *Discrete, Interactive and Algorithmic Mathematics, Algebra and Number Theory* (DIAMANT); a mathematics cluster funded by the *Netherlands Organisation for Scientific Research* (NWO).

ISBN 978-90-367-9368-1 (printed version)
ISBN 978-90-367-9367-4 (electronic version)

rijksuniversiteit
groningen

The arithmetic of maximal curves, the Hesse pencil and the Mestre curve

Proefschrift

ter verkrijging van de graad van doctor aan de
Rijksuniversiteit Groningen
op gezag van de
rector magnificus prof. dr. E. Sterken
en volgens besluit van het College voor Promoties.

De openbare verdediging zal plaatsvinden op

maandag 5 december 2016 om 11.00 uur

door

Ane Schelte Izaäk Anema

geboren op 17 januari 1986
te Sneek

Promotor
Prof. dr. J. Top

Beoordelingscommisie
Prof. dr. T. Dokchitser
Prof. dr. S. Siksek
Prof. dr. H. Waalkens

Contents

Acknowledgement **vii**

Introduction **ix**

1 Elliptic curves maximal over finite extensions **1**

1.1 Supersingular case 2

1.2 Ordinary case 4

1.2.1 Upper bounds on the degree 4

1.2.2 Convergents 9

1.2.3 Algorithm 11

1.2.4 Upper bound on the cardinality 13

1.3 Maximal over cubic extensions 14

2 Maximal curves of genus 2 **19**

3 Hesse pencil and Galois action on 3-torsion **29**

3.1 The flex points 30

3.2 The 3-torsion group 31

3.3 The Weil-pairing 32

3.4 The Weierstrass form 33

3.5 Linear change of coordinates I 33

3.6 Linear change of coordinates II 34

3.7 Proof of the theorem 36

3.8 Characteristic two 37

3.9 Comparison with the literature 37

4 Jacobian variety of the Mestre curve **39**

4.1 Mestre curve 41

4.2 Galois theory 42

4.3 Idempotent relations 43

4.4 Geometrically simple 44

4.5 Computer search 45
4.5.1 The case $a_0 = 60$, $b_0 = 20$ 47

5 Faltings method 49
5.1 Applications 50
5.2 Deviation group 51
5.3 Residue kernel 53
5.4 Proof of the theorem 54
5.5 Remarks 55

6 Galois extensions with exponent four group 59
6.1 Maximal p-extensions 60
6.2 Exponent four quotients 61
6.3 Transitive groups 62
6.4 Composita 63
6.5 Determine $\mathbb{Q}_{S,4}$ for $S = \{2, 3, \infty\}$ 64
6.5.1 Exponent two extensions 65
6.5.2 The number fields 66
6.6 Frobenius elements 67
6.6.1 Computing the polynomials Γ_C 70
6.6.2 Searching for a polynomial h 70
6.6.3 Computing the Frobenius elements 71
6.6.4 The primes 71
6.7 Consequences for the Faltings method 71
6.7.1 The case $S = \{2, \infty\}$ 73
6.8 Other exponent 4 extensions 74
6.8.1 Elliptic curve example 74
6.9 Open questions 76

7 Van Wamelen method 79
7.1 Theory 79
7.2 Application 81

Conclusion 85

Samenvatting 87

Bibliography 93

Index 99

Curriculum Vitae 101

Acknowledgement

With pleasure I thank my supervisor Jaap Top for offering me the opportunity to write a PhD thesis and to benefit from his extensive knowledge. At random times I entered his office with a question and often either he knew the answer and enthusiastically explained it or he knew where to look for the answer. He showed me that teaching is an important part of the job.

I would like to thank Tim Dokchitser, Samir Siksek and Holger Waalkens as members of the assessment committee for the time they invested in reading this manuscript.

Also I would like to thank the DIAMANT mathematics cluster for financially supporting my PhD position.

The organizers of and the speakers at the numerous Intercity Number Theory Seminars at the mathematics departments throughout the Netherlands did a wonderful job. They reminded me of the broadness of mathematics: There will always be another interesting topic to study. The same can be said for the various DIAMANT symposiums.

The colleagues at the mathematics department provided a very pleasant atmosphere; many of them I consider a friend. I enjoyed the many conversations, especially during lunchtime. It is impossible to name all, but I do want to mention my office mates Filip Koerts, Nima and Pooya Monshizadeh, and my colleagues in the algebra group Arthemy Kiselev, Max Kronberg, Andrey Krutov, Thinh Nguyen, Marius van der Put, Sietse Ringers, Eduardo Ruiz Duarte, Afzal Soomro and Jaap Top.

In het bijzonder wil ik mijn moeder en mijn broer bedanken voor de onmisbare steun die zij voor mij vormen. Bij hen kan ik altijd terecht voor hulp, raad of gewoon gezelligheid.

Introduction

The present thesis is the result of studying questions concerning three topics in arithmetic geometry. Here we will describe and motivate these questions.

Preliminaries

We briefly and informally introduce a couple of frequently used concepts in this introduction. Let k be a field and $\overline{k}$ an algebraic closure of k.

Loosely speaking, a variety over k is an irreducible topological space X together with a ring of function $\mathcal{O}_X$ such that locally X is the set of zeros in $\overline{k}^n$ of a finite system of polynomial equations in $k[x_1, \ldots, x_n]$. The set $X(k)$ consists of the solutions with coordinates in k. More formally, a *variety* X over k is a geometrically integral scheme separable and of finite type over k. A *curve* over k is a variety over k of dimension 1, and a *surface* over k is a variety over k of dimension 2.

An *abelian variety* A over k is a complete group variety over k. This implies that $A(l)$ is a group for every extension l of k and the group structure is compatible with field extensions. In fact the $A(l)$ are abelian groups. The n-torsion subgroup $A[n]$ is the subgroup of $A\left(\overline{k}\right)$ of elements of order dividing n. An *isogeny* $A_1 \to A_2$ of abelian varieties A_1 and A_2 is a surjective morphism compatible with the group structures such that the dimensions of A_1 and A_2 are equal. It is a weaker version of an isomorphism.

An *elliptic curve* E over k is an abelian variety over k of dimension 1. If the characteristic of k is different from 2 and 3, then the underlying set of E is the set of solutions of a short Weierstrass equation

$$y^2 = x^3 + ax + b$$

and a point O at infinity, where a, b are constants in k such that $4a^3 + 27b^2 \neq 0$.

Let C be a complete non-singular curve over k of genus g. Although C itself is never an abelian variety for $g > 1$, we can assign an abelian variety $\mathrm{Jac}\,(C)$ to C called the *Jacobian variety*. The group structure on $\mathrm{Jac}\,(C)\left(\overline{k}\right)$ is related to the group of divisors on C modulo an equivalence relation. *Divisors* are formal finite sums of points in $C\left(\overline{k}\right)$. The dimension of $\mathrm{Jac}\,(C)$ is equal to g.

A *Galois representation* is a continuous homomorphism $G \to \mathrm{GL}_d(K)$, where G is a usually infinite Galois group and K is a topological field such as $\mathbb{F}_p$ or $\mathbb{Q}_p$. An important construction of Galois representations works as follows. Let A be an abelian variety over k. The action of $\mathrm{Gal}\left(\overline{k}/k\right)$ on the coordinates of the points in $A\left(\overline{k}\right)$ restricts to an action on $A[n]$. Since $A[n]$ is a free $\mathbb{Z}/n\mathbb{Z}$-module, for $n = p$ a prime different from the characteristic of k we get a Galois representation

$$\mathrm{Gal}\left(\overline{k}/k\right) \longrightarrow \mathrm{GL}_d(\mathbb{F}_p),$$

where $d = 2 \dim A$. Another representation is obtained by gluing together the modules $A[n]$ for $n = p, p^2, p^3, \dots$ via multiplication by p, namely

$$\mathrm{Gal}\left(\overline{k}/k\right) \longrightarrow \mathrm{GL}_d(\mathbb{Q}_p).$$

We provide a few references to the literature for a more rigorous background. An elementary introduction to algebraic geometry is given in [18, 47], and for more advanced topics see [25, 40, 66]. Abelian and Jacobian varieties are described in [45, 46]. An elementary introduction to elliptic curves is available from [63], and a more advanced discussion is provided in [61, 74]. For Galois representations see [12, Chapter 9].

Maximal curves

The first topic of this thesis deals with curves over finite fields such that the curve has many rational points. The number of rational points on a curve C of genus g over the field $\mathbb{F}_q$ with q elements is restricted by the well-known Hasse-Weil-Serre bound

$$q + 1 - g\lfloor 2\sqrt{q}\rfloor \leq |C(\mathbb{F}_q)| \leq q + 1 + g\lfloor 2\sqrt{q}\rfloor.$$

We call the curve C *maximal* over $\mathbb{F}_q$ if the upper bound is attained.

Interest in curves with many points comes from coding theory. A linear code is a subspace of a finite dimensional vector space over $\mathbb{F}_q$. It is used to encode information in such a way that errors can be detected and corrected. Goppa in 1981 introduced a method to construct a linear code from a curve over a finite field: Let C be a curve over $\mathbb{F}_q$, D a rational divisor on C and $\mathcal{P} = \{P_1, \dots, P_n\} \subset C(\mathbb{F}_q)$ a subset of rational points such that $\mathrm{Supp}\,(D) \cap \mathcal{P} = \emptyset$. Consider the linear map

$$\begin{aligned} \mathcal{L}(D) &\longrightarrow \mathbb{F}_q^n \\ f &\longmapsto (f(P_1), \dots, f(P_n)) \end{aligned}$$

that evaluates functions on C with poles bounded by D. The image of this map is a subspace of $\mathbb{F}_q^n$, that is a linear code of length n. The more rational points the curve C has, the longer the corresponding linear code. See [68] for more information on curves and their linear codes.

A curve with many points is also interesting in itself. Consider the quantity

$$N_q(g) := \max\left\{|C(\mathbb{F}_q)| : C \text{ a curve of genus } g \text{ over } \mathbb{F}_q\right\}$$

and its asymptotic value

$$A_q := \limsup_{g\to\infty} \frac{N_q(g)}{g}.$$

A precise description of $N_q(g)$ is known for $g = 0, 1, 2$, see [75, Theorem 4.1] and [54, Théorèmes 3 et 4] for the latter two cases. For higher genus such a description is unknown. However tables of lower and upper bounds on $N_q(g)$ for small q and g are available online at [19]. These tables are the successors to the tables listed in [20].

The Hasse-Weil-Serre bound provides an upper bound on $N_q(g)$ and A_q, but in general the bound is suboptimal. For example by considering $C(\mathbb{F}_q) \subset C\bigl(\mathbb{F}_{q^2}\bigr)$ Ihara deduced that if C is maximal over $\mathbb{F}_q$, then the genus of C is bounded from above in terms of q, that is if the genus g is sufficiently large with respect to the cardinality of $\mathbb{F}_q$, a maximal curve of genus g does not exists over $\mathbb{F}_q$. Moreover the Drinfeld-Vladut bound is

$$A_q \leq \sqrt{q} - 1,$$

whereas the Hasse-Weil-Serre bounds only gives $A_q \leq \lfloor 2\sqrt{q} \rfloor$. For a concrete pair of a field $\mathbb{F}_q$ and genus g the Hasse-Weil-Serre bound can sometimes be improved by considering for example the Jacobian variety of C as in [26, 27]. See also [68] for more information on upper bounds on $N_q(g)$ and A_q.

Lower bounds on $N_q(g)$ and A_q are usually obtained by providing actual curves with many points. Often constructions of such curves are motivated by the following fact: If a curve C is maximal over $\mathbb{F}_q$ and there is a surjective morphism of curves $C \to D$, then D is also maximal over $\mathbb{F}_q$. Therefore it seems reasonable to start with a curve D with many points and then consider morphisms $C \to D$ such that C has the desired genus. See [20] and references therein for various constructions.

In Chapter 1 we study elliptic curves E over $\mathbb{F}_q$ such that E is maximal over a finite extension of $\mathbb{F}_q$, that is

$$|E(\mathbb{F}_{q^n})| = q^n + 1 + \lfloor 2\sqrt{q}^n \rfloor$$

for some $n > 1$. We ask if the degree n of the field extension can be bounded, and how many elliptic curves are maximal over such an extension.

In Chapter 2 we construct curves of genus 2 over $\mathbb{Q}$ and over quadratic number fields such that for a positive proportion of the set of all primes p their reduction modulo a prime (above) p is maximal over $\mathbb{F}_{p^2}$. As in [35] we use the theory of complex multiplication of elliptic curves to obtain a precise description of the reduction modulo p.

The Hesse pencil

The second topic of this thesis deals with an explicit family of elliptic curves whose Galois representation on the 3-torsion subgroup is constant. The interest in such families started with the proof of the Modularity Theorem for semi-stable elliptic curves over $\mathbb{Q}$.

We briefly introduce modular elliptic curves. Consider the upper half-plane $\mathbb{H} := \{z \in \mathbb{C} : \operatorname{Im}(z) > 0\}$ and the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ by Möbius transformations. The quotient space of $\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ by the subgroup

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \mod N \right\}$$

is a compact Riemann surface, which in this case is an algebraic curve $X_0(N)$ over $\mathbb{Q}$. An elliptic curve E over $\mathbb{Q}$ is called *modular* if there exists a positive integer N and a surjective morphism

$$X_0(N) \longrightarrow E$$

over $\mathbb{Q}$. Wiles proved in 1995 that every semi-stable elliptic curve over $\mathbb{Q}$ is modular [76, Theorem 5.2]. Later this was extended to all elliptic curves over $\mathbb{Q}$ in [7, Theorem A]. See [12] for an introduction to the Modularity Theorem.

The work of Wiles generated interest in explicit families of elliptic curves over $\mathbb{Q}$ in which every elliptic curve has the same Galois representation on its p-torsion subgroup for a fixed prime p. The idea was to explicitly prove that infinitely many $j_0 \in \mathbb{Q}$ occur as the j-invariant of a modular elliptic curve. Such a family is constructed in [53] for $p = 3$ and $p = 5$.

In Chapter 3 we use the Hesse pencil of a given elliptic curve E over k to construct a family of elliptic curves such that for every curve the Galois representation on its 3-torsion subgroup is isomorphic to

$$\operatorname{Gal}\left(\overline{k}/k\right) \longrightarrow \operatorname{Aut}\left(E[3]\right),$$

and we give an elementary proof of its universal property. The classical Hesse pencil is given by

$$\mathcal{C} : x^3 + y^3 + z^3 + 6txyz = 0 \quad \subset \quad \mathbb{P}^2$$

with parameter t, see also [1]. It has 9 base points and these points are precisely the flex points of the cubics in this family. Since for an elliptic curve given by a Weierstrass equation the flex points coincide with the points of order dividing 3, the Hesse pencil appears to be the natural candidate for such a family.

The Mestre curve

The remaining topics of this thesis originated from a question concerning a hyperelliptic curve of genus 6 constructed by Mestre in [44], which we call the Mestre curve.

Consider an elliptic curve E over $\mathbb{Q}$. The group of rational points $E(\mathbb{Q})$ is abelian, and is finitely generated by the Mordell-Weil Theorem, that is

$$E(\mathbb{Q}) \cong A \times \mathbb{Z}^r$$

with A a finite abelian group and r the *rank* of E. Elkies found an example of an elliptic curve over $\mathbb{Q}$ with rank at least 28. It is unknown which ranks of elliptic curves over $\mathbb{Q}$ actually do occur, but on average the rank is bounded from above [3, Corollary 1.2]. See [59] for a concise survey on ranks of elliptic curves over $\mathbb{Q}$.

In Chapter 4 we study the Jacobian variety of the Mestre curve. This curve is used in [67] to construct a family of elliptic curves over $\mathbb{Q}$ such that the rank is at least 2 for infinitely many curves. Since the rank of these curves is related to the Jacobian variety of the Mestre curve, we hope to say more on the resulting rank by studying the Jacobian variety.

In Chapter 5 we consider the Faltings method to compare Galois representations attached to abelian varieties. This method allows us in principle to decide if two abelian varieties are isogeneous or not. We discuss if it is possible to apply this method explicitly to the Jacobian variety of a genus 2 curve and a product of two elliptic curves from Chapter 4.

In Chapter 6 we try to compute Galois extensions K of $\mathbb{Q}$ such that the Galois group has exponent 4, that is every automorphism $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ has order dividing 4. We need to determine such a field extension as a first step to apply the method in Chapter 5 to abelian surfaces.

In Chapter 7 we consider complex uniformization of abelian varieties as an alternative to the Faltings method. This method is employed in [72, 73] to explicitly compute isogenies between the Jacobian varieties of genus 2 curves. We apply this method to explicitly compute a morphism from a genus 2 curve to an elliptic curve over $\mathbb{Q}$.

Chapter 1

Elliptic curves maximal over finite extensions

Let E be an elliptic curve over $\mathbb{F}_q$. Recall the well-known Hasse bound on the number of points on an elliptic curve

$$||E(\mathbb{F}_{q^n})| - q^n - 1| \leq \left\lfloor 2\sqrt{q}^n \right\rfloor,$$

see for example [61, Theorem V.1.1] or [65, Theorem 5.1.1]. If E attains the Hasse upper bound over some finite extension, that is

$$|E(\mathbb{F}_{q^n})| = q^n + 1 + \left\lfloor 2\sqrt{q}^n \right\rfloor$$

for some n, then we say E is *maximal* over $\mathbb{F}_{q^n}$. We are interested in:

Question. *Let E be an elliptic curve over $\mathbb{F}_q$. Is E maximal over some finite extension of $\mathbb{F}_q$?*

This question is studied and partially answered by Doetjes in [14]. He shows that every elliptic curve over $\mathbb{F}_2$ is maximal over some extension, that elliptic curves over $\mathbb{F}_3$ in five isogeny classes are maximal over some extension, that elliptic curves over $\mathbb{F}_3$ in the remaining two isogeny classes are not maximal over extensions of low degree, and that elliptic curves over $\mathbb{F}_q$ with q a square are maximal over some extension in precisely three cases.

Our first result is summarized as:

Theorem 1.1. *Let E be an elliptic curve over $\mathbb{F}_q$ and $a_1 = q + 1 - |E(\mathbb{F}_q)|$.*

1. *If E is supersingular, that is $a_1 \in \left\{0, \pm\sqrt{q}, \pm\sqrt{2q}, \pm\sqrt{3q}, \pm 2\sqrt{q}\right\}$, then E is maximal over infinitely many extensions of $\mathbb{F}_q$ except when $a_1 \in \left\{-\sqrt{q}, 2\sqrt{q}\right\}$. In these exceptional cases extensions over which E is maximal do not exist.*

2. *If E is ordinary, that is $\gcd(a_1, q) = 1$, then there are at most finitely many extensions of $\mathbb{F}_q$ over which E is maximal. Furthermore if q is a square, then such extensions do not exist.*

We prove the first part of the theorem in Section 1.1. The second part we treat in Section 1.2. There we also give an explicit bound on the degree of the extension and list the pairs q, a_1 with $q < 1000$ corresponding to ordinary elliptic curves over $\mathbb{F}_q$ maximal over some finite extension. In Subsection 1.2.4 we show that the degree of the extension is at most 11 for sufficiently large q.

Our second result is:

Theorem 1.2. *For infinitely many primes p there exists an elliptic curve E over $\mathbb{F}_p$ such that E is maximal over $\mathbb{F}_{p^3}$.*

This confirms an observation made by Soomro in [65, Section 2.7] as well as our computations in Subsection 1.2.3. We prove the theorem in Section 1.3.

Notice that the property of E to be maximal over $\mathbb{F}_{q^n}$ depends only on the isogeny class of E, because isogeneous elliptic curves over a finite field have the same number of points, see [9, Lemma 15.1]. The isogeny classes of elliptic curves over $\mathbb{F}_q$ correspond to integers a_1 such that $|a_1| \leq 2\sqrt{q}$ and some additional conditions, see [75, Theorem 4.1]. Define the integers a_n as

$$a_n = q^n + 1 - |E(\mathbb{F}_{q^n})|.$$

If α is an eigenvalue of Frobenius, that is a root of the polynomial $X^2 - a_1 X + q$, then $a_n = \alpha^n + \bar{\alpha}^n$ with $\bar{\alpha}$ the conjugate of α, see [61, Section V.2]. So, the a_n's satisfy the recurrence relation

$$a_{n+1} = a_1 a_n - q a_{n-1}$$

for n a positive integer and $a_0 = 2$. Hence we reduced our question to:

Question. *Let q be a prime power and a_1 an integer such that $|a_1| \leq 2\sqrt{q}$. Is there a positive integer n such that $-a_n = \lfloor 2\sqrt{q}^n \rfloor$?*

In this chapter q, a_1 are integers with $q \geq 2$ and $|a_1| \leq 2\sqrt{q}$, α is a root of $X^2 - a_1 X + q$ and $\beta = \frac{\alpha}{\sqrt{q}}$. Fix an embedding $\mathbb{Q}(\sqrt{q}, \alpha) \to \mathbb{C}$ such that $\sqrt{q} > 0$ and α lies in the upper half-plane, that is $\arg(\alpha) \in [0, \pi]$.

If β is a root of unity, then the pair q, a_1 is called *supersingular*, otherwise the pair is called *ordinary*. This definition agrees with the one for elliptic curves whenever the pair q, a_1 corresponds to an isogeny class of elliptic curves, see again [75, Theorem 4.1].

The answer to the question is divided into two cases, namely the supersingular case and the ordinary case.

1.1 Supersingular case

The first part of Theorem 1.1 follows directly from:

Proposition 1.3. *Let q, a_1 be integers with $q \geq 2$ and $|a_1| \leq 2\sqrt{q}$. If the pair q, a_1 is supersingular, then $-a_n = \lfloor 2\sqrt{q}^n \rfloor$ for some positive integer n if and only if*

$$a_1 \in \left\{0, \sqrt{q}, \pm\sqrt{2q}, \pm\sqrt{3q}, -2\sqrt{q}\right\}.$$

Moreover if such an integer n exists, then there exist infinitely many.

The proposition above extends the result for $\mathbb{F}_q$ with q a square presented in [14, Chapter 5] to arbitrary $q \geq 2$. The new proof uses the following results:

Lemma 1.4. *If β is a root of the polynomial $X^2 - \frac{a_1}{\sqrt{q}}X + 1$ with q, a_1 integers and q non-zero, then β is a root of unity if and only if*

$$a_1 \in \left\{0, \pm\sqrt{q}, \pm\sqrt{2q}, \pm\sqrt{3q}, \pm 2\sqrt{q}\right\}.$$

Proof. Suppose that β is a primitive root of unity of order n. Let φ denote Euler's function, then $[\mathbb{Q}(\beta) : \mathbb{Q}] = \varphi(n)$. Since $\left[\mathbb{Q}\left(\sqrt{q}, \beta\right), \mathbb{Q}\right] \in \{1, 2, 4\}$, the same is true for $[\mathbb{Q}(\beta) : \mathbb{Q}]$. The cyclotomic polynomials of degree dividing 4 are listed in Table 1.1. Evaluate $X^2 - \frac{a_1}{\sqrt{q}}X + 1$ in a primitive root of unity ζ_n of order n for $n = 1, 2, 3, 4, 6$ to obtain $a_1 = 2\sqrt{q}, -2\sqrt{q}, -\sqrt{q}, 0, \sqrt{q}$ respectively. Notice that β is also a root of $X^4 + \left(2 - \frac{a_1^2}{q}\right)X^2 + 1$, and this polynomial and the cyclotomic polynomial both have degree 4 for $n = 5, 8, 10, 12$. This implies that $a_1 = \pm\sqrt{2q}, \pm\sqrt{3q}$ for $n = 8, 12$ respectively, and that the cases $n = 5, 10$ are impossible. Hence a_1 is as desired.

Assume that

$$a_1 \in \left\{0, \pm\sqrt{q}, \pm\sqrt{2q}, \pm\sqrt{3q}, \pm 2\sqrt{q}\right\}.$$

If $a_1 = \pm 2\sqrt{q}$, then $X^2 - \frac{a_1}{\sqrt{q}}X + 1 = (X \mp 1)^2$, that is β is a root of unity. Since β is a root of $X^2 - \frac{a_1}{\sqrt{q}}X + 1$, β is also a root of $X^4 + \left(2 - \frac{a_1^2}{q}\right)X^2 + 1$. If $a_1 \neq \pm 2\sqrt{q}$, then one of both polynomials is listed Table 1.1, that is β is a root of unity. Hence in either case β is a root of unity. □

Lemma 1.5. *Let q, a_1 be integers with q positive and $|a_1| \leq 2\sqrt{q}$. If n is a positive integer, then*

$$-a_n = \lfloor 2\sqrt{q}^n \rfloor \quad \Longleftrightarrow \quad |\beta^n + 1| < \frac{1}{\sqrt[4]{q}^n}.$$

Proof. Notice that $-a_n = \lfloor 2\sqrt{q}^n \rfloor$ is equivalent to $-a_n \leq 2\sqrt{q}^n < -a_n + 1$, which is the same as $0 \leq a_n + 2\sqrt{q}^n < 1$. Since $|a_n| \leq 2\sqrt{q}^n$ implies $0 \leq a_n + 2\sqrt{q}^n$, in fact $-a_n = \lfloor 2\sqrt{q}^n \rfloor$ if and only if $\left|a_n + 2\sqrt{q}^n\right| < 1$.

Recall that $a_n = \alpha^n + \bar{\alpha}^n$ and $|\alpha| = \sqrt{q}$ and $\beta = \frac{\alpha}{|\alpha|}$. Observe that

$$a_n + 2\sqrt{q}^n = \alpha^n + \bar{\alpha}^n + 2\sqrt{q}^n = \bar{\alpha}^n\left(\beta^{2n} + 1 + 2\beta^n\right) = \bar{\alpha}^n\left(\beta^n + 1\right)^2.$$

Substitute this relation in the last inequality to complete the proof. □

Table 1.1: The list of all cyclotomic polynomials Φ_n of degree d dividing 4. Recall that $\varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = d$.

d	n	Φ_n
1	1	$X-1$
	2	$X+1$
2	3	X^2+X+1
	4	X^2+1
	6	X^2-X+1
4	5	$X^4+X^3+X^2+X+1$
	8	X^4+1
	10	$X^4-X^3+X^2-X+1$
	12	X^4-X^2+1

Proof of Proposition 1.3. Suppose that $|\beta^n+1| < \frac{1}{\sqrt[4]{q^n}}$ for some positive integer n and $\beta^m+1 \neq 0$ for all integers m. Recall that β is a root of $X^2 - \frac{a_1}{\sqrt{q}}X + 1$ and by assumption β is also a root of unity. Thus the order of β is odd. According to Lemma 1.4 and its proof β has order 1 or 3. If the order is 1, then $|\beta^m+1| = 2$ for all integers m. If the order is 3, then $|\beta^m+1| \geq 1$ for all integers m. In either case this contradicts $|\beta^n+1| < \frac{1}{\sqrt[4]{q^n}}$. Hence for n a positive integer

$$|\beta^n+1| < \frac{1}{\sqrt[4]{q}^n} \quad \Longleftrightarrow \quad \beta^n+1=0.$$

Lemma 1.4 implies that $\beta^n+1=0$ for some positive integer n if and only if the order of β is even if and only if $a_1 \in \{0, \sqrt{q}, \pm\sqrt{2q}, \pm\sqrt{3q}, -2\sqrt{q}\}$.

The proposition follows from Lemma 1.5. □

1.2 Ordinary case

The first result restricting the possible values of q and n in this case is:

Proposition 1.6. *Let q, a_1 be integers with $q \geq 2$ and $|a_1| \leq 2\sqrt{q}$. If the pair q, a_1 is ordinary and $-a_n = \lfloor 2\sqrt{q}^n \rfloor$ for some positive integer n, then q is not a square and n is odd.*

Proof. Assume that $-a_n = \lfloor 2\sqrt{q}^n \rfloor$ for some positive integer n. Recall that $\beta = \frac{\alpha}{|\alpha|}$. If q is a square or n is even, then $\lfloor 2\sqrt{q}^n \rfloor = 2\sqrt{q}^n$, that is $\beta^n+1=0$ (see Lemma 1.5). However by assumption β is not a root of unity. □

1.2.1 Upper bounds on the degree

Given an ordinary pair q, a_1 we derive an upper bound on the n's such that $-a_n = \lfloor 2\sqrt{q}^n \rfloor$ using estimates for linear forms in logarithms.

Proposition 1.7. *Let q, a_1 be integers with $q \geq 2$ and $|a_1| \leq 2\sqrt{q}$. If the pair q, a_1 is ordinary, then $-a_n = \lfloor 2\sqrt{q}^n \rfloor$ for at most finitely many n.*

If β is an algebraic number, then the *height* of β is defined as the maximum of the absolute value of the coefficients of the primitive irreducible polynomial over $\mathbb{Z}$ with root β.

We denote the principal value of the complex logarithm by log.

Lemma 1.8. *If β is an algebraic number such that $|\beta| = 1$ and β is not a root of unity, then*

$$\log|\log(-\beta^n)| > -(32d)^{400} \log(4) \log\log(4) \log(h) \log(n)$$

for all integers $n \geq 4$, where $d = [\mathbb{Q}(\beta) : \mathbb{Q}]$ and $h \in \mathbb{Z}_{\geq 4}$ is an upper bound on the height of β.

This is a consequence of Baker's Theorem [2].

Proof. Notice that

$$\log(-\beta^n) = \log(-1) + n\log(\beta) + 2\pi k i = (2k+1)\log(-1) + n\log(\beta)$$

for some integer k. Define $m = 2k+1$. Since β is not a root of unity, $|\log(\beta)| < \pi$ and $|\log(-\beta^n)| < \pi$. This gives

$$|m|\pi = |\log(-\beta^n) - n\log(\beta)| \leq |\log(-\beta^n)| + n|\log(\beta)| < (n+1)\pi,$$

that is $|m| \leq n$ as m, n are integers. The lemma follows from [2, Theorem 2] with $4, h$ as the upper bounds on the heights of $-1, \beta$ respectively. □

Lemma 1.9. *Let q, a_1 be integers with $q \geq 2$ and $|a_1| \leq 2\sqrt{q}$. If the pair q, a_1 is ordinary and q is not a square, then the minimal polynomial of β over $\mathbb{Q}$ is*

$$X^4 + \left(2 - \frac{a_1^2}{q}\right)X^2 + 1.$$

Proof. Since β is a root of $X^2 - \frac{a_1}{\sqrt{q}}X + 1$, it is also a root of the polynomial above. Proposition 1.3 gives $a_1 \neq 0, \pm 2\sqrt{q}$, because β is not a root of unity. Thus $\sqrt{q} \in \mathbb{Q}(\beta)$ and $\mathbb{R}(\beta) = \mathbb{C}$. Hence $[\mathbb{Q}(\beta) : \mathbb{Q}] = 4$, that is the degree 4 polynomial is irreducible. □

Proof of Proposition 1.7. Suppose that the pair q, a_1 is ordinary, that is β is not a root of unity. Assume without loss of generality that q is not a square, because if $-a_n = \lfloor 2\sqrt{q}^n \rfloor$ for some positive integer n then q is not a square by Proposition 1.6.

Assume that $-a_n = \lfloor 2\sqrt{q}^n \rfloor$ for some positive integer n. Since $-\log(1-z) = \sum_{k=1}^{\infty} \frac{z^k}{k}$ and $\sum_{k=0}^{\infty} z^k = \frac{1}{1-z}$ for all $|z| < 1$,

$$|\log(1-z)| = \left|\sum_{k=1}^{\infty} \frac{z^k}{k}\right| < \sum_{k=1}^{\infty} c^k = \frac{c}{1-c}$$

for all $|z| < c < 1$. Take $z = \beta^n + 1$ and $c = \frac{1}{\sqrt[4]{q}^n}$. Since $|z| < c$ by Lemma 1.5 and $c < 1$ by assumption, the inequality above gives

$$|\log(-\beta^n)| < \frac{1}{\sqrt[4]{q}^n - 1}.$$

The minimal polynomial of β over $\mathbb{Z}$ has degree 4 and height at most $2q$ by Lemma 1.9. If $n \geq 4$, then Lemma 1.8 gives

$$\log|\log(-\beta^n)| > -\tilde{c}\log(2q)\log(n).$$

with $\tilde{c} = 2^{2800}\log(4)\log\log(4)$.

Let $d \in \mathbb{R}$ be a positive constant such that $d\sqrt[4]{q}^n \leq \sqrt[4]{q}^n - 1$ for all $n \geq 4$. If $-a_n = \lfloor 2\sqrt{q}^n \rfloor$ for some integer $n \geq 4$, then

$$-\tilde{c}\log(2q)\log(n) < \log|\log(-\beta^n)| < -\log(d) - \frac{n}{4}\log(q),$$

thus $n \leq n_0$ for some integer n_0, because the left-hand side of the inequality is logarithmic in n whereas the right-hand side is linear in n. Notice that n_0 depends only on q. Hence $-a_n = \lfloor 2\sqrt{q}^n \rfloor$ only for finitely many n. □

The proposition tells us that in this case there are at most finitely many solutions to $-a_n = \lfloor 2\sqrt{q}^n \rfloor$, but the bound on n is weak because the constant $\tilde{c}$ is huge. We obtain a much better bound by using a result from [39] instead of Baker's Theorem. The improved bound is:

Proposition 1.10. *Let q, a_1 be integers with $q \geq 2$ and $|a_1| \leq 2\sqrt{q}$.*

- *If $2 \leq q \leq 535$, then let N be the unique zero of*

$$n \longmapsto 123.6\pi^2\log^2\left(\frac{2n}{\pi}\right) - \frac{n\log(q)}{4} + \log(2)$$

larger than $\frac{\pi}{2}e^{\frac{21}{2}}$.

- *If $536 \leq q \leq 161043557$, then let N be the unique zero of*

$$n \longmapsto 61.8\pi\log(q)\log^2\left(\frac{n}{\pi} + \frac{2n}{\log(q)}\right) - \frac{n\log(q)}{4} + \log(2)$$

larger than $\frac{\pi\log(q)}{2\pi+\log(q)}e^{\frac{21}{2}}$.

- *If $161043558 \leq q$, then let $N = 85621$.*

If the pair q, a_1 is ordinary and $-a_n = \lfloor 2\sqrt{q}^n \rfloor$ for some n, then $n < N$.

In the case $q = 3$ Doetjes observed in [14] that for $a_1 = -2$ and $a_1 = 1$ there are no $n < 1000000$ such that $-a_n = \left\lfloor 2\sqrt{q}^n \right\rfloor$, and he expected that such n do not exist at all. Our upper bound on n shows that his observation is correct.

Notice that in the previous proposition the upper bound on n depends on q for $q \leq 161043557$, but is independent of q for larger q. This is due to the max term on right-hand side of the inequality in the lemma below.

The *logarithmic height* of an algebraic number β is defined as

$$\frac{1}{n}\left(\log|b| + \sum_{i=1}^{n} \log\max\{1, |\beta_i|\}\right)$$

with $b\prod_{i=1}^{n}(X - \beta_i)$ the minimal polynomial of β over $\mathbb{Z}$.

Lemma 1.11. *Let β be an algebraic number of absolute value one. If β is not a root of unity, then*

$$\log|\log(-\beta^n)| \geq -30.9\pi c \max\left\{d\log\left(\frac{n}{\pi} + \frac{n}{c}\right), 21, \frac{d}{2}\right\}^2$$

for all positive integers n, where $c = \max\{dl, \pi\}$ with l an upper bound on the logarithmic height of β and $d = \frac{[\mathbb{Q}(\beta):\mathbb{Q}]}{[\mathbb{R}(\beta):\mathbb{R}]}$.

Proof. Recall from the proof of Lemma 1.8 that

$$\log(-\beta^n) = m\log(-1) + n\log(\beta)$$

with m an odd integer such that $|m| \leq n$.

Assume that m is negative. After a change of notation the lemma follows from [39, Corollaire 1]: Let $\alpha_1 = \beta$, $\alpha_2 = -1$, $b_1 = n$, $b_2 = -m$ and $D = d$. The α_1 and α_2 are multiplicatively independent, because β is not a root of unity. Denote the logarithmic height of α by $h(\alpha)$. Since $h(\alpha_1) \leq l$ and $|\log(\alpha_1)| < \pi$, choose A_1 such that

$$\log(A_1) = \max\left\{l, \frac{\pi}{D}\right\}.$$

Notice that $h(\alpha_2) = 0$ and $|\log(\alpha_2)| = \pi$. Choose $\log(A_2) = \frac{\pi}{D}$. Finally use $b' \leq n\left(\frac{1}{\pi} + \frac{1}{c}\right)$ to obtain the desired lower bound.

Assume that m is positive. Observe that the logarithmic height of β and $\bar{\beta}$ are equal and $\log\left(\bar{\beta}\right) = -\log(\beta)$. Thus

$$|\log(-\beta^n)| = \left|-m\log(-1) + n\log\left(\bar{\beta}\right)\right|.$$

Apply [39, Corollaire 1] to the right-hand side just as before, but now with $\alpha_1 = \bar{\beta}$ and $b_2 = m$. □

Proof of Proposition 1.10. Suppose that the pair q, a_1 is ordinary. Recall from the proof of Proposition 1.7 that if $-a_n = \left\lfloor 2\sqrt{q}^n \right\rfloor$ for some positive integer n, then q is not a square and

$$|\log(-\beta^n)| < \frac{1}{\sqrt[4]{q}^n - 1}.$$

Notice that if $n_0 > 0$ and $d = 1 - \frac{1}{\sqrt[4]{q}^{n_0}}$, then $d\sqrt[4]{q}^n \le \sqrt[4]{q}^n - 1$ for all $n \ge n_0$.

The minimal polynomial of β over $\mathbb{Z}$ divides $qX^4 + \big(2q - a_1^2\big)X^2 + q$ by Lemma 1.9. Since $|\beta| = 1$ and β is not a root of unity, β, $\bar{\beta}$, $-\beta$ and $-\bar{\beta}$ are distinct roots of this polynomial. Therefore the logarithmic height of β is at most $\frac{1}{4}\log(q)$. Notice that $[\mathbb{Q}(\beta) : \mathbb{Q}] = 2|\mathbb{R}(\beta) : \mathbb{R}|$. Hence Lemma 1.11 gives

$$-30.9\pi c \max\left\{2\log\left(\frac{n}{\pi} + \frac{n}{c}\right), 21\right\}^2 \le \log|\log(-\beta^n)|$$

with $c = \max\left\{\frac{1}{2}\log(q), \pi\right\}$.

Consider the case that $\frac{1}{2}\log(q) \le \pi$ and choose $n_0 = 4$. Then the lower and upper bounds on $|\log(-\beta^n)|$ imply

$$0 < 30.9\pi^2 \max\left\{2\log\left(2\frac{n}{\pi}\right), 21\right\}^2 - \frac{n}{4}\log(q) + \log(2).$$

Denote the right-hand side by $f_1(q,n)$. Let $n_1 = \frac{\pi}{2}e^{\frac{21}{2}}$. Notice that

$$f_1(q,n_1) = 13626.9\pi^2 - \frac{\pi}{8}e^{\frac{21}{2}}\log(q) + \log(2)$$

is a decreasing function of q and $f_1\big(e^{2\pi}, n_1\big) > 0$. Therefore $f_1(q,n_1) > 0$ for all $q \le e^{2\pi}$. For $n \ge n_1$ the second derivative

$$\frac{\partial^2 f_1}{\partial n^2}(q,n) = 123.6\pi^2 \frac{1 - \log\left(\frac{2n}{\pi}\right)}{n^2}$$

is negative. Hence $n \mapsto f_1(q,n)$ is a concave function for $n \ge n_1$ and so for every $q \le e^{2\pi}$ it has a unique zero $n_2 \in (n_1, \infty)$. If $n \ge n_2$, then $f_1(q,n) \le 0$ and in particular $-a_n \ne \lfloor 2\sqrt{q}^n \rfloor$.

In the remainder of the proof assume that $\frac{1}{2}\log(q) > \pi$. Choose $n_0 = 12$. The lower and upper bounds on $|\log(-\beta^n)|$ imply $0 < f_2(q,n) - \log(d)$ with

$$f_2(q,n) = 15.45\pi\log(q)\max\left\{2\log\left(\frac{n}{\pi} + \frac{2n}{\log(q)}\right), 21\right\}^2 - \frac{n}{4}\log(q).$$

Let $n_1 = \frac{\pi\log(q)}{2\pi + \log(q)}e^{\frac{21}{2}}$. Then

$$f_2(q,n_1) = \frac{\pi e^{\frac{21}{2}}}{4}\left(\frac{27253.8 - e^{\frac{21}{2}}}{e^{\frac{21}{2}}}\log(q) + 2\pi - \frac{4\pi^2}{2\pi + \log(q)}\right).$$

Observe that $q \mapsto f_2(q,n_1)$ has only one extremum on $[e^{2\pi}, \infty)$, which is a maximum at $q \approx 541.9$. From $f_2\big(e^{2\pi}, n_1\big) \approx 44887.2$ and $f_2(q_1, n_1) > 4 \cdot 10^{-6}$ for $q_1 = 161043557$ follows $f_2(q,n_1) > 4 \cdot 10^{-6}$ for all $q \in [e^{2\pi}, q_1]$. On the other hand from $f_2(q_1 + 1, n_1) < -2 \cdot 10^{-5}$ follows $f_2(q,n_1) < -2 \cdot 10^{-5}$ for all $q \in [q_1 + 1, \infty)$. Notice that $-10^{-8} < \log(d) < 0$ for all $q > e^{2\pi}$. Hence $f_2(q,n_1) - \log(d) > 0$ for all $e^{2\pi} < q \le q_1$ and $f_2(q,n_1) - \log(d) < 0$ for all $q \ge q_1 + 1$.

For $n \geq n_1$ the first and second derivatives of f_2 with respect to n are

$$\frac{\partial f_2}{\partial n}(q,n) = 123.6\pi \log(q) \frac{\log\left(\frac{n}{\pi} + \frac{2n}{\log(q)}\right)}{n} - \frac{\log(q)}{4},$$
$$\frac{\partial^2 f_2}{\partial n^2}(q,n) = 123.6\pi \log(q) \frac{1 - \log\left(\frac{n}{\pi} + \frac{2n}{\log(q)}\right)}{n^2}.$$

The first derivative is negative for $n = n_1$. The second derivative is negative for all $n \geq n_1$. Hence $n \mapsto f_2(q,n) - \log(d)$ is a strictly decreasing function for $n \geq n_1$. If $q \geq q_1 + 1$, then it does not have a zero for $n \geq n_1$. For every $e^{2\pi} < q \leq q_1$ it has a unique zero $n_2 \in (n_1, \infty)$. As before if $n \geq n_2$, then $f_2(q,n) - \log(d) \leq 0$ and so $-a_n \neq \lfloor 2\sqrt{q}^n \rfloor$.

Consider the last case $q \geq q_1 + 1$ and $n < n_1$. Then $0 < f_2(q,n) - \log(d)$ is equivalent to

$$n < 27253.8\pi - \frac{4d}{\log(q)}.$$

Hence $n < 85621$. □

1.2.2 Convergents

An efficient method to determine the possible n such that $-a_n = \lfloor 2\sqrt{q}^n \rfloor$ is to compute convergents of a number associated to q and a_1, as described in [14, Section 6.1]. The reason why is given by [14, Stelling 6.8]. We reformulate and extend this result in the proposition and corollary below.

Proposition 1.12. *Let q, a_1 be integers with $q \geq 2$ and $a_1 = 2\sqrt{q}\cos(\theta)$ for some $\theta \in [0, \pi]$. If $-a_n = \lfloor 2\sqrt{q}^n \rfloor$ for some positive integer n, then*

$$\left| \frac{\theta}{\pi} - \frac{m}{n} \right| < \frac{1}{\pi} \sqrt{\frac{48}{48 - \pi^2}} \frac{1}{n \sqrt[4]{q}^n}$$

with m an odd integer.

Notice that the proposition is closely related to the upper bound on

$$|\log(-\beta^n)| = |m \log(-1) + n \log(\beta)|,$$

because $\log(-1) = i\pi$ and $\log(\beta) = i\theta$ by the choice of $\beta \in \mathbb{C}$.

The proof is a reformulation of the proof of [14, Stelling 6.8].

Proof. Notice that $a_n = 2\sqrt{q}^n \cos(n\theta)$. Therefore $-a_n = \lfloor 2\sqrt{q}^n \rfloor$ is equivalent to $1 + \cos(n\theta) < \frac{1}{2\sqrt{q}^n}$. Choose $\phi = n\theta - m\pi$ with $m \in \mathbb{Z}$ such that $\phi \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right)$. In fact m must be odd and $|\phi| < \frac{\pi}{2}$, otherwise

$$\cos(n\theta) = \cos(m\pi + \phi) = (-1)^m \cos(\phi) \geq 0$$

in contradiction with $1+\cos(n\theta) < \frac{1}{2\sqrt{q}^n}$. Thus

$$1-\cos(\phi) = 1+\cos(m\pi+\phi) = 1+\cos(n\theta) < \frac{1}{2\sqrt{q}^n}.$$

Use $\cos(x) \leq 1-\frac{1}{2}x^2+\frac{1}{24}x^4$ and $|\phi| < \frac{\pi}{2}$ to obtain

$$\frac{48-\pi^2}{48}\phi^2 < \phi^2\left(1-\frac{1}{12}\phi^2\right) = \phi^2-\frac{1}{12}\phi^4 \leq 2-2\cos(\phi) < \frac{1}{\sqrt{q}^n}.$$

Apply the inequality to $\left|\frac{\theta}{\pi}-\frac{m}{n}\right| = \frac{|\phi|}{\pi n}$ and the proposition follows. □

Corollary 1.13. *Let q, a_1 be integers with $q \geq 2$ and $a_1 = 2\sqrt{q}\cos(\theta)$ for some $\theta \in [0,\pi]$ and $x \in \mathbb{R}$ such that for some positive integer N*

$$\left|x-\frac{\theta}{\pi}\right| \leq \frac{1}{2N^2}\cdot\begin{cases} 1-\frac{2}{\pi}\sqrt{\frac{48}{48-\pi^2}}\frac{13}{\sqrt[4]{2}^{13}} & \text{if } q=2, \\ 1-\frac{2}{\pi}\sqrt{\frac{48}{48-\pi^2}}\frac{3}{\sqrt[4]{q}^3} & \text{if } q \geq 3. \end{cases}$$

If $-a_n = \lfloor 2\sqrt{q}^n \rfloor$ for some odd integer $3 \leq n \leq N$ and either $q \geq 3$ or $n \geq 13$, then $\frac{m}{n}$ is a convergent of x for some odd m.

This and Proposition 1.6 together imply [14, Stelling 6.8] for $x = \frac{\theta}{\pi}$.

Proof. Assume that $-a_n = \lfloor 2\sqrt{q}^n \rfloor$ for some $n \in \mathbb{Z}_{>0}$. If $x \in \mathbb{R}$ such that

$$\left|x-\frac{\theta}{\pi}\right| \leq \frac{1}{2n^2}-\frac{1}{\pi}\sqrt{\frac{48}{48-\pi^2}}\frac{1}{nq^{\frac{n}{4}}},$$

then $\left|x-\frac{m}{n}\right| \leq \left|x-\frac{\theta}{\pi}\right|+\left|\frac{\theta}{\pi}-\frac{m}{n}\right| < \frac{1}{2n^2}$ for some odd m by Proposition 1.12. Hence $\frac{m}{n}$ is a convergent of x by [23, Theorem 184].

Define the function $f : \mathbb{R} \to \mathbb{R}$ as

$$f(n) = 1-\frac{2}{\pi}\sqrt{\frac{48}{48-\pi^2}}\frac{n}{\sqrt[4]{q}^n}.$$

It has a global minimum at $n_0 = \frac{4}{\log(q)}$, because

$$\frac{df}{dx}(n) = -\frac{1}{2\pi}\sqrt{\frac{48}{48-\pi^2}}\frac{4-n\log(q)}{\sqrt[4]{q}^n}$$

is positive for $n > n_0$ and negative for $n < n_0$. In particular

$$f(n_0) = 1-\frac{2}{\pi}\sqrt{\frac{48}{48-\pi^2}}\frac{4}{e\log(q)},$$

which is positive for all q except $q = 2$. If $q = 2$, then $n = 13$ is the first integer for which $f(n)$ is positive. If $q = 3$, then $3 < n_0 < 4$ and $f(3) < f(5)$. If $q \geq 4$, then $n_0 < 3$. Since $3 \leq n \leq N$ is odd and either $q \geq 3$ or $n \geq 13$,

$$\frac{f(n)}{2n^2} \geq \frac{f(n)}{2N^2} \geq \frac{1}{2N^2} \begin{cases} f(13) & \text{if } q = 2, \\ f(3) & \text{if } q \geq 3. \end{cases} \geq \left| x - \frac{\theta}{\pi} \right|.$$

Hence $\frac{m}{n}$ is a convergent of x. □

Beware that if $-a_n = \lfloor 2\sqrt{q}^n \rfloor$ for some suitable q and n, then $\frac{m}{n}$ is a convergent of $\frac{\theta}{\pi}$ according to the corollary, but m and n need not be relative prime. However if $d = \gcd(m, n)$, then $-a_{n'} = \left\lfloor 2\sqrt{q}^{n'} \right\rfloor$ for $n' = \frac{n}{d}$, because for ϕ as in the proof of Proposition 1.12 the equality for n' is equivalent to

$$1 + \cos(n'\theta) = 1 - \cos\left(\frac{\phi}{d}\right) \leq 1 - \cos(\phi) < \frac{1}{\sqrt{q}^n} \leq \frac{1}{\sqrt{q}^{n'}}$$

by the proof of Proposition 1.12.

1.2.3 Algorithm

The previous two subsections together give a simple algorithm to compute for a given ordinary pair of integers q, a_1 with $q \geq 2$ and $|a_1| \leq 2\sqrt{q}$ the n's such that $-a_n = \lfloor 2\sqrt{q}^n \rfloor$. See Algorithm 1.1.

We implemented the algorithm in Pari/GP [50] for pairs q, a_1 corresponding to isogeny classes of ordinary elliptic curves, that is q is a prime power, $|a_1| \leq 2\sqrt{q}$ and $\gcd(q, a_1) = 1$. Two implementation details:

- The execution time of the function ConvergentsToSolutions can be reduced by verifying the necessary condition in Proposition 1.12 before calling IsSolution.

- In practice the value of $\frac{\theta}{\pi}$ is known only up to some error ε. Let N be the upper bound from Proposition 1.10. If $|\varepsilon| \leq 10^{-15}$, then by Corollary 1.13 a convergent $\frac{m}{n}$ of $\frac{\theta}{\pi}$ with $n \leq N$ is also a convergent of $\frac{\theta}{\pi} + \varepsilon$.

Using our program we computed the triples (q, a_1, n) with $q < 1000000$ a prime power, $|a_1| \leq 2\sqrt{q}$, $\gcd(q, a_1) = 1$ and $n > 1$ such that $-a_n = \lfloor 2\sqrt{q}^n \rfloor$. All triples have $n = 3$ or $n = 5$, except for $(2, 1, 13)$ and $(5, 1, 7)$. The triples with $n = 3$ and $q < 1000$ are listed in Table 1.2 and the triples with $n = 5$ and $q < 1000000$ are listed in Table 1.3. Based on these results we expect that the cases $n = 3$ and $n = 5$ occur infinitely often, whereas the cases $n \geq 7$ happen at most finitely many times.

Algorithm 1.1 The procedure MaximalCurves takes as input integers q, a_1 with $q \geq 2$ and $|a_1| \leq 2\sqrt{q}$ such that the pair is ordinary and outputs the n's with $n > 1$ such that $-a_n = \lfloor 2\sqrt{q}^n \rfloor$. The function MaximalDegree(q) returns the upper bound on n from Proposition 1.10, the function Convergents(x, N) computes the convergents of x with denominator at most N and the function IsSolution(q,a_1,n) checks $-a_n = \lfloor 2\sqrt{q}^n \rfloor$.

```
procedure MaximalCurves($q$, $a_1$)
    if $q$ not square then
        $\theta \leftarrow$ ArcCos($\frac{a_1}{2\sqrt{q}}$)
        $N \leftarrow$ MaximalDegree($q$)
        $C \leftarrow$ Convergents($\frac{\theta}{\pi}$, $N$)
        if $q = 2$ then
            for all $n \in \{3, 5, 7, 9, 11\}$ do
                if IsSolution($q$, $a_1$, $n$) then
                    print $n$
                end if
            end for
        end if
        for all $\frac{m}{n} \in C : m$ odd, $n$ odd do
            ConvergentsToSolutions($q$, $a_1$, $N$, $n$)
        end for
    end if
end procedure

function ConvergentsToSolutions($q$, $a_1$, $N$, $n$)
    if IsSolution($q$, $a_1$, $n$) then
        if $n > 1$ then
            print $n$
        end if
        for all $p \in \left\{3, \ldots, \left\lfloor \frac{N}{n} \right\rfloor\right\} : p$ prime do
            ConvergentsToSolutions($q$, $a_1$, $N$, $pn$)
        end for
    end if
end function
```

Table 1.2: The list of all pairs q, a_1 with $q < 1000$ a prime power, $|a_1| \leq 2\sqrt{q}$ and $\gcd(q, a_1) = 1$ such that $-a_3 = \lfloor 2\sqrt{q}^3 \rfloor$.

q	a_1	q	a_1	q	a_1	q	a_1	q	a_1	q	a_1
2	1	37	6	103	10	229	15	479	22	787	28
3	2	47	7	167	13	257	16	487	22	839	29
5	2	61	8	173	13	293	17	571	24	967	31
8	3	67	8	193	14	359	19	577	24		
11	3	79	9	197	14	397	20	673	26		
17	4	83	9	199	14	401	20	677	26		
23	5	97	10	223	15	439	21	727	27		
27	5	101	10	227	15	443	21	733	27		

Table 1.3: The list of all pairs q, a_1 with $q < 1000000$ a prime power, $|a_1| \leq 2\sqrt{q}$ and $\gcd(q, a_1) = 1$ such that $-a_5 = \lfloor 2\sqrt{q}^5 \rfloor$.

q	a_1	q	a_1
2	-1	8807	-58
3	-1	10391	-63
11	-2	10399	165
23	-3	22159	-92
31	9	122147	-216
128	-7	192271	-271
317	-11	842321	1485
2851	-33		

1.2.4 Upper bound on the cardinality

In this subsection we determine an upper bound on q and conclude:

Theorem 1.14. *There exist only finitely many ordinary pairs q, a_1 such that $-a_n = \lfloor 2\sqrt{q}^n \rfloor$ for some $n \geq 13$.*

Since the proof of Proposition 1.7 also gives an upper bound on the degree n independent of q, the theorem is an immediate consequence of:

Proposition 1.15. *Let $n \geq 13$ be an integer. There exists a constant q_n such that if $-a_n = \lfloor 2\sqrt{q}^n \rfloor$ for some integers q, a_1 with $q \geq 2$ and $|a_1| \leq 2\sqrt{q}$, then $q \leq q_n$ or the pair q, a_1 is supersingular.*

Proof. Assume that q, a_1 are integers with $q \geq 2$ and $|a_1| \leq 2\sqrt{q}$ such that $-a_n = \lfloor 2\sqrt{q^n} \rfloor$ for some n, then $|\beta^n + 1| < \frac{1}{\sqrt[4]{q^n}}$ by Lemma 1.5. Moreover assume that the pair q, a_1 is ordinary, that is β is not a root of unity.

Observe that $\beta^n + 1 = \prod_{i=1}^{n} \left(\beta - \zeta_{2n}^{2i+1}\right)$. Let i_0 be an integer such that

$$\left|\beta - \zeta_{2n}^{2i_0+1}\right| = \min_i \left|\beta - \zeta_{2n}^{2i+1}\right|,$$

which determines i_0 uniquely modulo n because β is not a root of unity. Since

$$\left|\beta - \zeta_{2n}^{2i+1}\right| \geq \min\left\{\left|\zeta_{2n}^{2i_0} - \zeta_{2n}^{2i+1}\right|, \left|\zeta_{2n}^{2i_0+2} - \zeta_{2n}^{2i+1}\right|\right\} > 0,$$

for all $i \not\equiv i_0 \bmod n$, there exists a positive constant c_n such that

$$|\beta^n + 1| \geq c_n|\beta - \zeta_{2n}^m| \geq c_n\left|\frac{a_1}{2\sqrt{q}} - \cos\left(\frac{m\pi}{n}\right)\right|$$

with $m = 2i_0 + 1$. Let $\varepsilon > 0$. According to [8, Theorem 2.7] there exists an ineffective constant c_0' depending on $\cos\left(\frac{m\pi}{n}\right)$ and ε such that

$$\left|\frac{a_1}{2\sqrt{q}} - \cos\left(\frac{m\pi}{n}\right)\right| \geq \frac{c_0'}{h^{3+\varepsilon}}$$

with h the height of $\frac{a_1}{2\sqrt{q}}$. Since there are n possible values of m, the above inequality is also true for some constant c_0 depending only on n and ε. The height of $\frac{a_1}{2\sqrt{q}}$ is at most $4q$. Therefore

$$|\beta^n + 1| \geq \frac{c_0 c_n}{(4q)^{3+\varepsilon}} = \frac{c}{q^{3+\varepsilon}}$$

for some positive constant c depending only on n and ε.

Choose $\varepsilon = \frac{1}{8}$ and $n \geq 13$. The upper and lower bounds on $|\beta^n + 1|$ imply $c < q^{3+\varepsilon-\frac{n}{4}}$. The right-hand side converges to zero for $q \to \infty$, but $c > 0$. Hence $q \leq q_n$ for some constant q_n independent of β. □

In some sense this proposition is the best possible in terms of n, because for $n = 7, 9, 11$ and m relative prime to n we deduce from [8, Theorem 2.8] that there exists a constant $\tilde{c}$ and infinitely many algebraic numbers γ of degree 1 or 2 such that $\left|\gamma - \cos\left(\frac{m\pi}{n}\right)\right| < \frac{\tilde{c}}{h_\gamma^{3-\varepsilon}}$ where h_γ is the height of γ. If $h_\gamma \sim q$, then this upper bound is eventually smaller than $\frac{1}{\sqrt[4]{q^n}}$.

1.3 Maximal over cubic extensions

In this section we prove Theorem 1.2. For the sake of completeness we also discuss some properties of the case $n = 3$. The discussion is closely related to [65, Section 2.7].

Given a supersingular pair q, a_1 such that $|a_1| \leq 2\sqrt{q}$ and $-a_3 = \left\lfloor 2\sqrt{q}^3 \right\rfloor$, then $a_1 = -2\sqrt{q}$ or $a_1 = \sqrt{q}$ by Proposition 1.3. In this case q must be a square. Since q is a prime in Theorem 1.2, we only consider ordinary pairs.

Recall the recurrence relation $a_{n+1} = a_1 a_n - q a_{n-1}$ with $a_0 = 2$ mentioned in the introduction. From this we deduce $a_3 = a_1^3 - 3qa_1$. Therefore

$$-a_3 = \left\lfloor 2\sqrt{q}^3 \right\rfloor \quad \Longleftrightarrow \quad 0 \leq a_1^3 - 3qa_1 + 2\sqrt{q}^3 < 1.$$

Define the function $f_q : \left[-2\sqrt{q}, 2\sqrt{q}\right] \to \mathbb{R}$ as $x \mapsto x^3 - 3qx + 2\sqrt{q}^3$. The graph of f_q is shown in Figure 1.1.

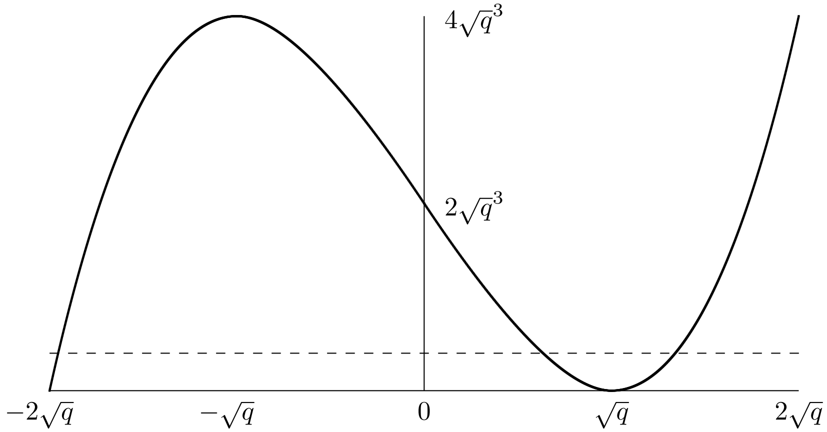

Figure 1.1: The graph of $f_q(a) = a^3 - 3qa + 2\sqrt{q}^3$.

Proposition 1.16. *Let q, a_1 be integers such that $q \geq 3$ and $|a_1| \leq 2\sqrt{q}$. If $-a_3 = \lfloor 2\sqrt{q}^3 \rfloor$, then $a_1 = -\lfloor 2\sqrt{q} \rfloor$ or $a_1 = \left[\sqrt{q}\right]$.*

Proof. Notice that f_q is maximal at $x = -\sqrt{q}, 2\sqrt{q}$ and that f_q is minimal at $x = -2\sqrt{q}$, $\sqrt{q}$ and

$$f_q(-2\sqrt{q}+1) = (3\sqrt{q}-1)^2 > 1$$

and

$$f_q\left(\sqrt{q} \pm \frac{1}{2}\right) = \frac{3}{4}\sqrt{q} \pm \frac{1}{8} > 1.$$

Hence $-2\sqrt{q} \leq a_1 < -2\sqrt{q}+1$ or $\sqrt{q} - \frac{1}{2} < a_1 < \sqrt{q} + \frac{1}{2}$, that is $a_1 = -\lfloor 2\sqrt{q} \rfloor$ or $a_1 = \left[\sqrt{q}\right]$. □

According to the following proposition the case $a_1 = -\lfloor 2\sqrt{q} \rfloor$ is possible only if the pair q, a_1 is supersingular.

Proposition 1.17. *Let q be an integer with $q \geq 2$ and $a_1 = -\lfloor 2\sqrt{q} \rfloor$. If $-a_3 = \lfloor 2\sqrt{q}^3 \rfloor$, then q is a square.*

Proof. Assume that q is not a square. Let $a = -a_1 = \lfloor 2\sqrt{q} \rfloor$.

The function f_q is strictly monotonically increasing and strictly concave on the interval $\left(-2\sqrt{q}, -\sqrt{q}\right)$, because $\frac{df_q}{dx} = 3x^2 - 3q$ and $\frac{d^2 f_q}{dx^2} = 6x$ are positive and negative respectively. Let x_0 be the intersection between the line $y = 1$ and the line through $\left(-2\sqrt{q}, 0\right)$ and $\left(-2\sqrt{q}+1, f_q\left(-2\sqrt{q}+1\right)\right)$. Then

$$a_1 + 2\sqrt{q} < x_0 + 2\sqrt{q} = \frac{1}{\left(3\sqrt{q}-1\right)^2}.$$

Notice that $4q = a^2 + b$ with $1 \leq b \leq 2a$. Since $\sqrt{1+x} \geq 1 + \left(\sqrt{2}-1\right)x$ for $0 \leq x \leq 1$,

$$a_1 + 2\sqrt{q} = a\left(-1 + \sqrt{1 + \frac{b}{a^2}}\right) \geq \left(\sqrt{2}-1\right)\frac{b}{a} \geq \frac{\sqrt{2}-1}{a} \geq \frac{\sqrt{2}-1}{\sqrt{q}}.$$

Combining the upper and lower bounds on $-a + 2\sqrt{q}$ yields

$$0 > \left(\sqrt{2}-1\right)(3\sqrt{q}-1)^2 - \sqrt{q},$$

but the right-hand side is positive by construction. Contradiction. □

We recall a sufficient condition on q such that $-a_3 = \lfloor 2\sqrt{q}^3 \rfloor$ for $a_1 = \lfloor \sqrt{q} \rfloor$. It is [65, Proposition 2.7.1] with a different proof.

Proposition 1.18 (Soomro). *If $q = a_1^2 + b$ with integers a_1, b such that $a_1 \geq 2$ and $|b| \leq \sqrt{a_1}$, then $-a_3 = \lfloor 2\sqrt{q}^3 \rfloor$.*

Proof. Let $0 < \epsilon \leq \frac{1}{3}$. Consider the function

$$g_\epsilon(x) = 1 + \frac{3}{2}x + \frac{3}{8}(1+\epsilon)x^2 - \sqrt{1+x}^3$$

and compute $\frac{dg_\epsilon}{dx} = \frac{3}{2} + \frac{3}{4}(1+\epsilon)x - \frac{3}{2}\sqrt{1+x}$ and $\frac{d^2 g_\epsilon}{dx^2} = \frac{3}{4}(1+\epsilon) - \frac{3}{4}\sqrt{1+x}^{-1}$. The function g_ϵ has extrema in $x = -\frac{4\epsilon}{(1+\epsilon)^2}$ and $x = 0$. The former is a maximum and the latter is a minimum. Let x_ϵ the unique zero of g_ϵ such that $-1 \leq x_\epsilon < -\frac{4\epsilon}{(1+\epsilon)^2}$. Hence for all $x > x_\epsilon$ and $x \neq 0$

$$\sqrt{1+x}^3 < 1 + \frac{3}{2}x + \frac{3}{8}(1+\epsilon)x^2.$$

Define $x = \frac{b}{a_1^2}$. Notice that

$$f_q(a_1) = -2{a_1}^3 - 3ba_1 + 2\sqrt{a_1^2 + b}^3 = 2a_1^3\left(-1 - \frac{3}{2}x + \sqrt{1+x}^3\right)$$

is minimal on (x_ϵ, ∞) for $x = 0$. If $x > x_\epsilon$ and $x \neq 0$, then

$$0 \leq f_q(a_1) = 2a_1^3\left(-1 - \frac{3}{2}x + \sqrt{1+x}^3\right) < \frac{3}{4}(1+\epsilon)\frac{b^2}{a_1}.$$

Observe that if $b = 0$ (or $x = 0$) then $f_q(a_1) = 0$.

Assume that $\epsilon = \frac{1}{3}$ and $|b| \leq \sqrt{a_1}$, then $x \geq -\sqrt{a_1}^{-3} > -1 = x_\epsilon$ and $0 \leq f_q(a_1) < \frac{3}{4}(1+\epsilon) = 1$. Hence $-a_3 = \lfloor 2\sqrt{q}^3 \rfloor$. □

A closer look at the proof tells us that in the proposition above the constraint $b^2 \leq a_1$ can be replaced by $b^2 \leq \frac{4}{3}\frac{1}{1+\epsilon}a_1$ at the expense of introducing a lower bound on a_1 in terms of ϵ.

Before proving Theorem 1.2, let us motivate that it is a non-trivial statement. Let q, a_1 be a pair such that q is an odd prime and $|a_1| \leq 2\sqrt{q}$. Then $a_1 = \lfloor \sqrt{q} \rfloor$ and the proposition above suggests that $q = a_1^2 + b$ with $b^2 \leq ca_1$ for some positive constant c. However the primes of this form have Dirichlet density zero, see [65, Remark 2.7.2]. Hence it is unlikely to find such primes.

The idea of the proof is to reduce the problem to a question on Gaussian primes in a small sector of the plane and apply [24, Theorem 1].

Proof of Theorem 1.2. Consider the set

$$S_1 = \left\{(a,b) \in \mathbb{Z}^2 : p = a^2 + b \text{ prime}, 0 < a, |b| \leq \sqrt{a}\right\}$$

and the subset $S_2 = \{(a,b) \in S_1 : b \text{ square}\}$. The set S_2 corresponds to

$$S_3 = \left\{(a,c) \in \mathbb{Z}^2 : p = a^2 + c^2 \text{ prime}, 0 < a, 0 \leq c \leq \sqrt[4]{a}\right\}.$$

Define for $\theta > 0$

$$S_4(\theta) = \left\{(a,c) \in \mathbb{Z}^2 : p = a^2 + c^2 \text{ prime}, 0 < a, 0 \leq c < p^{\theta}\right\}$$

and write $S_4(\theta) = S_5(\theta) \cup S_6(\theta)$ with $S_5(\theta) = \left\{(a,c) \in S_4(\theta) : a \geq p^{4\theta}\right\}$ and $S_6(\theta) = \left\{(a,c) \in S_4(\theta) : a < p^{4\theta}\right\}$. Observe that $S_5(\theta) \subset S_3$. If $\theta < \frac{1}{8}$, then the set $S_6(\theta)$ is finite, because $p = a^2 + c^2 < p^{8\theta} + p^{2\theta}$ and

$$\lim_{p \to \infty} \left(p^{8\theta - 1} + p^{2\theta - 1}\right) = 0.$$

The set $S_4(0.119)$ is infinite by [24, Theorem 1] and $0.119 < \frac{1}{8}$. Hence the sets $S_5(0.119) \subset S_3$ and $S_2 \subset S_1$ are also infinite. If $p = a_1^2 + b \in S_1$, then $|a_1| \leq 2\sqrt{q}$ and $-a_3 = \left\lfloor 2\sqrt{q}^3 \right\rfloor$ by Proposition 1.18. □

Chapter 2

Maximal curves of genus 2

We will construct curves of genus 2 over number fields such that for infinitely many primes the reduction of the curve at these primes is maximal over a quadratic extension of the residue field. The method is related to [35] and [65, Section 4.2].

Let C be a curve of genus g over $\mathbb{F}_q$. Recall the Hasse-Weil-Serre bound on the number of points on C:

$$||C(\mathbb{F}_q)| - q - 1| \leq g\lfloor 2\sqrt{q} \rfloor,$$

see [55] or [68, Theorem 5.3.1]. Analogous to Chapter 1, if the number of points on C attains the upper bound, that is

$$|C(\mathbb{F}_q)| = q + 1 + g\lfloor 2\sqrt{q} \rfloor,$$

then we call the curve C *maximal* over $\mathbb{F}_q$.

Suppose that C is a curve of genus g maximal over $\mathbb{F}_q$. In this case the proof of the Hasse-Weil-Serre bound shows that the characteristic polynomial of Frobenius is

$$\left(X^2 + \lfloor 2\sqrt{q} \rfloor X + q\right)^g.$$

This suggests – by Tate's Theorem [69, Theorem 1] – that the Jacobian variety $\mathrm{Jac}\,(C)$ of C is isogeneous over $\mathbb{F}_q$ to $E_1 \times \cdots \times E_g$ with E_i isogeneous elliptic curves over $\mathbb{F}_q$. If this is indeed the case, then C is maximal over $\mathbb{F}_q$ if and only if the E_i are maximal over $\mathbb{F}_q$.

We briefly recall some properties of elliptic curves with complex multiplication. Let E be an elliptic curve over a number field K. If the endomorphism ring $\mathrm{End}\,(E)$ is not isomorphic to $\mathbb{Z}$, then E has *complex multiplication*. In this case E has potential good reduction at every non-zero prime ideal in the maximal order $\mathcal{O}_K$ of K, see [62, Theorem II.6.1]. The ring $\mathrm{End}\,(E)$ is an order in a quadratic imaginary field L. Denote the maximal order of L by $\mathcal{O}_L$. If $\mathfrak{p} \subset \mathcal{O}_K$ is a prime ideal above p and E has good reduction at $\mathfrak{p}$, then the reduction of E at $\mathfrak{p}$ is supersingular if and only if the ideal (p) does not split in $\mathcal{O}_L$, see [38, Theorem 13.12]. Up to isomorphism there are only finitely many elliptic curves E

Table 2.1: A non-exhaustive list of complex multiplication by the order End (E) in a quadratic imaginary field L together with the corresponding j-invariant and the primes p such that $(p) \subset \mathcal{O}_L$ does not split.

End (E)	$j(E)$	
$\mathbb{Z}[\zeta_3]$	0	$p = 3$ or $p \equiv 2 \mod 3$
$\mathbb{Z}[i]$	$2^6 3^3$	$p = 2$ or $p \equiv 3 \mod 4$
$\mathbb{Z}\big[\frac{1}{2} + \frac{1}{2}\sqrt{-7}\big]$	$-3^3 5^3$	$p = 7$ or $p \equiv 3, 5, 6 \mod 7$
$\mathbb{Z}\big[\sqrt{-2}\big]$	$2^6 5^3$	$p = 2$ or $p \equiv 5, 7 \mod 8$

over $\mathbb{Q}$ with complex multiplication. The list of j-invariants can be found in [56, Appendix A.4] and [62, Appendix A.3]. Some of them are given in Table 2.1.

Given elliptic curves E_1 and E_2 over a field k of characteristic different from 2, we obtain a curve C over k by taking the fibre product of E_1 and E_2 along their x-coordinates, that is

$$\begin{tikzcd} C \arrow[r, "\pi_2"] \arrow[d, "\pi_1"'] & E_2 \arrow[d, "x_2"] \\ E_1 \arrow[r, "x_1"'] & \mathbb{P}^1. \end{tikzcd}$$

We assume that E_1 and E_2 have a unique point at infinity and that this point is the unit element of the group. In terms of function fields we have $k(E_i) = k(x_i, y_i)$ and $k(C) = k(x, y_1, y_2)$ with $x = x_1 = x_2$, $y_i^2 = f_i(x)$ and $f_i \in k[X]$ separable of degree 3. Denote the roots of f_i in $\bar{k}$ by α_{i1}, α_{i2} and α_{i3}. We want C geometrically irreducible, so f_1 is not a multiple of f_2 and $\deg(\pi_1) = 2$.

We compute the genus of C using the Hurwitz formula

$$2g(C) - 2 = \deg(\pi_1)(2g(E_1) - 2) + \sum_{P \in C(\bar{k})} (e_{\pi_1}(P) - 1).$$

The ramification index $e_{\pi_1}(P)$ can be read of from the divisor of $f_2(x_1)$ on E_1, because $k(C) = k(E_1)\Big(\sqrt{f_2(x_1)}\Big)$. Since $\operatorname{div}(f_2(x_1)) = x_1^*(\operatorname{div}(f_2(x)))$,

$$\operatorname{div}(f_2(x_1)) = \sum_{j=1}^{3} \left(\alpha_{2j}, \pm\sqrt{f_1(\alpha_{2j})}\right) - 6(O_1)$$

with $O_1 \in E_1(k)$ the point at infinity. A ramification point of π_1 corresponds to a point in the support of the above divisior and having odd multiplicity in the divisor. Hence if precisely 0, 1 or 2 of the roots of f_1 coincide with the roots of f_2, then the genus of C is 4, 3 or 2 respectively.

Assume that C has genus 2. In this case f_1 and f_2 share precisely two roots, say $\alpha_{11} = \alpha_{21}$ and $\alpha_{12} = \alpha_{22}$. So $f_i = \big(X^2 + aX + b\big)(X - c_i)$. Observe that $c_i \in k$, otherwise – using the minimal polynomial of c_i – the f_1 and f_2 have all roots in common. Thus also $a, b \in k$. We may assume that $a = 0$ by completing the square in $X^2 + aX + b$. Hence

$$E_i : y_i^2 = f_i(x_i) = \bigl(x_i^2 + b\bigr)(x_i - c_i)$$

for $i = 1, 2$. The j-invariant of E_i is

$$j(E_i) = 2^6 \frac{\bigl(3b - c_i^2\bigr)^3}{b\bigl(b + c_i^2\bigr)^2}.$$

Define $u = \frac{y_2}{y_1}$ and $v = y_1\bigl(1 - u^2\bigr)^2$ in $k(C)$. Then

$$x = x_1 = x_2 = \frac{c_2 - c_1 u^2}{1 - u^2} = c_2 + \frac{c_2 - c_1}{1 - u^2}$$

and

$$v^2 = (c_2 - c_1)\bigl(1 - u^2\bigr)\Bigl[\bigl(c_2 - c_1 u^2\bigr)^2 + b\bigl(1 - u^2\bigr)^2\Bigr].$$

Notice that $k(C) = k(u, v)$.

Proposition 2.1. *Let k be a field of characteristic different from 2. If $b, c_1, c_2 \in k$ such that $b \neq 0$, $c_1 \neq c_2$ and $c_i^2 + b \neq 0$, then the curve C given by*

$$v^2 = (c_2 - c_1)\bigl(1 - u^2\bigr)\Bigl[\bigl(c_2 - c_1 u^2\bigr)^2 + b\bigl(1 - u^2\bigr)^2\Bigr]$$

has genus 2 and

$$\pi_1 : C \longrightarrow E_1, \qquad (u, v) \longmapsto \left(\frac{c_2 - c_1 u^2}{1 - u^2}, \frac{v}{\bigl(1 - u^2\bigr)^2}\right)$$

$$\pi_2 : C \longrightarrow E_2, \qquad (u, v) \longmapsto \left(\frac{c_2 - c_1 u^2}{1 - u^2}, \frac{uv}{\bigl(1 - u^2\bigr)^2}\right)$$

are morphism to the elliptic curves E_i given by

$$y_i^2 = \bigl(x_i^2 + b\bigr)(x_i - c_i).$$

Moreover the Jacobian variety $\mathrm{Jac}\,(C)$ *of C is isogeneous to $E_1 \times E_2$.*

Proof. The inequalities $b \neq 0$, $c_1 \neq c_2$ and $c_i^2 + b \neq 0$ are equivalent to $X^2 + b$, $X - c_1$ and $X - c_2$ having distinct roots. The preceding discussion proves all but the last statement of Proposition 2.1.

The morphisms π_1 and π_2 induce a morphism

$${\pi_1}^* + {\pi_2}^* : E_1 \times E_2 \longrightarrow \mathrm{Jac}\,(C).$$

Since $E_1 \times E_2$ and $\mathrm{Jac}\,(C)$ both have dimension 2, it is sufficient to prove that ${\pi_1}^* + {\pi_2}^*$ is surjective. The morphism is surjective if and only if

$$(\pi_1, \pi_2)^* : \mathrm{H}^0\bigl(E_1, \Omega^1_{E_1}\bigr) \times \mathrm{H}^0\bigl(E_2, \Omega^1_{E_2}\bigr) \longrightarrow \mathrm{H}^0\bigl(C, \Omega^1_C\bigr)$$

is surjective. Since

$$\pi_1^*\left(\frac{dx_1}{y_1}\right) = 2(c_2 - c_1)\frac{udu}{v}$$
$$\pi_2^*\left(\frac{dx_2}{y_2}\right) = 2(c_2 - c_1)\frac{du}{v}$$

are linear independent, ${\pi_1}^* + {\pi_2}^*$ is indeed surjective. □

We introduce some notations which are used in each of the examples below. Let K be a number field of degree 1 or 2 over $\mathbb{Q}$. Denote the ring of integers of K by $\mathcal{O}_K$. Let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal above p. Notice that $\mathcal{O}_K/\mathfrak{p}$ is a field with p or p^2 elements. The constants $b, c_1, c_2 \in \mathcal{O}_K$ and the curves C, E_1, E_2 over K are as in the previous proposition. The reductions of C, E_1 and E_2 at $\mathfrak{p}$ are denoted by $C_\mathfrak{p}$, $E_{1,\mathfrak{p}}$ and $E_{2,\mathfrak{p}}$ respectively. If C, E_1 and E_2 have good reduction at $\mathfrak{p}$, then $C_\mathfrak{p}$ is maximal over $\mathbb{F}_{p^2}$ if and only if $E_{1,\mathfrak{p}}$ and $E_{2,\mathfrak{p}}$ are maximal over $\mathbb{F}_{p^2}$, because $\mathrm{Jac}\,(C_\mathfrak{p})$ and $E_{1,\mathfrak{p}} \times E_{2,\mathfrak{p}}$ are isogeneous over $\mathcal{O}_K/\mathfrak{p}$. Recall that if E is an elliptic curve defined over $\mathbb{F}_p$ and $p > 3$, then E is supersingular if and only if E is maximal over $\mathbb{F}_{p^2}$.

In our first example we choose E_1 and E_2 such that both have complex multiplication by $\mathbb{Z}[\zeta_3]$ with ζ_3 a primitive third root of unity. The result is essentially the same as [65, Example 4.2.3].

Proposition 2.2. *Let D be the curve over $\mathbb{Q}$ defined by*

$$v^2 = u^6 - 1$$

and $p \neq 2, 3$ a prime. The curve D has good reduction at p. The reduction of D at p is maximal over $\mathbb{F}_{p^2}$ if and only if $p \equiv 2 \mod 3$.

Proof. Let $K = \mathbb{Q}$ and $p \neq 2, 3$ a prime. Observe that $j(E_i) = 0$ if and only if $3b = c_i^2$. Choose $c_1 = 6$, $c_2 = -c_1$ and $b = \frac{1}{3}c_1^2$. The curve C is given by

$$v^2 = 2^6 3^2 \big(u^6 - 1\big).$$

Since $b = 12$, $c_1 - c_2 = 12$ and $c_i^2 + b = 48$, the curves C, E_1 and E_2 have good reduction at p. Define the curve D over $\mathbb{Q}$ by

$$v'^2 = u^6 - 1,$$

where $v' = \frac{v}{24}$. The curves C_p and D_p are isomorphic over $\mathbb{F}_p$.

The curve C_p is maximal over $\mathbb{F}_{p^2}$ if and only if $E_{1,p}$ and $E_{2,p}$ are maximal over $\mathbb{F}_{p^2}$. The elliptic curve $E_{i,p}$ is maximal over $\mathbb{F}_{p^2}$ precisely when $E_{i,p}$ is supersingular, because $E_{i,p}$ is defined over $\mathbb{F}_p$. Since E_i has complex multiplication by $\mathbb{Z}[\zeta_3]$, the elliptic curve $E_{i,p}$ is supersingular if and only if $p \equiv 2 \mod 3$, see Table 2.1.

Hence the curve D_p is maximal over $\mathbb{F}_{p^2}$ if and only if $p \equiv 2 \mod 3$. □

In the second example we let E_1 and E_2 be elliptic curves with complex multiplication by $\mathbb{Z}[\zeta_3]$ and $\mathbb{Z}[i]$ respectively.

Proposition 2.3. *Let D be the curve over $\mathbb{Q}$ defined by*

$$v^2 = \left(u^2-1\right)\left(4u^4-2u^2+1\right)$$

and let $p \neq 2,3$ be a prime. The curve D has good reduction at p. The reduction of D at p is maximal over $\mathbb{F}_{p^2}$ if and only if $p \equiv 11 \mod 12$.

Proof. Let $K = \mathbb{Q}$ and $p \neq 2,3$ a prime. Recall that $j(E_1) = 0$ if and only if $3b = c_1^2$. Observe that $j(E_2) = 2^6 3^3$ if and only if $c_2\left(9b+c_2^2\right) = 0$. Choose $c_1 = 3$, $c_2 = 0$ and $b = \frac{1}{3}c_1^2$. The curve C is given by

$$v^2 = 3^2\left(u^2-1\right)\left(4u^4-2u^2+1\right).$$

Since $b = 3$, $c_1 - c_2 = 3$, $c_1^2 + b = 12$ and $c_2^2 + b = 3$, the curves C, E_1 and E_2 have good reduction at p. Define the curve D over $\mathbb{Q}$ by

$$v'^2 = \left(u^2-1\right)\left(4u^4-2u^2+1\right),$$

where $v' = \frac{v}{3}$. The curves C_p and D_p are isomorphic over $\mathbb{F}_p$.

The curve C_p is maximal over $\mathbb{F}_{p^2}$ if and only if $E_{1,p}$ and $E_{2,p}$ are maximal over $\mathbb{F}_{p^2}$. Recall that $E_{1,p}$ is maximal over $\mathbb{F}_{p^2}$ if and only if $p \equiv 2 \mod 3$. Since E_2 has complex multiplication by $\mathbb{Z}[i]$, the elliptic curve $E_{2,p}$ is supersingular if and only if $p \equiv 3 \mod 4$. Thus $E_{2,p}$ is maximal over $\mathbb{F}_{p^2}$ if and only if $p \equiv 3 \mod 4$.

Hence the curve D_p is maximal over $\mathbb{F}_{p^2}$ if and only if $p \equiv 11 \mod 12$. □

We can also choose E_1 and E_2 such that they have complex multiplication by $\mathbb{Z}[\zeta_3]$ and $\mathbb{Z}\left[\frac{1}{2}+\frac{1}{2}\sqrt{-7}\right]$, but the genus 2 curve is no longer defined over $\mathbb{Q}$.

Proposition 2.4. *Let D be the curve over $K = \mathbb{Q}\left(\sqrt{21}\right)$ defined by*

$$v^2 = \left(u^2-1\right)\left(u^4-\left(\frac{1}{2}+\frac{3}{2}\sqrt{21}\right)u^2+16\right)$$

and $\mathfrak{p} \subset \mathcal{O}_K$ a prime ideal above $p \neq 2,3,5$. The curve D has good reduction at $\mathfrak{p}$. The reduction of D at $\mathfrak{p}$ is maximal over $\mathbb{F}_{p^2}$ if and only if $p \equiv 5,17,20 \mod 21$.

Proof. Let $K = \mathbb{Q}\left(\sqrt{21}\right)$ and $\mathfrak{p} \subset \mathcal{O}_K$ a prime ideal above $p \neq 2,3,5$. Recall that $j(E_1) = 0$ if and only if $3b = c_1^2$. Observe that $j(E_2) = -3^3 5^3$ if and only if $\left(63b - c_2^2\right)\left(81b^2 + 81bc_2^2 + 64c_2^4\right) = 0$. Choose $c_1 = 3\sqrt{21} - 3$, $c_2 = \sqrt{21}c_1$ and $b = \frac{1}{3}c_1^2$. The curve C is given by

$$v^2 = 2^2 3^2\left(1-\sqrt{21}\right)^4\left(u^2-1\right)\left[u^4-\left(\frac{1}{2}+\frac{3}{2}\sqrt{21}\right)u^2+16\right].$$

Since $b = 6\alpha$, $c_1 - c_2 = -6\alpha$, $c_1^2 + b = 24\alpha$ and $c_2^2 + b = 384\alpha$ with $\alpha = 11 - \sqrt{21}$, the curves C, E_1 and E_2 have good reduction at $\mathfrak{p}$. Let D over K be the curve

$$v'^2 = \left(u^2 - 1\right)\left[u^4 - \left(\frac{1}{2} + \frac{3}{2}\sqrt{21}\right)u^2 + 16\right],$$

where $v' = \frac{v}{12\alpha}$. The curves $C_\mathfrak{p}$ and $D_\mathfrak{p}$ are isomorphic over $\mathcal{O}_K/\mathfrak{p}$.

Observe that the elliptic curves $E_{1,\mathfrak{p}}$ and $E_{2,\mathfrak{p}}$ are defined over $\mathcal{O}_K/\mathfrak{p}$. Since E_1 has complex multiplication by $\mathbb{Z}[\zeta_3]$, the curve $E_{1,\mathfrak{p}}$ is supersingular if and only if $p \equiv 2 \mod 3$. Similar since E_2 has complex multiplication by $\mathbb{Z}\left[\frac{1}{2} + \frac{1}{2}\sqrt{-7}\right]$, the curve $E_{2,\mathfrak{p}}$ is supersingular if and only if $p = 7$ or $p \equiv 3, 5, 6 \mod 7$.

Suppose that $C_\mathfrak{p}$ is maximal over $\mathbb{F}_{p^2}$, that is $E_{1,\mathfrak{p}}$ and $E_{2,\mathfrak{p}}$ are maximal over $\mathbb{F}_{p^2}$. Thus $E_{1,\mathfrak{p}}$ and $E_{2,\mathfrak{p}}$ are supersingular. Hence $p \equiv 5, 17, 20 \mod 21$.

Suppose that $p \equiv 5, 17, 20 \mod 21$, that is $p \equiv 2 \mod 3$ and $p \equiv 3, 5, 6 \mod 7$, then $E_{1,\mathfrak{p}}$ and $E_{2,\mathfrak{p}}$ are supersingular. Notice that

$$\left(\frac{21}{p}\right) = \left(\frac{-3}{p}\right)\left(\frac{-7}{p}\right) = (-1)\cdot(-1) = 1,$$

because p is inert in $\mathbb{Z}[\zeta_3]$ and $\mathbb{Z}\left[\frac{1}{2} + \frac{1}{2}\sqrt{-7}\right]$. Thus the ideal $(p) \subset \mathcal{O}_K$ splits and $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_p$. Hence $E_{1,\mathfrak{p}}$ and $E_{2,\mathfrak{p}}$ are maximal over $\mathbb{F}_{p^2}$.

The curve $D_\mathfrak{p}$ is maximal over $\mathbb{F}_{p^2}$ if and only if $p \equiv 5, 17, 20 \mod 21$. □

Next we consider complex multiplication by $\mathbb{Z}[\zeta_3]$ and $\mathbb{Z}\left[\sqrt{-2}\right]$:

Proposition 2.5. *Let C be the curve over $K = \mathbb{Q}\left(\sqrt{-6}\right)$ defined by*

$$v^2 = \left(4 + 2\sqrt{-6}\right)\left(u^2 - 1\right)\left(4u^4 - 2\left(1 + \sqrt{-6}\right)u^2 - 1\right)$$

and $\mathfrak{p} \subset \mathcal{O}_K$ a prime ideal above $p \neq 2, 5$. The curve C has good reduction at $\mathfrak{p}$. The reduction of C at $\mathfrak{p}$ is maximal over $\mathbb{F}_{p^2}$ if and only if $p \equiv 5, 23 \mod 24$.

Proof. Let $K = \mathbb{Q}\left(\sqrt{-6}\right)$ and $\mathfrak{p} \subset \mathcal{O}_K$ a prime ideal above $p \neq 2, 5$. Recall that $j(E_1) = 0$ if and only if $3b = c_1^2$. Observe that $j(E_2) = 2^6 3^5$ if and only if

$$\left(2b + c_2^2\right)\left(49b^2 + 114bc_2^2 + c_2^4\right) = 0.$$

Choose $c_1 = -\sqrt{-6}$, $c_2 = 2$ and $b = -2$. The curve C is given by

$$v^2 = \left(4 + 2\sqrt{-6}\right)\left(u^2 - 1\right)\left(4u^4 - 2\left(1 + \sqrt{-6}\right)u^2 - 1\right).$$

Since $b = -2$, $c_1 - c_2 = -2 - \sqrt{-6}$, $c_1^2 + b = -8$ and $c_2^2 + b = 2$, the curves C, E_1 and E_2 have good reduction at $\mathfrak{p}$.

Since E_1 has complex multiplication by $\mathbb{Z}[\zeta_3]$, the curve $E_{1,\mathfrak{p}}$ is supersingular if and only if $p = 3$ or $p \equiv 2 \mod 3$. Similar since E_2 has complex multiplication by $\mathbb{Z}\left[\sqrt{-2}\right]$, the curve $E_{2,\mathfrak{p}}$ is supersingular if and only if $p \equiv 5, 7 \mod 8$.

Suppose that $C_\mathfrak{p}$ is maximal over $\mathbb{F}_{p^2}$, that is $E_{1,\mathfrak{p}}$ and $E_{2,\mathfrak{p}}$ are maximal over $\mathbb{F}_{p^2}$, then the elliptic curves are supersingular. Hence $p \equiv 5, 23 \mod 24$.

Suppose that $p \equiv 5 \mod 24$. The elliptic curves $E_{1,\mathfrak{p}}$ and $E_{2,\mathfrak{p}}$ are supersingular. Notice that

$$\left(\frac{-6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{-2}{p}\right)\left(\frac{-3}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot (-1) \cdot (-1) = 1,$$

because $p \equiv 5 \mod 8$ and p is inert in $\mathbb{Z}[\zeta_3]$ and $\mathbb{Z}\big[\sqrt{-2}\big]$. So the ideal $(p) \subset \mathcal{O}_K$ splits and $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_p$. Hence $E_{1,\mathfrak{p}}$ and $E_{2,\mathfrak{p}}$ are maximal over $\mathbb{F}_{p^2}$.

Suppose that $p \equiv 23 \mod 24$. Again the elliptic curves $E_{1,\mathfrak{p}}$ and $E_{2,\mathfrak{p}}$ are supersingular, but the ideal $(p) \subset \mathcal{O}_K$ is inert. Thus $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_{p^2}$. The curve $E_{1,\mathfrak{p}}$ is given by

$$y^2 = \big(x^2 - 2\big)\big(x + \sqrt{-6}\big) = i^3\Big(x'^2 + 2\Big)\Big(x' + \sqrt{6}\Big),$$

where $x = ix'$. Observe that $\zeta_8 \in \mathbb{F}_{p^2}$, because $p^2 \equiv 1 \mod 8$. So i is a square in $\mathbb{F}_{p^2}$. Also $\sqrt{6} \in \mathbb{F}_p$. Therefore $E_{1,\mathfrak{p}}$ is isomorphic (over $\mathbb{F}_{p^2}$) to an elliptic curve over $\mathbb{F}_p$. Hence $E_{1,\mathfrak{p}}$ is maximal over $\mathbb{F}_{p^2}$. The curve $E_{2,\mathfrak{p}}$ is defined over $\mathbb{F}_p$ and therefore maximal over $\mathbb{F}_{p^2}$.

Hence $C_\mathfrak{p}$ is maximal over $\mathbb{F}_{p^2}$ if and only if $p \equiv 5, 23 \mod 24$. □

The case of complex multiplication by $\mathbb{Z}[i]$ and $\mathbb{Z}[i]$:

Proposition 2.6. *Let D be the curve over $K = \mathbb{Q}$ defined by*

$$v^2 = \big(u^2 - 4\big)\big(u^4 + 10u^2 + 16\big)$$

and $p \neq 2, 3$ a prime. The curve D has good reduction at p. The reduction of D at p is maximal over $\mathbb{F}_{p^2}$ if and only if $p \equiv 3 \mod 4$.

Proof. Let $K = \mathbb{Q}$ and $p \neq 2, 3$ a prime. Recall that $j(E_i) = 2^6 3^3$ if and only if $c_i\big(9b + c_i^2\big) = 0$. Choose $c_1 = 9$, $c_2 = -c_1$ and $b = -\frac{1}{9}c_1^2$. The curve C is given by

$$v^2 = 3^4\big(u^2 - 1\big)\big(16u^4 + 40u^2 + 16\big).$$

Since $b = -9$, $c_1 - c_2 = 18$ and $c_i^2 + b = 72$, the curves C, E_1 and E_2 have good reduction at p. Define the curve D over $\mathbb{Q}$ by

$$v'^2 = \Big(u'^2 - 4\Big)\Big(u'^4 + 10u'^2 + 16\Big),$$

where $u' = 2u$ and $v' = \frac{2}{9}v$. The curves C_p and D_p are isomorphic over $\mathbb{F}_p$.

The remainder of the proof is analogous to the proof of Proposition 2.2 with complex multiplication by $\mathbb{Z}[i]$ instead. □

The case of complex multiplication by $\mathbb{Z}[i]$ and $\mathbb{Z}\big[\frac{1}{2} + \frac{1}{2}\sqrt{-7}\big]$:

Proposition 2.7. *Let D be the curve over $K = \mathbb{Q}$ defined by*

$$v^2 = \big(u^2 - 1\big)\big(u^4 - 2u^2 + 64\big)$$

and $p \neq 2, 3, 7$ a prime. The curve D has good reduction at p. The reduction of D at p is maximal over $\mathbb{F}_{p^2}$ if and only if $p \equiv 3, 19, 27 \mod 28$.

Proof. Let $K = \mathbb{Q}$ and $p \neq 2, 3, 7$ a prime. Recall that $j(E_1) = 2^6 3^3$ if and only if $c_1\bigl(9b + c_1^2\bigr) = 0$. Also recall that $j(E_2) = -3^3 5^3$ if and only if

$$\bigl(63b - c_2^2\bigr)\bigl(81b^2 + 81bc_2^2 + 64c_2^4\bigr) = 0.$$

Choose $c_1 = 0$, $c_2 = -63$ and $b = \frac{1}{63}c_2^2$. The curve C is given by

$$v^2 = 63^2\bigl(u^2 - 1\bigr)\bigl(u^4 - 2u^2 + 64\bigr).$$

Since $b = 63$, $c_1 - c_2 = 63$, $c_1^2 + b = 63$ and $c_2^2 + b = 2^6 3^2 7$, the curves C, E_1 and E_2 have good reduction at p. Define the curve D as

$$v'^2 = \bigl(u^2 - 1\bigr)\bigl(u^4 - 2u^2 + 64\bigr).$$

where $v' = \frac{v}{63}$. The curves C_p and D_p are isomorphic over $\mathbb{F}_p$.

The remainder of the proof is analogous to the proof of Proposition 2.3. □

The case of complex multiplication by $\mathbb{Z}[i]$ and $\mathbb{Z}\bigl[\sqrt{-2}\bigr]$:

Proposition 2.8. *Let D be the curve over $K = \mathbb{Q}$ defined by*

$$v^2 = \bigl(u^2 - 1\bigr)\bigl(u^4 - 2u^2 - 1\bigr)$$

and $p \neq 2$ a prime. The curve D has good reduction at p. The reduction of D at p is maximal over $\mathbb{F}_{p^2}$ if and only if $p \equiv 7 \mod 8$.

Proof. Let $K = \mathbb{Q}$ and $p \neq 2$ a prime. Recall that $j(E_1) = 2^6 3^3$ if and only if $c_1\bigl(9b + c_1^2\bigr) = 0$. Also recall that $j(E_2) = 2^6 5^3$ if and only if

$$\bigl(2b + c_2^2\bigr)\bigl(49b^2 + 114bc_2^2 + c_2^4\bigr) = 0.$$

Choose $c_1 = 0$, $c_2 = 2$ and $b = -\frac{1}{2}c_2^2$. The curve C is given by

$$v^2 = 2^2\bigl(u^2 - 1\bigr)\bigl(u^4 - 2u^2 - 1\bigr).$$

Since $b = -2$, $c_1 - c_2 = -2$, $c_1^2 + b = -2$ and $c_2^2 + b = 2$, the curves C, E_1 and E_2 have good reduction at p. Define the curve D as

$$v'^2 = \bigl(u^2 - 1\bigr)\bigl(u^4 - 2u^2 - 1\bigr).$$

where $v' = \frac{v}{2}$. The curves C_p and D_p are isomorphic over $\mathbb{F}_p$.

The remainder of the proof is analogous to the proof of Proposition 2.3. □

The case of complex multiplication by $\mathbb{Z}\bigl[\frac{1}{2} + \frac{1}{2}\sqrt{-7}\bigr]$ and $\mathbb{Z}\bigl[\frac{1}{2} + \frac{1}{2}\sqrt{-7}\bigr]$:

Proposition 2.9. *Let D be the curve over $K = \mathbb{Q}$ defined by*

$$v^2 = \bigl(u^2 - 1\bigr)\bigl(16u^4 + 31u^2 + 16\bigr)$$

and $p \neq 2, 3, 7$ a prime. The curve D has good reduction at p. The reduction of D at p is maximal over $\mathbb{F}_{p^2}$ if and only if $p \equiv 3, 5, 6 \mod 7$.

Proof. Let $K = \mathbb{Q}$ and $p \neq 2, 3, 7$ a prime. Recall that $j(E_i) = -3^3 5^3$ if and only if

$$\big(63b - c_2^2\big)\big(81b^2 + 81bc_2^2 + 64c_2^4\big) = 0.$$

Choose $c_1 = 2 \cdot 63$, $c_2 = -c_1$ and $b = \frac{1}{63}c_2^2$. The curve C is given by

$$v^2 = (8 \cdot 63)^2 \big(u^2 - 1\big)\big(16u^4 + 31u^2 + 16\big).$$

Since $b = 4 \cdot 63$, $c_1 - c_2 = 4 \cdot 63$ and $c_i^2 + b = 2^8 63$, the curves C, E_1 and E_2 have good reduction at p. Define the curve D as

$$v'^2 = \big(u^2 - 1\big)\big(16u^4 + 31u^2 + 16\big).$$

where $v' = \frac{v}{8 \cdot 63}$. The curves C_p and D_p are isomorphic over $\mathbb{F}_p$.

The remainder of the proof is analogous to the proof of Proposition 2.2. □

The case of complex multiplication by $\mathbb{Z}\big[\frac{1}{2} + \frac{1}{2}\sqrt{-7}\big]$ and $\mathbb{Z}\big[\sqrt{-2}\big]$:

Proposition 2.10. *Let C be the curve over $K = \mathbb{Q}\big(\sqrt{-14}\big)$ defined by*

$$v^2 = \big(4 + 6\sqrt{-14}\big)\big(u^2 - 1\big)\big(64u^4 - 2\big(1 + 3\sqrt{-14}\big)u^2 - 1\big)$$

and $\mathfrak{p} \subset \mathcal{O}_K$ a prime ideal above $p \neq 2, 5, 13$. The curve C has good reduction at $\mathfrak{p}$. The reduction of C at $\mathfrak{p}$ is maximal over $\mathbb{F}_{p^2}$ if and only if $p = 7$ or $p \equiv 5, 13, 31, 45, 47, 55 \mod 56$.

Proof. Let $K = \mathbb{Q}\big(\sqrt{-14}\big)$ and $\mathfrak{p} \subset \mathcal{O}_K$ a prime ideal above $p \neq 2, 5, 13$. Recall that $j(E_1) = -3^3 5^3$ if and only if $\big(63b - c_2^2\big)\big(81b^2 + 81bc_2^2 + 64c_2^4\big) = 0$. Also recall that $j(E_2) = 2^6 5^3$ if and only if

$$\big(2b + c_2^2\big)\big(49b^2 + 114bc_2^2 + c_2^4\big) = 0.$$

Choose $c_1 = -3\sqrt{-14}$, $c_2 = 2$ and $b = -2$. The curve C is given by

$$v^2 = \big(4 + 6\sqrt{-14}\big)\big(u^2 - 1\big)\big(64u^4 - 2\big(1 + 3\sqrt{-14}\big)u^2 - 1\big).$$

Since $b = -2$, $c_1 - c_2 = -2 - 3\sqrt{-14}$, $c_1^2 + b = -2^7$ and $c_2^2 + b = 2$, the curves C, E_1 and E_2 have good reduction at $\mathfrak{p}$.

The remainder of the proof is analogous to the proof of Proposition 2.5. □

The case of complex multiplication by $\mathbb{Z}\big[\sqrt{-2}\big]$ and $\mathbb{Z}\big[\sqrt{-2}\big]$:

Proposition 2.11. *Let D be the curve over $K = \mathbb{Q}$ defined by*

$$v^2 = \big(u^2 - 1\big)\big(u^4 + 6u^2 + 1\big)$$

and $p \neq 2$ a prime. The curve D has good reduction at p. The reduction of D at p is maximal over $\mathbb{F}_{p^2}$ if and only if $p \equiv 5, 7 \mod 8$.

Proof. Let $K = \mathbb{Q}$ and $p \neq 2$ a prime. Recall that $j(E_i) = 2^6 5^3$ if and only if

$$\big(2b + c_2^2\big)\big(49b^2 + 114bc_2^2 + c_2^4\big) = 0.$$

Choose $c_1 = 4$, $c_2 = -c_1$ and $b = -\frac{1}{2}c_1^2$. The curve C is given by

$$v^2 = 2^6\big(u^2 - 1\big)\big(u^4 + 6u^2 + 1\big).$$

Since $b = -8$, $c_1 - c_2 = 8$ and $c_i^2 + b = 8$, the curves C, E_1 and E_2 have good reduction at p. Define the curve D as

$$v'^2 = \big(u^2 - 1\big)\big(u^4 + 6u^2 + 1\big).$$

where $v' = \frac{v}{8}$. The curves C_p and D_p are isomorphic over $\mathbb{F}_p$.

The remainder of the proof is analogous to the proof of Proposition 2.2. □

Chapter 3

Hesse pencil and Galois action on 3-torsion

Let k be a perfect field of characteristic different from two and three. Denote the absolute Galois group of k by G_k. Given an elliptic curve E defined over k, we have a Galois representation on the 3-torsion group $E[3]$ of E. In this chapter we discuss a family of elliptic curves that have equivalent Galois representations on $E[3]$. Recall that the Galois representation on the 3-torsion of E and of another elliptic curve E' are equivalent if and only if $E[3]$ is isomorphic to $E'[3]$ as G_k-modules.

We introduce the notion of a symplectic homomorphism as in [37]. Let E and E' be elliptic curves defined over k and $\phi : E[3] \to E'[3]$ be a G_k-module homomorphism. If

$$e_3(S,T) = e_3'(\phi(S), \phi(T))$$

for all $S, T \in E[3]$ where e_3 and e_3' are the Weil-pairings on the 3-torsion of E and E' respectively, then ϕ is called a *symplectic* homomorphism, otherwise ϕ is called an *anti-symplectic* homomorphism.

Next we recall the definition of the Hessian of a polynomial. Let $F \in k[X,Y,Z]$ be a homogeneous polynomial of degree n. The *Hessian* $\operatorname{Hess}(F)$ of F is the determinant of the Hessian matrix of F, that is

$$\operatorname{Hess}(F) = \det \begin{pmatrix} \frac{\partial^2 F}{\partial X^2} & \frac{\partial^2 F}{\partial X \partial Y} & \frac{\partial^2 F}{\partial X \partial Z} \\ \frac{\partial^2 F}{\partial X \partial Y} & \frac{\partial^2 F}{\partial Y^2} & \frac{\partial^2 F}{\partial Y \partial Z} \\ \frac{\partial^2 F}{\partial X \partial Z} & \frac{\partial^2 F}{\partial Y \partial Z} & \frac{\partial^2 F}{\partial Z^2} \end{pmatrix},$$

which is either a homogeneous polynomial of degree $3n-6$ or zero.

Given a curve $C = Z(F)$ with $F \in k[X,Y,Z]$ homogeneous of degree three, the *Hesse pencil* of C is defined as

$$\mathcal{C} = Z(tF + \operatorname{Hess}(F))$$

over $k(t)$. Recall that the discrete valuations on $k(t)$ correspond to the points in $\mathbb{P}^1(k)$, where we usually write $(t_0 : 1)$ as t_0 and $(1 : 0)$ as ∞. We denote the reduced curve of $\mathcal{C}$ at $t_0 \in \mathbb{P}^1(k)$ by C_{t_0}. Notice that $C_\infty = C$ and for $t_0 \neq \infty$

$$C_{t_0} = Z(t_0 F + \mathrm{Hess}\,(F)).$$

In the special case that $C = E$ is an elliptic curve given by a Weierstrass equation, we have (see Section 3.1) that the point O at infinity is a point on E_{t_0} for every $t_0 \in \mathbb{P}^1(k)$. If E_{t_0} is a smooth curve, then this makes it an elliptic curve with unit element O.

The goal of this chapter is to prove the following theorem:

Theorem 3.1. *If E and E' are elliptic curves given by some Weierstrass equation defined over k, then $E_{t_0} \cong_k E'$ for some $t_0 \in \mathbb{P}^1(k)$ if and only if there exists a symplectic isomorphism $E[3] \to E'[3]$.*

In Sections 3.1, 3.2 and 3.3 we show that the 3-torsion groups of an elliptic curve in Weierstrass form and its Hesse pencil are identical not only as sets, but also have the same group structure and Weil-pairings. Using the Weierstrass form of the Hesse pencil computed in Section 3.4 and the relation between a linear change of coordinates and its restriction to the 3-torsion group described in Section 3.5, we prove in Section 3.6 that an isomorphism of the 3-torsion groups respecting the Weil-pairings is the restriction of a linear change of coordinates. The proof of the theorem is completed in Section 3.7. We compare our results with existing results in Section 3.9.

3.1 The flex points

Let $C = Z(F)$ be a curve with $F \in k[X, Y, Z]$ homogeneous of degree n and irreducible. A point P on C is called a *flex point* if there exists a line L such that the intersection number of C and L at P is at least three. Notice that in our definition P is allowed to be a singular point on C.

The *Hessian curve* of C is defined as $\mathrm{Hess}\,(C) = Z(\mathrm{Hess}\,(F))$.

Proposition 3.2. *If P is a point on C and* $\mathrm{char}\,(k) \nmid n - 1$*, then P is a flex point if and only if $P \in C \cap \mathrm{Hess}\,(C)$.*

Proof. See [18, Exercise 5.23]. □

From now on we will only work with curves of degree three, so the proposition above is only usable for fields k of characteristic different from two. This is the reason for why we exclude characteristic two in most of this chapter; see Section 3.8 for the excluded case.

Corollary 3.3. *If P is a flex point on C, then it is also a point on the Hesse pencil $\mathcal{C}$ and it is again a flex point.*

This is a well-known and old result in the case of $F = X^3 + Y^3 + Z^3$, see for example [51, Section VII.1].

Proof. A computation using Magma [4] shows that

$$\text{Hess}\,(tF + \text{Hess}\,(F)) = \alpha F + \beta \text{Hess}\,(F)$$

with $\alpha, \beta \in k[t]$.

Assume that P is a flex point, then $P \in C \cap \text{Hess}\,(C)$ by Proposition 3.2, that is $F(P) = 0$ and $\text{Hess}\,(F)(P) = 0$. So $(tF + \text{Hess}\,(F))(P) = 0$, which implies that $P \in \mathcal{C}$. The computation above also implies that

$$\text{Hess}\,(tF + \text{Hess}\,(F))(P) = 0,$$

that is $P \in \text{Hess}\,(\mathcal{C})$. Therefore $P \in \mathcal{C} \cap \text{Hess}\,(\mathcal{C})$. Hence P is a flex point on $\mathcal{C}$ by Proposition 3.2. □

Corollary 3.4. *Let $P \in C_{t_0} \cap C_{t_1}$. If $t_0 \neq t_1$, then P is a flex point on C.*

Proof. Suppose that $t_0 = (t_{00} : t_{01})$ and $t_1 = (t_{10} : t_{11})$, then

$$\begin{pmatrix} t_{00} & t_{01} \\ t_{10} & t_{11} \end{pmatrix} \begin{pmatrix} F(P) \\ \text{Hess}\,(F)(P) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

with the matrix being invertible since $t_0 \neq t_1$. Thus $F(P) = 0$ and $\text{Hess}\,(F)(P) = 0$, that is $P \in C \cap \text{Hess}\,(C)$. Hence Proposition 3.2 implies that P is a flex point on C. □

3.2 The 3-torsion group

Let $E = Z(F)$ be an elliptic curve with unit element O and $F \in k[X, Y, Z]$ homogeneous of degree 3.

Proposition 3.5. *Let S and T be points on E. If S is a flex point, then T is a flex point if and only if $S - T \in E[3]$.*

Proof. Let L_S and L_T be the tangent lines to E at S and T respectively.

Assume that T is also a flex point. Consider the function $\frac{L_S}{L_T}$ on E which has divisor $3(S) - 3(T)$. From [61, Corollary III.3.5] it follows that $3S - 3T = O$. Hence $S - T \in E[3]$.

Assume that T is not a flex point. Now the divisor of the function $\frac{L_S}{L_T}$ is $3(S) - 2(T) - (T')$ with $T' \neq T$. From this it follows that $3S - 2T - T' = O$, thus $3S - 3T = T' - T \neq O$. Hence $S - T \notin E[3]$. □

This result tells us that if O is a flex point on E, then the concepts of flex point and 3-torsion point coincide. In the previous section we learned that a flex point on E is also a flex point on $\mathcal{E}$. Hence if we combine these statements, then we obtain $E[3] \subset \mathcal{E}[3]$. Since the characteristic of k is different from three, these sets are equal in size, thus the same. Moreover suppose that E_{t_0} for some $t_0 \in \mathbb{P}^1(k)$ is non-singular. Provide $\mathcal{E}$ and E_{t_0} with a group structure by taking O as the unit element. Since the flex points of $\mathcal{E}$ and E_{t_0} are the same and a line that intersects an elliptic curve at two flex points will also intersect the curve at a third flex point, the group structures on $\mathcal{E}[3]$ and $E_{t_0}[3]$ are equal as well.

Recall that if the unit element O is a flex point on E, then we can find a projective linear transformation in $\mathrm{PGL}_3(k)$ such that E is given by a Weierstrass equation in the new coordinates. Moreover since the characteristic of k is different from two and three, we may even assume that $E : y^2 = x^3 + ax + b$ for some $a, b \in k$.

3.3 The Weil-pairing

In the previous section we saw that $\mathcal{E}[3] = E_{t_0}[3]$ for all $t_0 \in \mathbb{P}^1\big(\overline{k}\big)$ such that E_{t_0} is non-singular. Denote the Weil-pairing on the 3-torsion of $\mathcal{E}$ by e_3 and on the 3-torsion of E_{t_0} by $e_3^{t_0}$. An introduction to Weil-pairings can be found in [61, Section III.8] and [74, Sections 3.3 and 11.2].

Proposition 3.6. *Let E be an elliptic curve given by a Weierstrass equation and let $\mathcal{E}$ be its Hesse pencil. The Weil-pairings e_3 and $e_3^{t_0}$ on $E[3]$ are equal.*

Proof. Let $S, T \in E[3]$ generate $E[3]$. The Weil-pairing is determined by its value on (S, T). Follow [61, Exercise 3.16] to construct the Weil-pairings. Recall that O is a flex point on E.

Let L_O, L_S, L_T and L_{-T} be the tangent lines to $\mathcal{E}$ at O, S, T and $-T$ respectively. Define $D_S = (S) - (O)$ and $D_T = 2(T) - 2(-T)$. Notice that D_S and D_T have disjoint support. Since $2T - 2(-T) = T$ in $\mathcal{E}$, it follows that $D_T \sim (T) - (O)$. Consider the functions $f_S = \frac{L_S}{L_O}$ and $f_T = \left(\frac{L_T}{L_{-T}}\right)^2$, then $\operatorname{div}(f_S) = 3D_S$ and $\operatorname{div}(f_T) = 3D_T$. The Weil-pairing on $\mathcal{E}$ is defined as

$$\begin{aligned} e_3(S,T) &= \frac{f_S(D_T)}{f_T(D_S)} \\ &= \left(\frac{f_S(T)}{f_S(-T)}\right)^2 \frac{f_T(O)}{f_T(S)} \\ &= \left(\frac{L_S(T)L_O(-T)L_T(O)L_{-T}(S)}{L_O(T)L_S(-T)L_{-T}(O)L_T(S)}\right)^2. \end{aligned}$$

Let $s \in k(S,T)(t)$ be a local coordinate at t_0. Choose the equations of the tangent lines such that they are also defined over $k(S,T)[[s]]$ and are non-zero modulo s. Notice that L_O, L_S, L_T and L_{-T} modulo s are tangent lines to E_{t_0} at O, S, T and $-T$ respectively. Follow the construction above to obtain the Weil-pairing $e_3^{t_0}(S,T)$ on E_{t_0}.

Now $L_O(T)$ is a unit in $k(S,T)[[s]]$, because T is not contained in the tangent line L_O modulo s to E_{t_0} at O. Similarly the other terms in the expression of

$e_3(S,T)$ are units as well. Thus by construction $e_3(S,T) \bmod s = e_3^{t_0}(S,T)$. Recall that $e_3(S,T)$ is a root of unity. Hence $e_3 = e_3^{t_0}$. □

3.4 The Weierstrass form

Proposition 3.7. *Let E be an elliptic curve given by the Weierstrass equation $y^2z = x^3 + axz^2 + bz^3$ with $a, b \in k$. Then the Hesse pencil $\mathcal{E}$ can be given by*

$$ty^2z + 3xy^2 = tx^3 - 3ax^2z + (at - 9b)xz^2 + \left(bt + a^2\right)z^3$$

over $k(t)$. The linear change of coordinates

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = A \begin{pmatrix} \xi \\ \eta \\ \zeta \end{pmatrix} \quad \text{with} \quad A = \begin{pmatrix} t & 0 & 3at^2 - 27bt - 9a^2 \\ 0 & 1 & 0 \\ -3 & 0 & t^3 + 9at - 27b \end{pmatrix}$$

transforms this into the Weierstrass form $\mathcal{E}^W : \eta^2\zeta = \xi^3 + a_t\xi\zeta^2 + b_t\zeta^3$, with

$$\begin{aligned} a_t &= at^4 - 18bt^3 - 18a^2t^2 + 54abt - \left(27a^3 + 243b^2\right) \\ b_t &= bt^6 + 4a^2t^5 - 45abt^4 + 270b^2t^3 + 135a^2bt^2 \\ &\qquad + \left(108a^4 + 486ab^2\right)t - \left(243a^3b + 1458b^3\right). \end{aligned}$$

Moreover $\Delta\left(\mathcal{E}^W\right) = \Delta(E)(\det A)^3$ and $\det A = t^4 + 18at^2 - 108bt - 27a^2$.

Observe that the t in the proposition is equal to $8t$ in the previous sections.

Proof. The proof boils down to computing the map A, which can be found in three steps. First map the tangent line to $\mathcal{E}$ at O to the line at infinity. Next scale the z-coordinate so that the coefficient in front of x^3 and y^2z are equal up to minus sign. Finally shift the x-coordinate so that the x^2z term vanishes. □

This proposition shows that

$$j(\mathcal{E}) = 1728 \frac{4}{4a^3 + 27b^2} \left(\frac{at^4 - 18bt^3 - 18a^2t^2 + 54abt - \left(27a^3 + 243b^2\right)}{t^4 + 18at^2 - 108bt - 27a^2} \right)^3.$$

3.5 Linear change of coordinates I

Proposition 3.8. *Let $P_i \in \mathbb{P}^2(k)$ for $i = 1, ..., 4$ be points such that no three of them are collinear. If $Q_i \in \mathbb{P}^2(k)$ for $i = 1, ..., 4$ is another such set of points, then there exists a unique $A \in \mathrm{PGL}_3(k)$ such that $A(P_i) = Q_i$ for all $i = 1, ..., 4$.*

This is a well-known result. For convenience we include a proof. Observe that an analogous result holds for two sets of $n+2$ points in $\mathbb{P}^n(k)$ such that no $n+1$ of them lie on a hyperplane.

Proof. Recall that $A \in \mathrm{PGL}_3(k)$ can be represented by a $B \in \mathrm{GL}_3(k)$ which is unique up to a scalar multiple. Let $P_i = (x_i : y_i : z_i)$ and $Q_i = (\tilde{x}_i : \tilde{y}_i : \tilde{z}_i)$ for $i = 1, 2, 3, 4$. Define $u_i = (x_i, y_i, z_i)$ and $v_i = (\tilde{x}_i, \tilde{y}_i, \tilde{z}_i)$ for $i = 1, 2, 3, 4$. Then $A(P_i) = Q_i$ if and only if $Bu_i = \lambda_i v_i$ for some non-zero $\lambda_i \in k$.

The set $\{u_1, u_2, u_3\}$ is a basis of k^3 as the following argument shows: Suppose that u_1, u_2, u_3 are linearly dependent, that is $a_1u_1 + a_2u_2 + a_3u_3 = 0$ for some $a_1, a_2, a_3 \in k$ not all zero. In particular assume without loss of generality that $a_3 = -1$, then $u_3 = a_1u_1 + a_2u_2$. Let $L : b \cdot (x, y, z) = 0$ with $b \in k^3$ be the line containing P_1 and P_2, then $b \cdot u_3 = a_1 b \cdot u_1 + a_2 b \cdot u_2 = 0$, that is L contains P_3 as well, which is impossible by assumption. Hence $\{u_1, u_2, u_3\}$ is a basis of k^3.

Write $u_4 = \alpha_1u_1 + \alpha_2u_2 + \alpha_3u_3$ for some $\alpha_i \in k$. A reasoning along the same lines as above shows that each α_i must be non-zero. Similarly $\{v_1, v_2, v_3\}$ is a basis of k^3 and $v_4 = \beta_1v_1 + \beta_2v_2 + \beta_3v_3$ for some non-zero $\beta_i \in k$.

Let $B \in \mathrm{GL}_3(k)$ be such that u_i maps to $\frac{\beta_i}{\alpha_i}v_i$ for $i = 1, 2, 3$, then

$$Bu_4 = B\alpha_1u_1 + B\alpha_2u_2 + B\alpha_3u_3 = \beta_1v_1 + \beta_2v_2 + \beta_3v_3 = v_4.$$

Hence the induced $A \in \mathrm{PGL}_3(k)$ maps P_i to Q_i for $i = 1, 2, 3, 4$.

Suppose that $B' \in \mathrm{GL}_3(k)$ maps u_i to $\lambda_i v_i$ for $i = 1, 2, 3, 4$, then

$$\begin{aligned} \beta_1\lambda_4v_1 + \beta_2\lambda_4v_2 + \beta_3\lambda_4v_3 &= \lambda_4v_4 = B'u_4 \\ &= \alpha_1B'u_1 + \alpha_2B'u_2 + \alpha_3B'u_3 \\ &= \alpha_1\lambda_1u_1 + \alpha_2\lambda_2u_2 + \alpha_3\lambda_3u_3, \end{aligned}$$

so that $\lambda_i = \frac{\beta_i}{\alpha_i}\lambda_4$ for $i = 1, 2, 3$. Thus $B' = \lambda_4 B$ so that B and B' represent the same $A \in \mathrm{PGL}_3(k)$. Hence A is unique. □

Proposition 3.9. *Let E be an elliptic curve given by a Weierstrass equation defined over k. If $E[3] = \langle S, T\rangle$, then any line in $\mathbb{P}^2(\overline{k})$ contains at most two of the following points: O, S, T, $S + T$.*

Proof. Suppose that L is a line in $\mathbb{P}^2(\overline{k})$ containing three of the points O, S, T and $S + T$. Denote these by P_1, P_2 and P_3. Since E is given by a Weierstrass equation, O is a flex point, thus $P_1 + P_2 + P_3 = O$. However this is impossible for the points mentioned above. Hence such a line L does not exist. □

Suppose that we are given two elliptic curves E and E' as in the proposition above with $E[3] = \langle S, T\rangle$ and $E'[3] = \langle S', T'\rangle$, then Propositions 3.8 and 3.9 imply that there exists an $A \in \mathrm{PGL}_3(\overline{k})$ such that $O \mapsto O'$, $S \mapsto S'$, $T \mapsto T'$ and $S + T \mapsto S' + T'$ and that this A is unique.

3.6 Linear change of coordinates II

Proposition 3.10. *Let E and E' be elliptic curves given by a Weierstrass equation defined over k. If $\phi : E[3] \to E'[3]$ is an isomorphism which respects the Weil-pairings, then there exists a linear change of coordinates $\Phi : E_{t_0} \to E'$ for some $t_0 \in \mathbb{P}^1(\overline{k})$ such that $\Phi|_{E[3]} = \phi$.*

The essence of the proof of this proposition is the following: We determine the $t_i \in \mathbb{P}^1\big(\overline{k}\big)$ for which the j-invariant of E_{t_i} is equal to the j-invariant of E'. For each of these t_i's we obtain a number of linear changes of coordinates $E_{t_i} \to E$. A counting argument shows that ϕ is the restriction of one of those maps. The following observation is used in the counting argument:

Lemma 3.11. *Let E and E' be elliptic curves. Then 24 out of the 48 isomorphisms $E[3] \to E'[3]$ respect the Weil-pairings.*

Proof. Let $S, T \in E[3]$ be such that $E[3] = \langle S, T\rangle$ and $e_3(S,T) = \zeta_3$ with ζ_3 a fixed primitive third root of unity. Choose $S', T' \in E'[3]$ likewise. Since $E[3]$ and $E'[3]$ are two-dimensional vector spaces over $\mathbb{F}_3$, there exists a bijection

$$\begin{aligned} \mathrm{GL}_2(\mathbb{F}_3) &\longrightarrow \mathrm{Iso}\,(E[3], E'[3]) \\ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} &\longmapsto \phi_A(\alpha S + \beta T) = (\alpha a + \beta b)S' + (\alpha c + \beta d)T'. \end{aligned}$$

Notice that

$$\begin{aligned} e_3'(\phi_A(S), \phi_A(T)) &= e_3'(aS' + bT', cS' + dT') \\ &= e_3'(S', T')^{ad-bc} \\ &= \zeta_3^{\det A} \end{aligned}$$

So ϕ_A respects the Weil-pairings if and only if $\det A = 1$, that is $A \in \mathrm{SL}_2(\mathbb{F}_3)$. Now $|\mathrm{GL}_2(\mathbb{F}_3)| = 48$ and $[\mathrm{GL}_2(\mathbb{F}_3) : \mathrm{SL}_2(\mathbb{F}_3)] = 2$. Hence there are 48 isomorphisms $E[3] \to E'[3]$ of which 24 respect the Weil-pairings. □

Next we prove the proposition.

Proof of Proposition 3.10. Let j_0 and j_0' be the j-invariants of E and E' respectively. Denote the reduced curve of $\mathcal{E}^W$ at $t_0 \in \mathbb{P}^1\big(\overline{k}\big)$ by $E_{t_0}^W$. If $E_{t_0}^W$ is non-singular, then let $A_{t_0} : E_{t_0} \to E_{t_0}^W$ be the isomorphism induced by the linear change of coordinates A from Proposition 3.7 at t_0.

Assume that $j_0' \neq j_0, 0, 1728$. Consider the polynomial

$$\begin{aligned} G &= -1728(4a_t)^3 - j_0'\Delta\big(\mathcal{E}^W\big) \\ &= (j_0 - j_0')\Delta(E)\, t^{12} + 2^{13}3^6a^2b\, t^{11} + \ldots \end{aligned}$$

in $k[t]$, whose roots give $E_{t_0}^W$'s with j-invariant equal to j_0'. The polynomial G has degree 12 and its discriminant is

$$-3^{147}{j_0'}^8(j_0' - 1728)^6\Delta(E)^{44},$$

which is non-zero, so G has distinct roots $t_1, \ldots, t_{12}$ in $\overline{k}$. Since the j-invariant of $E_{t_i}^W$ is equal to j_0', there exists an isomorphism $\Psi_i : E_{t_i}^W \to E'$. An isomorphism respects the Weil-pairings, see [61, Proposition III.8.2] or [74, Theorem 3.9]. From

Sections 3.2 and 3.3 it follows that $E_{t_i}[3] = E[3]$ as groups with identical Weil-pairings. Therefore for every $i = 1, \dots, 12$ and $\sigma \in \mathrm{Aut}\,(E') \cong \mathbb{Z}/2\mathbb{Z}$

$$\phi_{i,\sigma} = (\sigma \circ \Psi_i \circ A_{t_i})|_{E_{t_i}[3]} : E[3] \to E'[3]$$

is an isomorphism respecting the Weil-pairings. Notice that $\sigma \circ \Psi_i \circ A_{t_i}$ is an element of $\mathrm{PGL}_3(\overline{k})$, because $E_{t_i}^W$ and E' are in Weierstrass form and A is a linear change of coordinates. All 24 isomorphisms $\phi_{i,\sigma}$ are distinct as the following argument shows. Suppose that $\phi_{i,\sigma} = \phi_{j,\tau}$, then $\sigma \circ \Psi_i \circ A_{t_i} = \tau \circ \Psi_j \circ A_{t_j}$ according to Section 3.5. Let $P \in E' \setminus E'[3]$, then $Q = (\sigma \circ \Psi_i \circ A_{t_i})^{-1}(P)$ is a point in $E_{t_i} \cap E_{t_j}$, so Corollary 3.4 implies that $t_i = t_j$, that is $i = j$. Since Ψ_i and A_{t_i} are isomorphisms, $\sigma = \tau$. Thus $\phi_{i,\sigma} = \phi_{j,\tau}$ if and only if $i = j$ and $\sigma = \tau$. Since the $\phi_{i,\sigma}$'s respect the Weil-pairings, Lemma 3.11 implies that these are all the possible isomorphisms $E[3] \to E'[3]$ that respect the Weil-pairings. Hence $\phi = \phi_{i,\sigma}$ for some $i = 1, \dots, 12$ and $\sigma \in \mathrm{Aut}\,(E')$, which proves the proposition in this case.

Suppose that $j_0' = j_0$ and $j_0' \neq 0, 1728$, then the G above has degree 11 and the discriminant of G is

$$-2^{130} 3^{195} a^{20} b^{10} \Delta(E)^{30},$$

which is again non-zero, so G has distinct roots $t_1, \dots, t_{11}$ in $\overline{k}$. In this case the j-invariant of E_∞ is also equal to j_0', so let $t_{12} = \infty$. The argument presented before now finishes the proof in this case.

Assume that $j_0' = 0$. This case is the same as before with the exception of the polynomial G, which in this case should be replaced by a_t. The four distinct t_i's and the six elements in $\mathrm{Aut}\,(E')$ again give 24 isomorphisms $\phi_{i,\sigma}$.

Finally, if $j_0' = 1728$, then replace G by b_t and proceed as before. □

3.7 Proof of the theorem

In the proof of Theorem 3.1 we need a result from Galois cohomology, namely:

Lemma 3.12. *If k is a perfect field, then* $\mathrm{PGL}_3(\overline{k})^{G_k} = \mathrm{PGL}_3(k)$.

Proof. Consider the short exact sequence of G_k-groups

$$1 \longrightarrow \overline{k}^* \longrightarrow \mathrm{GL}_3(\overline{k}) \longrightarrow \mathrm{PGL}_3(\overline{k}) \longrightarrow 1,$$

which induces the exact sequence in the first row of the diagram

$$\begin{tikzcd}
1 \arrow[r] & \overline{k}^{*G_k} \arrow[r] & \mathrm{GL}_3(\overline{k})^{G_k} \arrow[r] & \mathrm{PGL}_3(\overline{k})^{G_k} \arrow[r] & \mathrm{H}^1\left(G_k, \overline{k}^*\right) \\
1 \arrow[r] & k^* \arrow[r] \arrow[u] & \mathrm{GL}_3(k) \arrow[r] \arrow[u] & \mathrm{PGL}_3(k) \arrow[r] \arrow[u] & 1.
\end{tikzcd}$$

The second row is the definition of $\mathrm{PGL}_3(k)$ and the vertical maps are the inclusion maps. Hilbert's Theorem 90 gives that $\mathrm{H}^1\left(G_k, \overline{k}^*\right) = \{1\}$. Since $\overline{k}^{*G_k} = k^*$ and $\mathrm{GL}_3(\overline{k})^{G_k} = \mathrm{GL}_3(k)$, also $\mathrm{PGL}_3(\overline{k})^{G_k} = \mathrm{PGL}_3(k)$. □

Proof of Theorem 3.1. Assume that $\Phi : E_{t_0} \to E'$ for some $t_0 \in \mathbb{P}^1(k)$ is an isomorphism defined over k. This map respects the Weil-pairings according to [61, Proposition III.8.2]. So $\Phi|_{E_{t_0}[3]} : E_{t_0}[3] \to E'[3]$ is a symplectic isomorphism. In Sections 3.2 and 3.3 it was shown that $E[3] = E_{t_0}[3]$ as groups and have identical Weil-pairings. Thus $\Phi|_{E_{t_0}[3]}$ can be considered as a symplectic isomorphism $E[3] \to E'[3]$. Hence $\Phi|_{E_{t_0}[3]}$ is the desired map.

Suppose that there exists a symplectic isomorphism $\phi : E[3] \to E'[3]$, then Proposition 3.10 implies that there exists a $\Phi \in \mathrm{PGL}_3\bigl(\overline{k}\bigr)$ and a $t_0 \in \mathbb{P}^1\bigl(\overline{k}\bigr)$ such that $\Phi : E_{t_0} \to E'$ and $\phi = \Phi|_{E[3]}$. Since $\sigma \circ \phi = \phi \circ \sigma$ for all $\sigma \in G_k$,

$$\sigma(\Phi)(\sigma(S)) = \sigma \circ \Phi(S) = \sigma \circ \phi(S) = \phi \circ \sigma(S) = \Phi(\sigma(S))$$

for all $S \in E[3]$, so Propositions 3.8 and 3.9 imply that $\sigma(\Phi) = \Phi$. Therefore Lemma 3.12 implies that $\Phi \in \mathrm{PGL}_3(k)$. Hence $t_0 \in \mathbb{P}^1(k)$ and $E' \cong_k E_{t_0}$. □

3.8 Characteristic two

In this chapter we assumed k is a perfect field of characteristic different from two and three. Tuijp in [70] adapts the proof of Theorem 3.1 to characteristic two: She replaces the polynomial Hess$\,(F)$ by the 3-division polynomial of the elliptic curve, which is turned into a cubic in x and y by replacing x^4 by lower degree terms using the Weierstrass equation, see [70, Propositions 2.1 and 2.3]. Hence a result similar to Theorem 3.1 is true in characteristic two by a similar proof.

3.9 Comparison with the literature

Theorem 3.1 is part of a more general problem: Given an elliptic curve E over a field k and an integer n, describe the universal family of elliptic curves $\mathcal{E}$ such that for each member $\mathcal{E}_{t_0}$ the Galois representations on $E[n]$ and $\mathcal{E}_{t_0}[n]$ are isomorphic and the isomorphism is symplectic. For various n explicit families are known in the literature.

In [53] Rubin and Silverberg construct for any elliptic curve over $\mathbb{Q}$ such an explicit family for $n = 3$ and $n = 5$. Their proofs are motivated by the theory of modular curves. Our Theorem 3.1 corresponds roughly to [53, Theorem 4.1] and [53, Remark 4.2].

Using invariant theory and a generalization of the classical Hesse pencil, Fisher in [17] describes such families for elliptic curves defined over a perfect field of characteristic not dividing $6n$ with $n = 2, 3, 4, 5$. Theorem 3.1 is a special case of [17, Theorem 13.2]. It is unclear whether Fisher's proof of [17, Theorem 13.2] can be adapted to the case of characteristic two. Tuijp in [70] showed that the argument in this chapter is adaptable to characteristic two.

The Hesse pencil is also used by Kuwata in [37]. For any elliptic curve E over a number field he constructs two families of elliptic curves such that for each member the Galois representation on its 3-torsion is equivalent to the one on $E[3]$. In the first family the isomorphism of the 3-torsion groups is symplectic, whereas in the second family the isomorphism is anti-symplectic. The proofs use classical projective geometry and the classification of rational elliptic surfaces. Theorem 3.1 is essentially [37, Theorem 4.2]. Notice that the Weierstrass form of the Hesse pencil in [37, Remark 4.4] is the same as the one in Proposition 3.7 with t replaced by t^{-1} and the x and y coordinates scaled by some power of t.

An overview of the classical Hesse pencil is given by Artebani and Dolgachev in [1].

Chapter 4

Jacobian variety of the Mestre curve

Mestre in [44] constructed from two given elliptic curves a hyperelliptic curve admitting independent morphisms to the two given curves. The resulting curve is used by Stewart and Top in [67, Theorem 3] to construct a family of twists of a given elliptic curve over $\mathbb{Q}$ such that infinitely many members have Mordell-Weil rank at least two. In this chapter we show that the rank is in general at most two by studying the Jacobian variety of the Mestre curve.

We briefly recall the construction of a family of twists of a given elliptic curve E described in [67]. Let E be an elliptic curve over a field k of characteristic different from 2 and 3. Suppose that $j(E) \neq 0, 1728$ and $y^2 = x^3 + ax + b$ is a short Weierstrass equation for E. Let $f \in k[S]$ be a separable polynomial and let C be the hyperelliptic curve over k corresponding to the function field $k(s,t)$ with $t^2 = f(s)$. In this case a (quadratic) *twist* E_d of E is the elliptic curve over k given by the equation $dy^2 = x^3 + ax + b$ with $d \in k^*$ unique up to squares, see [61, Proposition X.5.4]. The family of twists of E is constructed by specifying a set of d's, namely the values of $f(s_0)$ for $s_0 \in k$. In other words the twists are obtained from $E_{f(s)}$ by specialization. The specialization map

$$E_{f(s)}(k(s)) \longrightarrow E_{f(s_0)}(k(s_0))$$

is an injective homomorphism for all but finitely many $s_0 \in k$, see [60, Theorem C]. Hence the rank of the twists is related to the rank of $E_{f(s)}(k(s))$.

The rank of $E_{f(s)}(k(s))$ is closely related to the decomposition of the Jacobian variety $\operatorname{Jac}(C)$ of C into simple abelian varieties, which we will illustrate now. Notice that $E_{f(s)}$ is isomorphic over $k(C)$ to E, via $(x,y) \mapsto (x,ty)$. The group

$E(k(C))$ is isomorphic to $\mathrm{Mor}_k(C, E)$. Moreover

$$\begin{tikzcd}
E_{f(s)}(k(C)) \arrow[r] & E(k(C)) \arrow[r] & \mathrm{Mor}_k(C, E) \\
E_{f(s)}(k(s)) \arrow[r] \arrow[u] & \{P : \iota^*(P) = -P\} \arrow[r] \arrow[u] & \{\phi : \phi \circ \iota = [-1] \circ \phi\} \arrow[u]
\end{tikzcd}$$

is a commutative diagram with $\iota : C \to C$ the hyperelliptic involution, the horizontal maps isomorphims and vertical maps inclusions. The Albanese property of $\mathrm{Jac}\,(C)$ implies that

$$\mathrm{Mor}_{k,\Delta}(C \times C, E) := \{\psi \in \mathrm{Mor}_k(C \times C, E) : \psi \circ \Delta = 0\} \cong \mathrm{Hom}_k(\mathrm{Jac}\,(C), E)$$

with $\Delta : C \to C \times C$ the diagonal morphism, see [46, Proposition 6.4]. Consider the homomorphism $\mathrm{Mor}_k(C, E) \to \mathrm{Mor}_{k,\Delta}(C \times C, E)$ defined as

$$\phi \longmapsto ((P_1, P_2) \mapsto \phi(P_1) - \phi(P_2)).$$

We obtain the following commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & E(k) \arrow[r] & \mathrm{Mor}_k(C, E) \arrow[r] & \mathrm{Mor}_{k,\Delta}(C \times C, E) \\
0 \arrow[r] & E(k)[2] \arrow[r] \arrow[u] & \{\phi : \phi \circ \iota = [-1] \circ \phi\} \arrow[r] \arrow[u] & \{\psi : \psi \circ (\iota \times \iota) = [-1] \circ \psi\} \arrow[u]
\end{tikzcd}$$

with exact rows and vertical inclusions. Observe that the condition $\psi \circ (\iota \times \iota) = [-1] \circ \psi$ is empty, because C is hyperelliptic. Let l be a finite Galois extension of k such that C has a l-rational point. The corresponding sequence for l

$$0 \longrightarrow E(l)[2] \longrightarrow \{\varphi : \varphi \circ \iota = [-1] \circ \varphi\} \longrightarrow \mathrm{Mor}_{l,\Delta}(C \times C, E) \longrightarrow 0$$

is a short exact sequence of $\mathrm{Gal}\,(l/k)$-modules. Since $\mathrm{Gal}\,(l/k)$ and $E(l)[2]$ are finite groups, the group $\mathrm{H}^1(\mathrm{Gal}\,(l/k), E(l)[2])$ is also finite. From the long exact sequence from Galois cohomology follows that

$$\mathrm{rank}\,\{\phi : \phi \circ \iota = [-1] \circ \phi\} = \mathrm{rank}\,\mathrm{Mor}_{k,\Delta}(C \times C, E).$$

Hence the rank of $E_{f(s)}(k(s))$ is equal to the rank of $\mathrm{Hom}_k(\mathrm{Jac}\,(C), E)$, which is equal to number of factors isogeneous over k to E in the decomposition of $\mathrm{Jac}\,(C)$ into simple abelian varieties.

We recall the construction of the Mestre curve in Section 4.1. In Section 4.2 we compute automorphisms of this curve and use them in Section 4.3 to decompose the Jacobian variety of the Mestre curve. We show in Section 4.4 that a 2-dimensional factor of the Jacobian variety of the Mestre curve is geometrically simple for $k = \mathbb{Q}(a, b)$ a function field over $\mathbb{Q}$ in two variables, but in Section 4.5 we find pairs $a, b \in \mathbb{Q}$ for which this factor most likely is not simple.

4.1 Mestre curve

We recall the construction of a hyperelliptic curve described in [44, Theorem 3] and derive an affine model for a special case as was done in [49, Section 4.2].

Let k be a field of characteristic different from 2 and 3. Suppose that E and E' are elliptic curves over k with j-invariant not both equal to 0 or 1728. Choose short Weierstrass equations $y^2 = f(x)$ and ${y'}^2 = f'(x')$ for E and E' respectively, where

$$f(x) = x^3 + ax + b$$
$$f'(x') = {x'}^3 + a'x' + b'$$

with $a, b, a', b' \in k$. Proceed as if these curves are isomorphic over k, that is there exists a u such that $x' = u^2 x$ and $y' = u^3 y$. Substitute these relations into the equations above to obtain

$$f'\left(u^2 x\right) = \left(u^3 y\right)^2 = u^6 y^2 = u^6 f(x).$$

Since the degree two terms in f and f' are zero, the equation can be rewritten as $x = \rho(u)$ with

$$\rho(u) = -\frac{bu^6 - b'}{au^6 - a'u^2}.$$

The assumptions on the j-invariants guarantee ρ is well-defined and non-zero. The curve C is defined by $y^2 = f \circ \rho(u)$ and it comes with the obvious maps $\pi : C \to E$ and $\pi' : C \to E'$.

The curve C is called the *Mestre curve* if $E = E'$. Restricting to this case and using the change of coordinates from [49, Subsection 4.2.2] with a different constant, that is $v = a^2\left(u^2+1\right)^2 u^3 y$, we obtain the following equation for C

$$v^2 = g_{ab}(u) := -ab\left(u^2+1\right)\left[b^2\left(u^4+u^2+1\right)^3 + a^3\left(u^2+1\right)^2 u^4\right].$$

The discriminant of g_{ab} is $-2^{14}a^{50}b^{50}\left(4a^3+27b^2\right)^6$. In this case the morphisms $\pi : C \to E$ and $\pi' : C \to E$ become

$$(u, v) \longmapsto \left(-\frac{b}{a}\frac{u^4+u^2+1}{\left(u^2+1\right)u^2}, \frac{1}{a^2}\frac{v}{\left(u^2+1\right)^2 u^3}\right)$$

and

$$(u, v) \longmapsto \left(-\frac{b}{a}\frac{u^4+u^2+1}{u^2+1}, \frac{1}{a^2}\frac{v}{\left(u^2+1\right)^2}\right)$$

respectively.

Unfortunately the construction does not seem to work in characteristic 2 and 3, because in these characteristics elliptic curves need not have a short Weierstrass equation as above. One can try the alternative short forms of the Weierstrass as given in [61, Proposition A.1.1]. In characteristic 3 and non-zero j-invariant one obtains a relation $x^2 = \tilde{\rho}(u)$, which is non-linear in x. In characteristic 2 it is unclear what the equivalent of $x = \rho(u)$ should be.

4.2 Galois theory

We will compute automorphisms of the Mestre curve C to obtain morphisms from C to curves of lower genus. In the next section we use these to decompose $\operatorname{Jac}(C)$ into a product of lower dimensional abelian varieties.

The automorphisms of C include the hyperelliptic involution and one derived in [49, Subsection 4.2.1]. Using Magma for the case $a = 1$ and $b = 1$ over $\mathbb{Q}$, we find eight automorphisms of C which as a group is isomorphic to the dihedral group $D_4 = \left\langle \rho, \sigma : \rho^4 = 1, \sigma^2 = 1, \sigma\rho\sigma = \rho^{-1} \right\rangle$ with $\rho : C \to C$ and $\sigma : C \to C$ given by

$$(u, v) \longmapsto \left(-\frac{1}{u}, -\frac{v}{u^7} \right)$$

and

$$(u, v) \longmapsto (-u, -v)$$

respectively. Notice that ρ^2 is equal to the hyperelliptic involution. In fact these morphisms define automorphisms of C in general. Hence $\operatorname{Aut}(C)$ contains a subgroup isomorphic to D_4.

Given a subgroup $H \subset D_4$, we get a curve C_H and a morphism $\pi_H : C \to C_H$. If H contains the hyperelliptic involution, then C_H is isomorphic to $\mathbb{P}^1$. If H does not contain the hyperelliptic involution, then H must be equal to $\langle \sigma \rangle$, $\left\langle \rho^2\sigma \right\rangle$, $\langle \rho\sigma \rangle$ or $\left\langle \rho^3\sigma \right\rangle$. The first two subgroups are conjugate subgroups (by ρ), so the corresponding C_H's are isomorphic. The same applies to the latter two subgroups.

The curve $C_{\langle \sigma \rangle}$ is given by the equation

$$\eta^2 = h_{ab}(\xi) := -ab\xi(\xi + 1)\left[b^2\left(\xi^2 + \xi + 1\right)^3 + a^3(\xi + 1)^2\xi^2 \right]$$

and the morphism $\pi_{\langle \sigma \rangle} : C \to C_{\langle \sigma \rangle}$ is given by $(u, v) \mapsto \left(u^2, uv\right)$[1]. The discriminant of h_{ab} is equal to $-a^{26}b^{28}\left(4a^3 + 27b^2\right)^3$.

The curve $C_{\langle \rho\sigma \rangle}$ is given by the equation

$$\tilde{\eta}^2 = \tilde{h}_{ab}\left(\tilde{\xi}\right) := -ab\tilde{\xi}\left(\tilde{\xi} - 2\right)\left[b^3\left(\tilde{\xi}^2 - 1\right)^3 + a^3\tilde{\xi}^2 \right]$$

and the morphism $\pi_{\langle \rho\sigma \rangle} : C \to C_{\langle \rho\sigma \rangle}$ sends $(u, v) \mapsto \left(u + \frac{1}{u}, \frac{u-1}{u^4}v\right)$. In this case the discriminant of $\tilde{h}_{ab}$ is $2^8a^{26}b^{26}\left(4a^3 + 27b^2\right)^4$.

We repeat the same procedure for $C_{\langle \sigma \rangle}$. The automorphism group of $C_{\langle \sigma \rangle}$ contains a subgroup of four elements generated by the hyperelliptic involution ι and the morphism $\alpha : C_{\langle \sigma \rangle} \to C_{\langle \sigma \rangle}$ given by $(\xi, \eta) \mapsto (-\xi - 1, \eta)$.

Consider the subgroup $\langle \alpha \rangle$. In this case $C_{\langle \sigma \rangle, \langle \alpha \rangle}$ is simply the curve E and the morphism $\pi_{\langle \sigma \rangle, \langle \alpha \rangle} : C_{\langle \sigma \rangle} \to E$ is given by

$$(\xi, \eta) \longmapsto \left(-\frac{b}{a}\frac{\xi^2 + \xi + 1}{\xi^2 + \xi}, \frac{1}{a^2}\frac{\eta}{\xi^2(\xi + 1)^2} \right).$$

[1] The curve $C_{\langle \sigma \rangle}$ and the morphism $\pi_{\langle \sigma \rangle}$ correspond to the curve C' and π_1' in the proof of [49, Proposition 4.8]

Notice that $\pi : C \to E$ statisfies $\pi = \pi_{\langle\sigma\rangle,\langle\alpha\rangle} \circ \pi_{\langle\sigma\rangle}$.

The subgroup $\langle \iota \circ \sigma\rangle$ corresponds to the curve $C_{\langle\sigma\rangle,\langle\iota\circ\alpha\rangle}$ given by

$$y'^2 = \bigl(x^3 + ax + b\bigr)(ax + b)(ax - 3b)$$

and the morphism $\pi_{\langle\sigma\rangle,\langle\iota\circ\alpha\rangle} : C_{\langle\sigma\rangle} \to C_{\langle\sigma\rangle,\langle\iota\circ\alpha\rangle}$ is given by

$$(\xi, \eta) \longmapsto \left(-\frac{b}{a}\frac{\xi^2 + \xi + 1}{\xi^2 + \xi}, \frac{b}{a^2}\frac{\eta}{\xi^3\langle\xi + 1\rangle^3} \right).$$

The discriminant is $-16a^2b^{10}\bigl(4a^3 + 27b^2\bigr)^3$.

We also repeat the above procedure for $C_{\langle\rho\sigma\rangle}$ and $C_{\langle\sigma\rangle,\langle\iota\circ\alpha\rangle}$, but only find the identity morphism and the hyperelliptic involution. Hence we do not find new morphims to curves of lower genus.

4.3 Idempotent relations

The automorphisms of C induce idempotent relations on the Jacobian variety $\mathrm{Jac}\,(C)$ of C and thereby possibly decompose $\mathrm{Jac}\,(C)$ into a product of abelian varieties, see for example [32].

We apply this method to C. Recall that D_4 is a subgroup of the automorphism group of C. This group admits the partition

$$D_4 = \langle\rho\rangle \cup \langle\sigma\rangle \cup \langle\rho\sigma\rangle \cup \bigl\langle\rho^2\sigma\bigr\rangle \cup \bigl\langle\rho^3\sigma\bigr\rangle.$$

Using [32, Theorem B] we find that $\mathrm{Jac}\,(C)^4 \times \mathrm{Jac}\,(C_{D_4})^8$ is isogeneous to

$$\mathrm{Jac}\,\bigl(C_{\langle\rho\rangle}\bigr)^4 \times \mathrm{Jac}\,\bigl(C_{\langle\sigma\rangle}\bigr)^2 \times \mathrm{Jac}\,\bigl(C_{\langle\rho\sigma\rangle}\bigr)^2 \times \mathrm{Jac}\,\bigl(C_{\langle\rho^2\sigma\rangle}\bigr)^2 \times \mathrm{Jac}\,\bigl(C_{\langle\rho^3\sigma\rangle}\bigr)^2.$$

Recall that C_{D_4} and $C_{\langle\rho\rangle}$ are isomorphic $\mathbb{P}^1$, so their Jacobian varieties are trivial. Also $C_{\langle\sigma\rangle} \cong C_{\langle\rho^2\sigma\rangle}$ and $C_{\langle\rho\sigma\rangle} \cong C_{\langle\rho^3\sigma\rangle}$. Hence the Poincaré Irreducibility Theorem (see [45, Proposition 12.1]) implies that

$$\mathrm{Jac}\,(C) \sim \mathrm{Jac}\,\bigl(C_{\langle\sigma\rangle}\bigr) \times \mathrm{Jac}\,\bigl(C_{\langle\rho\sigma\rangle}\bigr).$$

Instead we can also apply [32, Theorem B] to the subgroup $\bigl\langle\rho^2, \sigma\bigr\rangle$, which gives

$$\mathrm{Jac}\,(C)^2 \times \mathrm{Jac}\,\bigl(C_{\langle\rho^2,\sigma\rangle}\bigr)^4 \sim \mathrm{Jac}\,\bigl(C_{\langle\rho^2\rangle}\bigr)^2 \times \mathrm{Jac}\,\bigl(C_{\langle\sigma\rangle}\bigr)^2 \times \mathrm{Jac}\,\bigl(C_{\langle\rho^2\sigma\rangle}\bigr)^2.$$

Similar to before, this reduces to

$$\mathrm{Jac}\,(C) \sim \mathrm{Jac}\,\bigl(C_{\langle\sigma\rangle}\bigr)^2.$$

Observe that $\mathrm{Jac}\,\bigl(C_{\langle\sigma\rangle}\bigr)$ and $\mathrm{Jac}\,\bigl(C_{\langle\rho\sigma\rangle}\bigr)$ are in fact isogeneous by the Poincaré Irreducibility Theorem.

Now we apply the same method to $C_{\langle\sigma\rangle}$. Recall that $\langle\iota,\alpha\rangle$ is a subgroup of the automorphism group of $C_{\langle\sigma\rangle}$. Using [32, Theorem B] we find that

$$\mathrm{Jac}\left(C_{\langle\sigma\rangle}\right)^2 \times \mathrm{Jac}\left(C_{\langle\sigma\rangle,\langle\iota,\alpha\rangle}\right)^4 \sim \mathrm{Jac}\left(C_{\langle\sigma\rangle,\langle\iota\rangle}\right)^2 \times \mathrm{Jac}\left(C_{\langle\sigma\rangle,\langle\alpha\rangle}\right)^2 \times \mathrm{Jac}\left(C_{\langle\sigma\rangle,\langle\iota\alpha\rangle}\right)^2$$

Notice that $C_{\langle\sigma\rangle,\langle\iota,\alpha\rangle}$ and $C_{\langle\sigma\rangle,\langle\iota\rangle}$ are isomorphic to $\mathbb{P}^1$. Also $C_{\langle\sigma\rangle,\langle\alpha\rangle} \cong E$. So

$$\mathrm{Jac}\left(C_{\langle\sigma\rangle}\right) \sim E \times \mathrm{Jac}\left(C_{\langle\sigma\rangle,\langle\iota\alpha\rangle}\right).$$

To summarize:

Proposition 4.1. *The Jacobian variety of C is isogeneous over k to*

$$E^2 \times \mathrm{Jac}\left(C_{\langle\sigma\rangle,\langle\iota\alpha\rangle}\right)^2.$$

Proof. Combine the isogenies from the previous discussion. Notice that all the isogenies above are defined over k, because the mentioned automorphisms of C and $C_{\langle\sigma\rangle}$ are defined over k. □

4.4 Geometrically simple

In this section we show that the Jacobian variety of $D := C_{\langle\sigma\rangle,\langle\iota\alpha\rangle}$ is in general simple. More concretely, we restrict to $k = \mathbb{Q}(a,b)$ and show that D is simple over any finite extension of $\mathbb{Q}(a,b)$.

We view the curve D as the generic fibre of the family of curves

$$\mathcal{D} \longrightarrow D\big(ab\big(4a^3+27b^2\big)\big) \subset \mathbb{A}^2,$$

where $D(f) = \mathbb{A}^2 \setminus Z(f)$. If the Jacobian variety of some special fibre, say the curve D_{a_0,b_0} above the closed point (a_0,b_0), is simple, then $\mathrm{Jac}\,(D)$ is also simple. Similarly we can view D_{a_0,b_0} as the generic fibre of a family of curves

$$\mathcal{D}_{a_0,b_0} \longrightarrow \mathrm{Spec}\left(\mathbb{Z}_{(p)}\right)$$

for some prime $p \in \mathbb{Z}$. Again if the Jacobian variety of the special fibre $D_{a_0,b_0,p}$ over $\mathbb{F}_p$ is simple, then so is $\mathrm{Jac}\,(D_{a_0,b_0})$. In the case of an abelian variety over a finite field, an irreducible characteristic polynomial of Frobenius implies that the variety is simple. Combine the previous three steps and we obtain a method to show that the Jacobian variety of D is in general simple.

Proposition 4.2. *The Jacobian variety of $D_{1,1,17}$ is geometrically simple.*

The proof of the proposition is similar to the proof of [21, Proposition 2].

Proof. Recall that $D_{1,1}$ is the hyperelliptic curve over $\mathbb{Q}$ defined by

$$y^2 = \big(x^3+a_0x+b_0\big)(a_0x+b_0)(a_0x-3b_0)$$

with $a_0 = 1$ and $b_0 = 1$. Since the discriminant of the right-hand side equals $-2^4 31^3$, the curve $D_{1,1}$ has good reduction at $p = 17$. Denote the reduction $D_{1,1,17}$ of $D_{1,1}$ at $p = 17$ by $\bar{D}$.

Suppose that $\operatorname{Jac}(\bar{D})$ is not geometrically simple, then for some finite extension k of $\mathbb{F}_{17}$ the abelian variety $\operatorname{Jac}(\bar{D}_k)$ is isogeneous to a product of two elliptic curves. The characteristic polynomial of Frobenius on $\bar{D}$ is $\chi = t^4 + 2t^3 + 18t^2 + 34t + 289$, which is irreducible over $\mathbb{Q}$. Let $\pi \in \bar{\mathbb{Q}}$ be a root of χ. Then π^n with $n = [k : \mathbb{F}_{17}]$ is a root of the reducible characteristic polynomial of Frobenius on $\bar{D}_k$. Thus $\mathbb{Q}(\pi^n)$ is a proper subfield of $\mathbb{Q}(\pi)$. The proper subfields of $\mathbb{Q}(\pi)$ are $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{17})$. So $\mathbb{Q}(\pi^n) \subset \mathbb{Q}(\sqrt{17})$. Consider an embedding $\mathbb{Q}(\pi) \to \mathbb{C}$. According to the Weil conjectures $|\pi| = \sqrt{17}$. Since $\pi^n \in \mathbb{Q}(\sqrt{17}) \to \mathbb{R}$ implies $\pi^n = \pm\sqrt{17}^n$, $\frac{\pi}{\sqrt{17}}$ is a root of unity. However the minimal polynomial of $\frac{\pi}{\sqrt{17}}$ is $t^4 + 2t^3 + \frac{50}{17}t^2 + 2t + 1$, which is not a cyclotomic polynomial. □

Corollary 4.3. *The Jacobian variety of the curve D over $\mathbb{Q}(a, b)$ is also geometrically simple.*

4.5 Computer search

Although the Jacobian variety of D over $\mathbb{Q}(a, b)$ is geometrically simple, it may happen that for certain pairs a_0, b_0 the Jacobian variety of D_{a_0,b_0} is isogeneous to a product of elliptic curves. Using Magma [4] we search for such pairs a_0, b_0 and try to identify the elliptic curves.

Suppose that $\operatorname{Jac}(D_{a_0,b_0})$ is isogeneous over $\mathbb{Q}$ to $E'_{a_0,b_0} \times E''_{a_0,b_0}$. If p is a prime of good reduction of $\operatorname{Jac}(D_{a_0,b_0})$, then E'_{a_0,b_0} and E''_{a_0,b_0} also have good reduction at p. Moreover $\operatorname{Jac}(D_{a_0,b_0,p})$ is isogeneous over $\mathbb{F}_p$ to the product of the reductions $E'_{a_0,b_0,p}$ and $E''_{a_0,b_0,p}$. Thus the characteristic polynomial of Frobenius of $\operatorname{Jac}(D_{a_0,b_0})$ at p is a product of two quadratic polynomials.

We briefly describe our search. For all pairs of integers a_0, b_0 such that $-1000 \leq a_0, b_0 \leq 1000$ and $a_0 b_0 (4a_0^3 + 27b_0^2) \neq 0$ and for all primes p such that $p < 1000$ and D_{a_0,b_0} has good reduction at p we compute the characteristic polynomial of Frobenius at p. If for a pair a_0, b_0 one of these polynomials is irreducible and therefore $\operatorname{Jac}(D_{a_0,b_0})$ is simple over $\mathbb{Q}$, then we ignore this pair. The remaining pairs are $(60, \pm 20)$, $(240, \pm 160)$ and $(540, \pm 540)$.

Suppose that E'_{a_0,b_0} is a factor of $\operatorname{Jac}(D_{a_0,b_0})$. Since for each of the six remaining pairs a_0, b_0 the curve D_{a_0,b_0} has good reduction at $p \neq 2, 3, 5$, the Jacobian variety of D_{a_0,b_0} and the elliptic curve E'_{a_0,b_0} also have good reduction at $p \neq 2, 3, 5$. By the Shafarevich Theorem (see [61, Theorem IX.6.1]) there are up to isomorphism over $\mathbb{Q}$ only finitely many elliptic curves with good reduction at $p \neq 2, 3, 5$. The conductor of an elliptic curve is an ideal to encode the primes of non-good reduction, see [62, Section IV.10]. For many conductors the Cremona tables [11] contain a complete list of isogeny and isomorphism classes of elliptic curves over $\mathbb{Q}$.

Table 4.1: All the pairs of integers a_0, b_0 such that $-1000 \leq a_0, b_0 \leq 1000$, $a_0 b_0 \left(4a_0^3 + 27b_0^2\right) \neq 0$ and $\operatorname{Jac}(D_{a_0,b_0})$ not necessarily simple over $\mathbb{Q}$. The columns $[E'_{a_0,b_0}]$ and $[E''_{a_0,b_0}]$ contain the Cremona labels of the isogeny classes of the elliptic curves such that the characteristic polynomials of Frobenius of $\operatorname{Jac}(D_{a_0,b_0})$ and $E'_{a_0,b_0} \times E''_{a_0,b_0}$ at p agree for $5 < p < 1000$. The Cremona label of the elliptic curve E_{a_0,b_0} defined as $y^2 = x^3 + a_0 x + b_0$ is also given.

a_0	b_0	$[E'_{a_0,b_0}]$	$[E''_{a_0,b_0}]$	$[E_{a_0,b_0}]$
60	20	72a	1800i	1800t
60	-20	144b	3600q	3600n
240	160	576d	14400bv	14400bn
240	-160	576i	14400ei	14400dz
540	540	48a	1200h	1200f
540	-540	24a	600g	600b

We identified possible elliptic factors as follows. Let a_0, b_0 be one of the six remaining pairs. For all the available conductors of the form $\left(2^a 3^b 5^c\right)$ in the Cremona tables in Magma and for all the isogeny classes $[E]$ with corresponding conductor we compute the characteristic polynomials of Frobenius of E and of D_{a_0,b_0} at the primes p such that $5 < p < 1000$. If for some prime the former polynomial does not divide the latter, then E is not an elliptic factor of $\operatorname{Jac}(D_{a_0,b_0})$ and we ignore this isogeny class. For each pair we find two isogeny classes. Moreover for all primes p such that $5 < p < 1000$ the characteristic polynomial of Frobenius of D_{a_0,b_0} at p is equal to the product of the characteristic polynomials of Frobenius of the two elliptic curves at p. The results are given in Table 4.1.

Observe that the elliptic curves E_{a_0,b_0} for the six pairs a_0, b_0 in Table 4.1 are quadratic twists of each other. This also holds for the curves D_{a_0,b_0}. Since E_{a_0,b_0}, E'_{a_0,b_0} and E''_{a_0,b_0} fall in different isogeny classes, the elliptic curve E_{a_0,b_0} is not a factor of $\operatorname{Jac}(D_{a_0,b_0})$.

Following [31, Section 1], if $\operatorname{Jac}(D_{a_0,b_0})$ is isogeneous to $E'_{a_0,b_0} \times E''_{a_0,b_0}$, then for some $d > 1$ the d-torsion of both elliptic curves are isomorphic as Galois modules. Therefore if $p \nmid d$ and p is a prime of good reduction, then the traces of Frobenius on the elliptic curves at p are equal modulo d. Using Magma we see that

$$\gcd\left\{\left|E'_{a_0,b_0}(\mathbb{F}_p)\right| - \left|E''_{a_0,b_0}(\mathbb{F}_p)\right| : 5 < p < 100\right\} = 5$$

for every entry in Table 4.1. Hence we expect that in these six cases $\operatorname{Jac}(D_{a_0,b_0})$ and $E'_{a_0,b_0} \times E''_{a_0,b_0}$ are $(5,5)$-isogeneous over $\mathbb{Q}$.

The genus 2 curves whose Jacobian variety admit a $(5,5)$-isogeny to a pair of elliptic curves form a surface in the moduli space of genus 2 curves. Equations of this surface are available in [36, Section 6]. In principle one could compute the $a_0, b_0 \in \bar{\mathbb{Q}}$ such that D_{a_0,b_0} lies on this surface.

4.5.1 The case $a_0 = 60$, $b_0 = 20$

We treat this case in a bit more detail for later convenience. Recall that the curve $D_{60,20}$ is defined as

$$y^2 = \big(x^3 + 60x + 20\big)(60x + 20)(60x - 60).$$

The polynomial $x^3 + 60x + 20$ is Eisenstein at $p = 5$, so it is irreducible over $\mathbb{Q}$. Its discriminant is $-2^4 3^7 5^2$, which is not a square in $\mathbb{Q}^*$. A short computation shows that the splitting field is $\mathbb{Q}\big(\zeta_3, \sqrt[3]{10}\big)$ and has degree 6 over $\mathbb{Q}$. Therefore

$$\mathrm{Jac}\,(D_{60,20})(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Recall that we expect that $\mathrm{Jac}\,(D_{60,20})$ is $(5,5)$-isogeneous to $E'_{60,20} \times E''_{60,20}$. Thus the latter should also have 4 rational 2-torsion points.

According to the Cremona tables, the isogeny class with label 1800i contains precisely one isomorphism class. So $E''_{60,20}$ should be isomorphic to the elliptic curve defined by

$$y^2 = x^3 - 52500x - 5537500.$$

A computation shows that the right-hand side is an irreducible polynomial over $\mathbb{Q}$ and its splitting field is also $\mathbb{Q}\big(\zeta_3, \sqrt[3]{10}\big)$. Hence $E''_{60,20}$ has no rational points of order 2.

The curve $E'_{60,20}$ should therefore have the full 2-torsion subgroup rational. The isogeny class with label 72a in the Cremona tables contain six isomorphism classes of which only 72a2 and 72a4 have the full 2-torsion subgroup rational. Thus we expect that $E'_{60,20}$ is isomorphic to the elliptic curve either defined as

$$y^2 = x^3 - 39x - 70$$

or defined as

$$y^2 = x^3 - 219x + 1190.$$

Chapter 5

Faltings method

In this chapter we describe a method to compare two p-adic representations of a profinite group. Combined with the Isogeny Theorem this becomes a method to prove or disprove that two given abelian varieties are isogeneous.

The Faltings method is based on a group that measures the difference in the characters of two representations. In the proof of [16, Satz 5] Faltings introduces this group to show that up to some conditions there are only finitely many Galois representations on abelian varieties. In [57] Serre calls this group the deviation group and briefly explains the concept followed by an effective application to special 2-adic Galois representations on an elliptic curve. Livné describes in [41, Section 4] the method for two-dimensional 2-adic Galois representations with even trace and isomorphic residue representations. In [10, Chapter 5] Chênevert explains the deviation group in more detail and extends the method to two-dimensional 2-adic Galois representations with isomorphic residue representations. Grenié extends the method to general d-dimensional p-adic representations in [22]. We recall a version closely related to Chênevert's and Grenié's results.

We use the following notations: Let G be a profinite group, K be a local field with maximal order R and (finite) residue field k of characteristic p, π be a uniformizer of R and d be a positive integer. Given a closed subgroup H of G and a positive integer e, denote the closure of the group $\langle h^e : h \in H \rangle$ by H^e. Notice that if H is a closed normal subgroup of G, then so is H^e. Suppose that $\rho : G \to \mathrm{GL}_d(R)$ is a continuous representation, then $\bar{\rho} : G \to \mathrm{GL}_d(k)$ is the residue representation of ρ.

Our version of the Faltings method is:

Theorem 5.1. *Let $\rho_i : G \to \mathrm{GL}_d(R)$ for $i = 1, 2$ be continuous representations and e be an integer such that $d \leq p^e$. Suppose that $\Sigma \subset G$ is a subset such that the characteristic polynomials of $\rho_1(h)$ and $\rho_2(h)$ agree for all $h \in \Sigma$. Suppose that $N \subset G$ is an open normal subgroup such that $\bar{\rho}_i(N)$ is a p-group. If the set*

$$\overline{\Sigma} = \left\{ g h^n g^{-1} : h \in \Sigma, g \in G, n \in \mathbb{Z} \right\}$$

maps surjectively to G/N^{p^e}, then the characters of ρ_1 and ρ_2 are equal.

We explain how to apply the theorem to abelian varieties in Section 5.1 and prove the theorem in Sections 5.2, 5.3 and 5.4. In Section 5.5 we make some remarks and compare the theorem with other versions.

5.1 Applications

Suppose that the local field K has characteristic zero and the $\rho_i : G \to \mathrm{GL}_d(K)$ are semi-simple. Recall the following well-known result:

Theorem 5.2. *If K is a field of characteristic zero and $\rho_i : G \to \mathrm{GL}_d(K)$ for $i = 1, 2$ are semi-simple, then the representations ρ_1 and ρ_2 are isomorphic if and only if their characters are equal.*

Proof. Follows from the corollary to [6, §20, No. 6, Proposition 6]. □

Also recall that $\rho_i : G \to \mathrm{GL}_d(K)$ is isomorphic to some $\rho_i' : G \to \mathrm{GL}_d(R)$, because G is compact [12, Proposition 9.3.5]. Hence ρ_1 and ρ_2 are isomorphic if and only if the characters of ρ_1' and ρ_2' are equal. The latter statement can be checked with Theorem 5.1.

The application to abelian varieties relies on the Isogeny Theorem:

Theorem 5.3 (Faltings)**.** *If K is a number field, A_i is an abelian variety over K of dimension d for $i = 1, 2$ and ℓ is a prime, then the natural action of the absolute Galois group G_K on $\mathrm{T}_\ell A_i \otimes \mathbb{Q}_\ell$ is semi-simple for $i = 1, 2$ and there is an isomorphism*

$$\mathrm{Hom}_K(A_1, A_2) \otimes \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}_{\mathbb{Z}_\ell[G_K]}(\mathrm{T}_\ell A_1, \mathrm{T}_\ell A_2).$$

Proof. See [16, Satz 3 and 4] and corollaries. □

We now give an application to elliptic curves. Consider elliptic curves E_1 and E_2 over $\mathbb{Q}$. Let S be the set of primes at which E_1 or E_2 has bad reduction and the prime 2. Denote the Galois action on the 2-adic Tate module of E_i by $\rho_i : G_\mathbb{Q} \to \mathrm{Aut}\,(\mathrm{T}_2 E_i)$. After a choice of basis we get $\rho_i : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{Z}_2)$. Since the ρ_i are semi-simple, E_1 and E_2 are isogeneous over $\mathbb{Q}$ if and only if the characters of ρ_1 and ρ_2 are equal. If $p \notin S$ is a prime, then the inertia group at p is a subgroup of the kernel of both ρ_i. Therefore

$$\begin{tikzcd} G_\mathbb{Q} \arrow[r, "\rho_i"] \arrow[d] & \mathrm{GL}_2(\mathbb{Z}_2) \\ \mathrm{Gal}\,(\mathbb{Q}_S/\mathbb{Q}) \arrow[ur, dashed, "\rho_i'"'] & \end{tikzcd}$$

commutes, where $\mathbb{Q}_S$ is the maximal algebraic extension of $\mathbb{Q}$ unramified outside S. The characters of ρ_1 and ρ_2 are equal if and only if the same is true for ρ_1' and ρ_2'. We will apply Theorem 5.1 to ρ_1' and ρ_2'. Let $G = \mathrm{Gal}\,(\mathbb{Q}_S/\mathbb{Q})$, $d = 2$

and $e = 1$. Choose $N = \ker \bar{\rho}_1 \times \bar{\rho}_2$. The subgroup N^2 corresponds to the field L defined as the compositum of all quadratic extensions of $\mathbb{Q}(E_1[2], E_2[2])$ in $\mathbb{Q}_S$. By the Čhebotarev Density Theorem every conjugacy class of $G/N^2 = \mathrm{Gal}\,(L/\mathbb{Q})$ contains a Frobenius element of a prime not in S. Denote by Σ the (finite) set of a Frobenius elements in G for each of these primes. If the characteristic polynomials of $\rho_1'(g)$ and $\rho_2'(g)$ are equal for all $g \in \Sigma$, then Theorem 5.1 implies that the characters of ρ_1' and ρ_2' are isomorphic, that is E_1 and E_2 are isogeneous over $\mathbb{Q}$. On the other hand if the characteristic polynomials are different for some $g \in \Sigma$, then $\mathrm{tr}\,\rho_1'(g^n) \neq \mathrm{tr}\,\rho_2'(g^n)$ for some n, that is the characters of ρ_1' and ρ_2' differ, so E_1 and E_2 are not isogeneous over $\mathbb{Q}$.

5.2 Deviation group

In this section we define the deviation group and prove some of its properties. Recall that $\rho_i : G \to \mathrm{GL}_d(R)$ for $i = 1, 2$ are continuous representations with R the ring of integers of a local field with uniformizer π.

Consider the group homomorphism $\rho = (\rho_1, \rho_2) : G \to \mathrm{GL}_d(R) \times \mathrm{GL}_d(R)$. Let $\tilde{\rho} : R[G] \to \mathrm{M}_d(R) \oplus \mathrm{M}_d(R)$ be the ring homomorphism obtain by R-linear extension of ρ. Denote the image of $\tilde{\rho}$ by M. Notice that πM is an ideal in M. The *deviation map* δ is defined as follows

$$\begin{tikzcd}
R[G] \arrow[r, two heads, "\tilde{\rho}"] \arrow[dr, dashed, two heads, "\delta"'] & M \arrow[d, two heads] \\
 & M/\pi M
\end{tikzcd}$$

and the subgroup $\delta(G)$ of $(M/\pi M)^*$ is called the *deviation group*.

Proposition 5.4. *Let $\Sigma \subset G$ be a subset such that for every conjugacy class C of $\delta(G)$ there exists a $g \in \Sigma$ with $\delta(g) \in C$. If the characters of ρ_1 and ρ_2 are different, then so are their restrictions to Σ.*

The statement of the proposition and its proof below are a reformulation of those found in [57] and [10, Proposition 5.2.3].

Proof. Suppose that the characters of ρ_1 and ρ_2 are different, then the set

$$\{n \in \mathbb{Z} : \mathrm{tr}\,\rho_1 \equiv \mathrm{tr}\,\rho_2 \mod \pi^n\}$$

is finite and has a maximum m. Choose $g \in G$ such that $\mathrm{tr}\,\rho_1(g) \not\equiv \mathrm{tr}\,\rho_2(g) \mod \pi^{m+1}$. Take $h \in \Sigma$ such that $\delta(h) = \delta\big(aga^{-1}\big)$ for some $a \in G$, which is possible by assumption.

Consider the R-module homomorphism $\psi : M \to R/\pi^{m+1}$ defined as

$$(A, B) \longmapsto \mathrm{tr}\,A - \mathrm{tr}\,B \mod \pi^{m+1}.$$

Notice that $\pi M \subset \ker \psi$, because $\rho(G)$ generates M and $\psi \circ \rho(\tilde{g}) \in \pi^m/\pi^{m+1}$ for all $\tilde{g} \in G$ by definition of m. Thus ψ induces an R-module homomorphism $\tilde{\psi} : M/\pi M \to R/\pi^{m+1}$. In particular $\psi \circ \rho = \tilde{\psi} \circ \delta$. So

$$\psi \circ \rho(h) = \tilde{\psi} \circ \delta(h) = \tilde{\psi} \circ \delta\big(aga^{-1}\big) = \psi \circ \rho\big(aga^{-1}\big) = \psi \circ \rho(g) \neq 0.$$

Hence $\operatorname{tr} \rho_1(h) \not\equiv \operatorname{tr} \rho_2(h) \mod \pi^{m+1}$, that is $\operatorname{tr} \rho_1|_\Sigma \neq \operatorname{tr} \rho_2|_\Sigma$. □

Observe that the residue representation $\bar{\rho} : G \to \mathrm{GL}_d(k) \times \mathrm{GL}_d(k)$ factors through $\delta(G)$, but in general the deviation group is not isomorphic to $\bar{\rho}(G)$. For example there exist non-isogeneous elliptic curves E_1 and E_2 over $\mathbb{Q}$ with all two-torsion rational, so for the associated 2-adic Galois representations $\bar{\rho}(G_\mathbb{Q})$ is trivial but $\delta(G_\mathbb{Q})$ is not.

We can also define the deviation group as the inverse limit of some finite discrete topological groups. For positive integers n consider the continuous homomorphism $\rho_{(n)} : G \to \mathrm{GL}_d(R/\pi^n) \times \mathrm{GL}_d(R/\pi^n)$ induced by ρ. Repeat the deviation group construction for $\rho_{(n)}$ to obtain a continuous homomorphism $\delta_{(n)} : G \to \delta_{(n)}(G)$ and a discrete topological group $\delta_{(n)}(G)$. Since R is complete, $\delta(G) = \varprojlim \delta_{(n)}(G)$. Notice that $\delta_{(1)} = \bar{\rho}$. Hence $\delta(G)$ is a profinite group and the homomorphisms in the following commutative diagram are continuous:

$$\begin{tikzcd} G \arrow[r, two heads, "\delta"] \arrow[dr, "\bar{\rho}"'] & \delta(G) \arrow[d] \\ & \mathrm{GL}_d(k) \times \mathrm{GL}_d(k). \end{tikzcd}$$

In fact the deviation group is a finite discrete topological group by

Proposition 5.5. *The order of $\delta(G)$ is less than $|k|^{2d^2}$.*

The proof is identical to [10, Proposition 5.2.2].

Proof. Consider M as an R-submodule of the free R-module $\mathrm{M}_d(R) \oplus \mathrm{M}_d(R)$ of rank $2d^2$. Since R is a principal ideal domain, as R-module M is free and has rank at most $2d^2$. Thus $M/\pi M$ as a k-vector space has dimension at most $2d^2$. Hence

$$|\delta(G)| \leq \left|(M/\pi M)^*\right| < |M/\pi M| \leq |k|^{2d^2}.$$

□

By combining the previous two propositions we see that it is sufficient to compare the traces $\operatorname{tr} \rho_1(g)$ and $\operatorname{tr} \rho_2(g)$ for finitely many $g \in G$ to decide if the characters of ρ_1 and ρ_2 are equal or not. The problem is to find the finitely many elements g.

5.3 Residue kernel

How to compute the deviation group $\delta(G)$ for two representations $\rho_i : G \to \mathrm{GL}_d(R)$ is unclear. In particular directly computing a set $\Sigma \subset G$ as in Proposition 5.4 is therefore not feasible. The solution is to approximate the deviation group by another group such that the homomorphism δ factors through this group.

In the case $d = 2$ and R the maximal order in a finite extension of $\mathbb{Q}_2$ the method described in [41, Section 4] and [10, Sections 5.4 and 5.5] uses that up to certain conditions on the residue representations $\bar{\rho}_i$ the deviation group $\delta(G)$ has exponent two. These conditions on $\bar{\rho}_1$ and $\bar{\rho}_2$ are closely related to the images of the residue representations being trivial.

Suppose for a moment that $N = \ker \bar{\rho} = \ker \bar{\rho}_1 \cap \ker \bar{\rho}_2$. Consider the following exact sequence

$$1 \longrightarrow \delta(N) \longrightarrow \delta(G) \longrightarrow \bar{\rho}(G) \longrightarrow 1.$$

In principle $\bar{\rho}(G)$ is well-known. To get a better understanding of $\delta(G)$ we should therefore study $\delta(N)$. The latter group is a pro-p group, because $\rho(N)$ is a pro-p group. Moreover $\delta(N)$ has the following crucial property:

Proposition 5.6. *Let $e \in \mathbb{Z}$ be such that $d \leq p^e$ and $N \subset G$ a subgroup such that $\bar{\rho}(N)$ is a p-group. If $n \in N$ and the characteristic polynomials of $\rho_i(n)$ agree, then the order of $\delta(n)$ divides p^e.*

This proposition is a generalization of [10, Proposition 5.4.2].

Proof. Denote the characteristic polynomial of $\rho_i(n)$ by $\chi_i \in R[x]$. Using the ring homomorphism $\mathrm{M}_d(R) \to \mathrm{M}_d(k)$, it follows that $\chi_i \mod \pi$ is equal to the characteristic polynomial $\bar{\chi}_i$ of $\bar{\rho}_i(n)$.

We claim that $\bar{\chi}_i = (x-1)^d$: Let l be the splitting field of $\bar{\chi}_i$ over k. The field l is also finite and of characteristic p. Now $\bar{\rho}_i(n)$ has a Jordan normal form over l, that is it is conjugate to a matrix with blocks of the form

$$\begin{pmatrix} \ddots & & & \\ & \lambda & 1 & \\ & & \lambda & \\ & & & \ddots \end{pmatrix}$$

with $\lambda \in l^*$. The order of λ in l^* is a power of p, because the order of $\bar{\rho}_i(n)$ is a power of p. The order of λ also divides the order of l^*, which is not divisible by p. Hence $\lambda = 1$ and the claim follows.

Assume that $\chi_1 = \chi_2$, then $\chi_i = (x-1)^d - \pi F$ for some $F \in R[x]$. The Cayley-Hamilton Theorem gives $\chi_i(\rho_i(n)) = 0$, that is

$$(\rho_i(n) - 1)^d = \pi F(\rho_i(n)),$$

which implies that $(\rho(n) - 1)^d = \pi F(\rho(n)) \in \pi M$. Thus $\delta(n)^{p^e} = 1$, because π divides p and by the definition of e. □

In general the order of $\delta(n)$ divides $p^{e'}$ with $e' \in \mathbb{Z}$ such that $2d \leq p^{e'}$. The proof is the same as above except for the final step where χ_i is replaced by $\chi_1\chi_2$.

5.4 Proof of the theorem

We need the following proposition in the proof of Theorem 5.1.

Proposition 5.7. *Let p be a prime number and e be a positive integer. Suppose that G is a finite p-group and write $N = G^{p^e}$. If for every $gN \in G/N$ there exists a $h \in G[p^e]$ such $gN = hN$, then G has exponent dividing p^e.*

This is a generalization of [10, Lemma 5.4.7] and equivalent to [22, Lemma 7].

Proof. Suppose that G does not have exponent dividing p^e, then N is a non-trivial normal subgroup.

The group N has a subgroup M of index p which is normal in G: Let N_p be the Frattini quotient of N. Remark that N_p is a non-trivial $\mathbb{F}_p$-vector space, because N is a non-trivial p-group. A normal subgroup of N of index p corresponds to a (normal) subgroup of N_p of index p, which again corresponds to a non-zero element from the vector space dual of N_p. If the set of normal subgroups of N of index p is denoted by Ω, then $|\Omega| = p^n - 1$ for some $n \in \mathbb{Z}_{>0}$. Let the group G act on the set Ω by conjugation. This action has a fixed point, otherwise the order of the orbits are divisible by p in contradiction with the order of Ω being coprime to p. Choose M to be a fixed point of this action.

The subgroup N/M is contained in the center of G/M: Consider the action of G/M by conjugation on N/M. Since G/M is a p-group and $\mathrm{Aut}\,(N/M) \cong \mathrm{Aut}\,(\mathbb{Z}/p\mathbb{Z})$ is a group of $p-1$ elements, the action must be trivial. Hence $gM \cdot nM \cdot (gM)^{-1} = nM$, that is $gM \cdot nM = nM \cdot gM$ for all $nM \in N/M$ and $gM \in G/M$.

A diagram chase in the following commutative diagram will result into a contradiction, thereby proving the proposition.

$$\begin{tikzcd}
1 \arrow[r] & N \arrow[r] \arrow[d] & G \arrow[r] \arrow[d] & G/N \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & N/M \arrow[r] & G/M \arrow[r] & G/N \arrow[r] & 1
\end{tikzcd}$$

Let $gM \in G/M$. By assumption there exists a $h \in G[p^e]$ such that $gN = hN$. Thus $gM = hM \cdot nM$ for some $n \in N$. Using that $N/M \subset Z(G/M)$ and $N/M \cong \mathbb{Z}/p\mathbb{Z}$, shows that gM has order dividing p^e. Thus G/M has exponent dividing p^e. However this implies that $N = G^{p^e} \subset M$, contradicting $[N : M] = p$. □

The proof below is a generalization of the proof of [10, Theorem 5.4.8].

Proof of Theorem 5.1. Recall that N is an open normal subgroup of G and δ is a continuous homomorphism. Since $\delta(G)$ is a discrete topological group, so is $\delta(N)$. Hence the kernel of

$$G \longrightarrow \delta(N) \longrightarrow \delta(N)/\delta(N)^{p^e}.$$

is closed and therefore contains N^{p^e}.

Recall the set

$$\overline{\Sigma} = \big\{ g h^n g^{-1} : h \in \Sigma, g \in G, n \in \mathbb{Z} \big\}.$$

For every $h \in \Sigma$ the characteristic polynomials of $\rho_1(h)$ and $\rho_2(h)$ are equal. Using the fundamental theorem of symmetric polynomials and the fact that the characteristic polynomial only depends on the conjugacy class it follows that for every $g \in \overline{\Sigma}$ the characteristic polynomials of $\rho_1(g)$ and $\rho_2(g)$ are equal.

The kernel of δ contains N^{p^e}: Consider the commutative diagram

$$\begin{tikzcd}
N \arrow[r, two heads, "\delta"] \arrow[d, two heads] & \delta(N) \arrow[d, two heads] \\
N/N^{p^e} \arrow[r, two heads, dashed] & \delta(N)/\delta(N)^{p^e}.
\end{tikzcd}$$

Take any $x \in \delta(N)/\delta(N)^{p^e}$. Let $\tilde{x} \in N$ be a lift of x. Since $N/N^{p^e} \subset G/N^{p^e}$, by assumption there exists a $g \in \overline{\Sigma}$ such that $gN^{p^e} = \tilde{x}N^{p^e}$. In fact $g \in N$ as $\tilde{x} \in N$ and $N^{p^e} \subset N$. Now $\delta(g) \in \delta(N)[p^e]$ by Proposition 5.6, because the characteristic polynomials of $\rho_i(g)$ are equal. The pro-p group $\delta(N)$ is finite by Proposition 5.5. Therefore the group $\delta(N)^{p^e}$ is trivial by Proposition 5.7. Hence N^{p^e} is a subgroup of $\ker \delta$.

Assume that the characters of ρ_i are different. Consider

$$\begin{tikzcd}
G \arrow[r, two heads, "\delta"] \arrow[d, two heads] & \delta(G) \\
G/N^{p^e} \arrow[ur, two heads, dashed, "\tilde{\delta}"'] &
\end{tikzcd}$$

Take any conjugacy class $C \subset \delta(G)$. Choose a $g \in G$ such that $\delta(g) \in C$. By assumption there is a $h \in \overline{\Sigma}$ such that $gN^{p^e} = hN^{p^e}$. So $\delta(g) = \delta(h)$. Thus by Proposition 5.4 the restriction of the characters of ρ_i to $\overline{\Sigma}$ are different. However this contradicts the construction of $\overline{\Sigma}$.

Hence the characters of ρ_1 and ρ_2 are equal. □

5.5 Remarks

In the proof of Theorem 5.1 we approximated the deviation group $\delta(G)$ by G/N^{p^e}. Although the group $\delta(G)$ is finite, it is not obvious whether in general the same is true for the approximation.

Proposition 5.8. *Let G be a profinite group, $N \subset G$ be an open subgroup, p be a prime and $e \geq 1$. The group G/N^{p^e} is finite if and only if the pro-p quotient of N is finitely generated.*

Proof. Since

$$1 \longrightarrow N/N^{p^e} \longrightarrow G/N^{p^e} \longrightarrow G/N \longrightarrow 1$$

is exact and G/N finite by N being open, the group G/N^{p^e} is finite if and only if N/N^{p^e} is finite. Denote the pro-p quotient of N by N_p. Then $N/N^{p^e} \cong N_p/N_p^{p^e}$. Moreover the Frattini quotients of N_p and $N_p/N_p^{p^e}$ are equal.

The Frattini quotient of N_p is finite if and only if N_p is finitely generated by [13, Proposition 1.14]. Hence if N/N^{p^e} is finite, then N_p is finitely generated.

Assume that N_p is finitely generated, then the same is true for $N_p/N_p^{p^e}$. Let d be the number of generators. Observe that $N_p/N_p^{p^e}$ is an inverse limit of groups of exponent dividing p^e with at most d generators. The solution to the Restricted Burnside Problem [79, 80] implies that the order of a finite group of exponent p^e and d generators is bounded in terms of p^e and d. Hence $N_p/N_p^{p^e}$ is finite. □

More on the Restricted Burnside Problem can be found in [71].

We first compare the approximation of the deviation group in Theorem 5.1 with the approximation in the proof of [16, Satz 5]. In group theory terms the latter is given by G/M, where M is the intersection of all open subgroups of G of index at most $|\delta(G)| < |k|^{2d^2}$. To obtain the best of both versions, the group N^{p^e} in Theorem 5.1 should be replaced by the intersection M' of all subgroups H of G such that $N^{p^e} \subset H \subset N$ and $[G : H] \leq |\delta(G)| < |k|^{2d^2}$.

Now we compare Theorem 5.1 with Grenié's version. If G is a pro-p group, then Theorem 5.1 is essentially identical to [22, Proposition 9]. The main result [22, Theorem 3] is a corollary to [22, Proposition 9] obtained by:

1. Given a restriction on the eigenvalues of $\bar{\rho}_i(g)$ and on the dimension d of the ρ_i, the representations ρ_i can be modified such that their images are pro-p groups.

2. Assume that $\rho(G)$ is a pro-p group. Since ρ factors through the pro-p quotient of G, we may assume that G is a pro-p group. Let r be the rank of $\rho(G)$ as defined in [13]. By the theory of *powerful* pro-p groups there exists an n depending on r, p and e such that $\Phi^n(\rho(G)) \subset \rho(G)^{p^e}$ with $\Phi(H)$ the Frattini subgroup of H. We have $\rho(\Phi^n(G)) = \Phi^n(\rho(G))$. In this case the deviation group is approximated by $G/\Phi^n(G)$. Moreover

$$\Phi^n(G) \subset \Phi^{n-1}(G) \subset \cdots \subset G$$

is a sequence of open subgroups such that $\Phi^i(G)/\Phi^{i+1}(G)$ is abelian of exponent p.

The second step can also improve Theorem 5.1. Apply the theory of powerful pro-p groups to $\rho(N)$ in order to obtain a n such that $\Phi^n(\rho(N)) \subset \rho(N)^{p^e}$. Since $\Phi^n\big(N/N^{p^e}\big)$ is contained in the kernel of

$$N/N^{p^e} \longrightarrow \delta(N)/\delta(N)^{p^e}.$$

the deviation group is also approximated by $\big(G/N^{p^e}\big)/\Phi^n\big(N/N^{p^e}\big)$. We expect that $\Phi^n\big(N/N^{p^e}\big)$ is non-trivial especially when the minimal number of generators of N/N^{p^e} is large compared to the rank r of $\rho(N)$.

Chapter 6

Galois extensions with exponent four group

The content of this chapter resulted from the desire to use the Faltings method described in Chapter 5 to decide whether or not two given abelian varieties are isogeneous over a given field. The motivating question: Is the Jacobian variety of the hyperelliptic curve

$$C : y^2 = \bigl(x^3 + 60x + 20\bigr)(60x + 20)(60x - 60)$$

isogeneous over $\mathbb{Q}$ to the product of the two elliptic curves

$$E_1 : y^2 = x^3 - 39x - 70$$

and

$$E_2 : y^2 = x^3 - 52500x - 5537500.$$

Since these abelian varieties have good reduction at the primes different from 2, 3 and 5, the Galois representations on the 2-adic Tate modules are unramified above the other primes. If we are able to compute the maximal exponent four extension of

$$\mathbb{Q}(\mathrm{Jac}\,(C)[2], E_1[2], E_2[2]) = \mathbb{Q}\Bigl(\zeta_3, \sqrt[3]{10}\Bigr)$$

unramified outside 2, 3 and 5 and the characteristic polynomial of Frobenius for sufficiently many primes, then we can decide if the two abelian varieties are isogeneous over $\mathbb{Q}$ using Theorem 5.1.

We describe the Galois group of the maximal p-extension for certain cases in Section 6.1 and from it derive the Galois group of the maximal exponent four subfield in Section 6.2. In Sections 6.3, 6.4 and 6.5 this subfield is computed explicitly for $\mathbb{Q}$ and ramification only above $\{2, 3, \infty\}$. We compute the conjugacy class of Frobenius automorphisms of this field in Section 6.6 and describe the consequences for the Faltings method in Section 6.7. An idea to compute other exponent four extensions is briefly discussed in Section 6.8. The last Section 6.9 lists some open questions.

Many computations in this chapter are implicitly performed using Magma. Especially the combinatorial parts appear to be impossible without the help of a computer.

6.1 Maximal p-extensions

Let K be a number field and L/K be a Galois extension with exponent four Galois group unramified outside a set of places S. This is an example of a 2-extension of K. In fact L is a subfield of the *maximal 2-extension* $\hat{K}_S$ of K unramified outside S, that is the union of all finite 2-extensions of K unramified outside S.

The Galois group $\hat{G}_S$ of the extension $\hat{K}_S/K$ is a pro-2 group. It can be analysed using presentations of pro-2 groups and Galois cohomology. Moreover in special cases $\hat{G}_S$ is described exactly. See [34, 48, 58] for an introduction to Galois cohomology and see [77] for profinite groups.

We first consider the case $K = \mathbb{Q}$ and $S = \{2, 3, \infty\}$. The Galois group $\hat{G}_S$ is described in [34, Example 11.18] as the pro-2 presentation

$$\left\langle s_3, t_3, t_\infty : t_3^2\left[t_3^{-1}, s_3^{-1}\right], t_\infty^2\right\rangle,$$

where s_3 is a lift of the Frobenius automorphism at 3, t_3 is a generator of the inertia group at 3 and t_∞ is the complex conjugation. In the related case $S = \{2, \infty\}$ the Galois group is described in [43] (as mentioned in [5] and [33]) as the pro-2 presentation

$$\left\langle s_3, t_\infty : t_\infty^2\right\rangle.$$

Suppose that $K = \mathbb{Q}\left(\sqrt[3]{10}\right)$ and S the set of prime ideals above 2 and 3 and the unique embedding in $\mathbb{R}$. The maximal order $\mathcal{O}_K$ is a principal ideal domain and its unit group has rank one. The generators of the unit group are $-1, u$ with

$$u = \frac{1}{3}\left(-2\sqrt[3]{10}^2 + \sqrt[3]{10} + 7\right).$$

The prime ideals above 2 and 3 satisfy $(2) = \mathfrak{p}_2^3$ and $(3) = \mathfrak{p}_{3a}\mathfrak{p}_{3b}^2$ where $\mathfrak{p}_2, \mathfrak{p}_{3a}, \mathfrak{p}_{3b}$ are generated by

$$\begin{aligned} p_2 &= \frac{1}{3}\left(\sqrt[3]{10}^2 + \sqrt[3]{10} + 4\right) \\ p_{3a} &= \frac{1}{3}\left(-\sqrt[3]{10}^2 + 2\sqrt[3]{10} - 1\right) \\ p_{3b} &= \frac{1}{3}\left(-\sqrt[3]{10}^2 - \sqrt[3]{10} - 1\right) \end{aligned}$$

respectively. Thus $S = \{\mathfrak{p}_2, \mathfrak{p}_{3a}, \mathfrak{p}_{3b}, \infty_\mathbb{R}\}$. According to [78] the pro-2 presentation of $\hat{G}_S$ is given by

$$\left\langle s_{p_{3a}}, t_{p_{3a}}, s_{p_{3b}}, t_{p_{3b}}, t_\infty : t_{p_{3a}}^2\left[t_{p_{3a}}^{-1}, s_{p_{3a}}^{-1}\right], t_{p_{3b}}^2\left[t_{p_{3b}}^{-1}, s_{p_{3b}}^{-1}\right], t_\infty^2\right\rangle$$

provided that the following group is trivial:

$$V_{\mathfrak{p}_2}^S = \Big\{a \in K^* : a \in K_{\mathfrak{p}_2}^2, a \in U_{\mathfrak{q}} K_{\mathfrak{q}}^{*2} \ \forall \mathfrak{q} \notin S\Big\}/K^{*2}.$$

This is indeed true, because

$$V_{\mathfrak{p}_2}^S = \big\{a = -1^{i_1} u^{i_2} p_{3a}^{i_3} p_{3b}^{i_4} : a \in K_{\mathfrak{p}_2}^2, i_j \in \{0,1\}\big\}/K^{*2}$$

and a is a square in $\mathcal{O}_K/\mathfrak{p}_2^7$ only for $i_1 = i_2 = i_3 = i_4 = 0$. The pro-2 presentation of $\hat{G}_S$ in the related case $S = \{\mathfrak{p}_2, \infty_{\mathbb{R}}\}$ is easily derived to be

$$\big\langle s_{p_{3a}}, s_{p_{3b}}, t_\infty : t_\infty^2 \big\rangle.$$

Unfortunately in the case $K = \mathbb{Q}$ and $S = \{2, 3, 5, \infty\}$ a complete description is unavailable as V_2^S is non-trivial: -15 is a square in $\mathbb{Q}_2$. Hence for certain unknown relations $r_1, \ldots, r_n$ the Galois group has a pro-2 presentation

$$\big\langle s_3, t_3, s_5, t_5 : t_3^2\big[t_3^{-1}, s_3^{-1}\big], t_5^4\big[t_5^{-1}, s_5^{-1}\big], r_1, \ldots, r_n\big\rangle.$$

Note that all maximal p-extensions above are infinite, because for $K = \mathbb{Q}$ and $S = \{2, \infty\}$ the extension is already infinite by for example the Golod-Shafarevich Theorem or the infinite abelian quotient of $\hat{G}_S$.

6.2 Exponent four quotients

Given a number field K, a set of places S and the Galois group $\hat{G}_S$ of the maximal 2-extension of K unramified outside S we can describe the Galois group $G_{S,4}$ of the maximal exponent four extension $K_{S,4}$ of K unramified outside S as the maximal exponent four quotient of $\hat{G}_S$.

The exponent four quotient $G_{S,4}$ of $\hat{G}_S$ is computed using the p-quotient algorithm implemented in Magma. We list the order of $G_{S,4}$ and its 2-class in Table 6.1 for the cases considered in the previous section. Based on the order of $G_{S,4}$ for $K = Q\big(\sqrt[3]{10}\big)$ computing the corresponding extension appears to be infeasible. Note that the groups $G_{S,4}$ are much smaller than the maximal exponent four groups with equal number of generators as shown in Table 6.2.

A naive way to compute the maximal exponent four extension $K_{S,4}$ is to build it as a tower of (abelian) exponent two extensions with the number of steps roughly related to the 2-class. In the case $\mathbb{Q}$ and $S = \{2, 3, \infty\}$ this gives

$$\mathbb{Q} \xrightarrow{8} \mathbb{Q}(\zeta_{24}) \xrightarrow{128} L \xrightarrow{32} \mathbb{Q}_{S,4}.$$

Since L is totally imaginary and $[L : \mathbb{Q}] = 1024$, the maximal exponent two extension M of L has degree $[M : L] > 2^{512}$ (due to the 512 generators of $\mathcal{O}_L{}^*$). This suggests it is too difficult to compute $\mathbb{Q}_{S,4}$ from M.

Table 6.1: The orders of the Galois group $G_{S,4}$ of the maximal exponent four extension of the number field K unramified outside the set of primes S.

K	S	$\lvert G_{S,4}\rvert$	2-class	conjugacy classes
$\mathbb{Q}$	$2, \infty$	2^6	4	13
$\mathbb{Q}$	$2, 3, \infty$	2^{15}	5	272
$\mathbb{Q}(\sqrt[3]{10})$	$\mathfrak{p}_2, \infty$	2^{37}	7	1 832 960
$\mathbb{Q}(\sqrt[3]{10})$	$\mathfrak{p}_2, \mathfrak{p}_{3a}, \mathfrak{p}_{3b}, \infty$	2^{234}	7	
$\mathbb{Q}$	$2, 3, 5, \infty$	$\leq 2^{73}$	≤ 5	

Table 6.2: The orders and 2-class of the Burnside groups on n generators of exponent four. Cases $n = 1, 2, 3, 4$ are mentioned in [42] and case $n = 5$ is mentioned in [71, Chapter 6].

n	$\lvert B(n,4)\rvert$	2-class
1	2^2	2
2	2^{12}	5
3	2^{69}	7
4	2^{422}	10
5	2^{2728}	13

6.3 Transitive groups

Instead of directly computing the field $K_{S,4}$ we can also try to identify subfields by studying the Galois group $G_{S,4}$ and consulting tables of number fields. An important concept is transitive groups.

Recall that a *transitive group* is a group G and a set X with a faithful and transitive action of G on X. If the set X and the action of G are clear from the context, then simply write G for the transitive group. The *degree* of the transitive group is defined to be the order of X. An isomorphism class of transitive groups is labelled $d\mathrm{T}n$ with d the degree and n a positive integer following Magma [4].

Consider the table of number fields described in [29]. An entry in the table consists of an irreducible polynomial f, an isomorphism class $[G]$ of a transitive group G and some other data. The polynomial f defines the number field up to isomorphism as $K = \mathbb{Q}[x]/(f)$ and G is the Galois group of the normal closure of K together with its action on the roots of f.

A transitive group is a special case of a *coset action*, that is the action of a group G on the coset space G/H for some subgroup H. Notice that in the case above H is the subgroup fixing the field K. A coset action (G, H) is a transitive group if and only if the normal core of H in G is trivial, that is

$$\bigcap_{g \in G} g^{-1} H g = \{e\}.$$

Table 6.3: These irreducible polynomials define up to isomorphism all number fields of degree 8 and unramified outside $\{2,\infty\}$ with the Galois group acting on the roots as the transitive group 8T30. Obtained from [29].

$$x^8+4x^6+4x^4-2$$
$$x^8-4x^6+4x^4-2$$
$$x^8+4x^6+6x^4+4x^2-1$$
$$x^8-4x^6+6x^4-4x^2-1$$

Conjugate subgroups give isomorphic coset actions.

Consider the case $\mathbb{Q}$ and $S=\{2,\infty\}$ from the previous section. The group $G_{S,4}$ contains up to conjugacy 4 subgroups with trivial normal core in G and lowest possible index 8. In each of the four cases the corresponding transitive group has label 8T30. According to [29] there are precisely four number fields up to isomorphism with this particular transitive group and ramification only above S, see Table 6.3. The splitting fields of the four polynomials are pairwise isomorphic, and are also isomorphic to the number field defined by the degree 64 polynomial in [22, Section 4.2].

The case $\mathbb{Q}$ and $S=\{2,3,\infty\}$ needs a different approach: The lowest possible index of a subgroup of $G_{S,4}$ with trivial normal core is 128 and at the time of writing [29] contains no fields of degree 128 unramified outside S.

6.4 Composita

Recall that a compositum of subfields of $K_{S,4}$ corresponds to the intersection of the corresponding subgroups of $G_{S,4}$. Thus the Galois group $G_{S,4}$ also gives us information on the composita of subfields such as if $K_{S,4}$ is equal to the compositum of small extensions of K.

A subfield L of $K_{S,4}$ is called *special* if L is not contained in a compositum of Galois extension of K in $K_{S,4}$ of lower degree, that is the subgroup H of $G_{S,4}$ corresponding to L is called *special* if H does not contain an intersection of normal subgroups of $G_{S,4}$ of lower index. Notice that a subgroup is special if and only if its normal core in $G_{S,4}$ is special.

We restrict ourself to the case $K=\mathbb{Q}$ and $S=\{2,3,\infty\}$. The lattice $\mathcal{N}$ of normal subgroups in $G_{S,4}$ provides us with insight into the special normal subgroups and their composita. A computation with Magma shows $G_{S,4}$ contains 382 normal subgroups.

Denote the subset of $\mathcal{N}$ of special normal subgroups by $\mathcal{N}_S$. It contains 69 subgroups of which 23 are minimal. A minimal subgroup in $\mathcal{N}_S$ has index 64, 512 or 2048. The normal closure of $\langle t_3\rangle$ in $G_{S,4}$ is special (and minimal), that is $\mathbb{Q}_{\{2,\infty\},4}$ is a special subfield of $\mathbb{Q}_{S,4}$.

Suppose $A\subset\mathcal{N}_S$ is a set of special normal subgroups such that $\bigcap_{N\in A}N$ is trivial, then A contains at least 3 subgroups of which one must have index 2048 (and be minimal). There are 216 such subsets A with 3 subgroups. If one of the three special subgroups is $\overline{\langle t_3 \rangle}$, then there are 24 triples with trivial intersection.

More information can be obtained from $\mathcal{N}$ and $\mathcal{N}_S$ such as inclusions of special subfields and common subfields.

6.5 Determine $\mathbb{Q}_{S,4}$ for $S = \{2, 3, \infty\}$

In this section we determine $\mathbb{Q}_{S,4}$ (for $S = \{2, 3, \infty\}$) as the splitting field of a polynomial over $\mathbb{Q}$ of degree $8 + 16 + 16$. The main ingredients are the previous two sections and taking into account the maximal (abelian) exponent 2 subfield $\mathbb{Q}_{S,2}$ of $\mathbb{Q}_{S,4}$.

If $N_1, N_2 \in \mathcal{N}_S$ is a pair such that $\overline{\langle t_3 \rangle} \cap N_1 \cap N_2$ is trivial, then the minimal transitive degree of $G_{S,4}/N_i$ is equal to 16 or 32. There are 12 such pairs with the minimal transitive degree of the quotient equal to 16 for both $i = 1, 2$. Denote the set of the 8 N_i's appearing in such a pair by $\mathcal{N}_{S,1}$. For 6 of them the index in $G_{S,4}$ is equal to 512 and for 2 of them it is equal to 2048. The pairs are precisely the 12 combinations of one of both indices.

Denote the set of all conjugacy classes of subgroups of $G_{S,4}$ of index dividing 16 by $\mathcal{H}$. For each $[H] \in \mathcal{H}$ compute the coset action $G_{S,4} \to S_{[G_{S,4}:H]}$. Denote its kernel by $N_{[H]}$ (the normal core of H in $G_{S,4}$) and its image as a transitive group by $T_{[H]}$.

As a bonus one can deduce that $\mathbb{Q}_{S,4}$ is not equal to the Galois closure of a compositum of extensions of $\mathbb{Q}$ of degree dividing 8 and one field of degree dividing 16, namely the intersection N of $N_{[H]}$ over all $H \in \mathcal{H}$ of index dividing 8 is non-trivial and $N \cap N_{[H]}$ is also non-trivial for all $[H]$ of index equal to 16. However $\overline{\langle t_3 \rangle} \cap N_1 \cap N_2$ is trivial for some $N_i \in \mathcal{N}_{S,1}$ (as above). Hence $\mathbb{Q}_{S,4}$ is the splitting field of a polynomial over $\mathbb{Q}$ of degree $8 + 16 + 16 = 40$ and this is the lowest possible degree.

Consider for each $N \in \mathcal{N}_{S,1}$ the $[H] \in \mathcal{H}$ such that $N = N_{[H]}$. The N's can be divided into three cases according to the transitive groups $T_{[H]}$:

1. $T_{[H]}$ is isomorphic (as transitive groups) to 16T824, 16T867, 16T915 or 16T926. There are four such N's with $[G_{S,4} : N] = 512$.

2. $T_{[H]}$ is isomorphic to 16T956, 16T960, 16T985 or 16T996. Two such N's with $[G_{S,4} : N] = 512$.

3. $T_{[H]}$ is isomorphic to 16T1468. Two such N's with $[G_{S,4} : N] = 2048$.

Notice that $N_{[H]} \in \mathcal{N}_{S,1}$ for all $[H] \in \mathcal{H}$ such that $T_{[H]}$ of the type given in the first and third cases. However this is false for the second case. Denote the subset of $\mathcal{N}_{S,1}$ corresponding to the first and last cases by $\mathcal{N}_{S,2}$. Hence we can identify the fields corresponding to the subgroups in $\mathcal{N}_{S,2}$ as the Galois closure of the degree 16 extensions of $\mathbb{Q}$ with the listed transitive Galois groups.

In order to avoid computing all degree 16 extensions K of $\mathbb{Q}$ unramified outside S we derive restrictions on $K \cap \mathbb{Q}_{S,2}$ and the intermediate fields.

Denote the maximal (abelian) exponent two quotient of $G_{S,4}$ by $G_{S,2}$ and let $\pi : G_{S,4} \to G_{S,2}$ be the canonical homomorphism. For $[H] \in \mathcal{H}$ such that $N_{[H]} \in \mathcal{N}_{S,2}$ the index of $\pi(H)$ is equal to 2 if $T_{[H]}$ is isomorphic to 16T824 or 16T867 and it is index is equal to 4 otherwise.

Recall that $\bar{s}_3 = \pi(s_3)$, $\bar{t}_3 = \pi(t_3)$ and $\bar{t}_\infty = \pi(t_\infty)$ form a basis of $G_{S,2}$. If $[H] \in \mathcal{H}$ such that $T_{[H]}$ is isomorphic to 16T915 or 16T926, then $\pi(H) = \langle \bar{s}_3\bar{t}_3\bar{t}_\infty \rangle$ or $\pi(H) = \langle \bar{s}_3\bar{t}_\infty \rangle$, that is $\pi(H)$ corresponds to $\mathbb{Q}\big(i, \sqrt{6}\big)$ or $\mathbb{Q}(\zeta_{12})$. If $[H] \in \mathcal{H}$ such that $T_{[H]}$ is isomorphic to 16T1468, then $\pi(H) = \langle \bar{t}_\infty \rangle$, that is $\pi(H)$ corresponds to $\mathbb{Q}\big(\sqrt{2}, \sqrt{3}\big)$.

Let $[H] \in \mathcal{H}$ such that $T_{[H]}$ is isomorphic to 16T915 or 16T926. A subgroup $H' \subset G_{S,4}$ of index 8 such that $H \subset H' \subset \pi^{-1}\pi(H)$ has $T_{H'}$ isomorphic to 8T9. Similarly for $T_{[H]}$ isomorphic to 16T1468 the corresponding $T_{H'}$ is isomorphic to 8T31.

In the first subsection we recall how to compute exponent two extensions. This is used in the second subsection to determine up to isomorphism all subfields of $\mathbb{Q}_{S,4}$ with Galois group over $\mathbb{Q}$ equal to 16T915, 16T926 or 16T1468.

6.5.1 Exponent two extensions

Let K be a number field, $\mathcal{O}_K$ the maximal order of K and S a finite set of primes of $\mathcal{O}_K$ containing the primes above 2. Denote the group of principal ideals in $\mathcal{O}_K$ by $\mathcal{P}$ and the group of invertible ideals by $\mathcal{I}$. We briefly recall how to compute the maximal Galois extension of K unramified outside S having exponent two Galois group. Recall that a group of exponent two is abelian. This subsection is roughly based on [10, Section 5.6].

According to Kummer theory the exponent two extensions of K correspond to the subgroups of $K^*/{K^*}^2$. Consider the following commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & {\mathcal{O}_K}^* \arrow[r] \arrow[d] & K^* \arrow[r] \arrow[d] & \mathcal{P} \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & {\mathcal{O}_K}^* \arrow[r] & K^* \arrow[r] & \mathcal{P} \arrow[r] & 1,
\end{tikzcd}$$

where the rows are the usual exact sequences and the vertial maps correspond to $x \mapsto x^2$. Apply the Snake Lemma and use the unique factorization into prime ideals to obtain the exact sequence

$$1 \longrightarrow {\mathcal{O}_K}^*/{\mathcal{O}_K}^{*2} \longrightarrow K^*/{K^*}^2 \longrightarrow \mathcal{P}/\mathcal{P}^2 \longrightarrow 1.$$

Consider another commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & \mathcal{P} \arrow[r] \arrow[d] & \mathcal{I} \arrow[r] \arrow[d] & \mathrm{Cl}\,(\mathcal{O}_K) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \mathcal{P} \arrow[r] & \mathcal{I} \arrow[r] & \mathrm{Cl}\,(\mathcal{O}_K) \arrow[r] & 1,
\end{tikzcd}$$

where again the vertical maps correspond to $x \mapsto x^2$. This gives the exact sequence

$$1 \longrightarrow \mathrm{Cl}\,(\mathcal{O}_K)[2] \longrightarrow \mathcal{P}/\mathcal{P}^2 \longrightarrow \mathcal{I}/\mathcal{I}^2 \longrightarrow \mathrm{Cl}\,(\mathcal{O}_K)/\mathrm{Cl}\,(\mathcal{O}_K)^2 \longrightarrow 1.$$

Together the two exact sequences describe all exponent two extensions of K. In particular such an extension is unramified outside S if and only if the image of the corresponding subgroup of $K^*/{K^*}^2$ in $\mathcal{I}/\mathcal{I}^2$ is contained in the subgroup generated by the primes in S.

We can now compute the maximal exponent two extension of K unramified outside S (with S finite) as follows: Compute a basis $\mathfrak{p}_1\mathcal{I}^2, \ldots, \mathfrak{p}_m\mathcal{I}^2$ of the intersection of the kernel of

$$\mathcal{I}/\mathcal{I}^2 \longrightarrow \mathrm{Cl}\,(\mathcal{O}_K)/\mathrm{Cl}\,(\mathcal{O}_K)^2$$

with the subgroup $\langle \mathfrak{p}\mathcal{I}^2 : \mathfrak{p} \in S \rangle$. Compute a basis $\mathfrak{q}_1\mathcal{P}, \ldots, \mathfrak{q}_{\tilde{m}}\mathcal{P}$ of $\mathrm{Cl}\,(\mathcal{O}_K)[2]$. Compute generators p_i and q_j of $\mathfrak{p}_i$ and $\mathfrak{q}_j^2$ respectively. Compute generators $\zeta, u_1, \ldots, u_n$ of the unit group ${\mathcal{O}_K}^*$. The desired extension is given by

$$K\Big(\sqrt{\zeta}, \sqrt{u_1}, \ldots, \sqrt{u_n}, \sqrt{p_1}, \ldots, \sqrt{p_m}, \sqrt{q_1}, \ldots, \sqrt{q_{\tilde{m}}}\Big).$$

6.5.2 The number fields

In this subsection we describe how to compute the number fields $\mathbb{Q}_{S,4}^H$ discussed earlier up to isomorphism.

Consider a number field $K/\mathbb{Q}$ with Galois group 16T915 or 16T926. In this case we have

$$\mathbb{Q} \longrightarrow L \longrightarrow M \longrightarrow K$$

with $L = \mathbb{Q}\big(i, \sqrt{6}\big)$ or $L = \mathbb{Q}(\zeta_{12})$, and the Galois group of M equal to 8T9. Such M are listed in Table 6.4. For all fields M in this table and for all quadratic extensions K' of M unramified outside S compute the Galois group of $K'/\mathbb{Q}$. This gives 23 and 26 number fields with Galois group 16T915 and 16T926 respectively. Since some of them are isomorphic, we consider them up to isomorphism and find 8 isomorphism classes of number fields for both groups. The number of classes agrees with the number of conjugacy classes in $\mathcal{H}$ inducing a transitive group isomorphic to 16T915 and 16T926 respectively. The defining polynomials are given in Tables 6.5 and 6.6.

Next consider a number field $K/\mathbb{Q}$ with Galois group 16T1468. In this case we have

$$\mathbb{Q} \longrightarrow \mathbb{Q}\Big(\sqrt{2}, \sqrt{3}\Big) \longrightarrow M \longrightarrow K$$

with the Galois group of $M/\mathbb{Q}$ isomorphic to 8T31. The possible M are given in Table 6.7. Following the same procedure as before we find up to isomorphism 64 number fields K with Galois group 16T1468, which agrees with the number of conjugacy classes in $\mathcal{H}$ associated with this transitive group. The defining polynomials of the number fields K are listed in Table 6.8.

Hence $\mathbb{Q}_{S,4}$ is the splitting field of the product of a polynomial from Table 6.3 with a polynomial from either Table 6.5 or 6.6 with a polynomial from Table 6.8.

Table 6.4: Of the 28 number fields $M/\mathbb{Q}$ with Galois group 8T9 unramified outside $S = \{2, 3, \infty\}$ (up to isomorphism) listed in [29], only the following three and three fields contain $\mathbb{Q}(\zeta_{12})$ and $\mathbb{Q}(i, \sqrt{6})$ respectively.

$$x^8 - 2x^6 + 2x^4 - 4x^2 + 4$$
$$x^8 - 6x^6 + 14x^4 - 12x^2 + 4$$
$$x^8 - 6x^6 + 6x^4 + 36x^2 + 36$$

$$x^8 - 4x^7 + 16x^6 - 32x^5 + 54x^4 - 64x^3 + 52x^2 - 32x + 10$$
$$x^8 - 8x^6 + 24x^4 - 32x^2 + 25$$
$$x^8 + 30x^4 + 9$$

Table 6.5: Up to isomorphism all the number fields K unramified outside $S = \{2, 3, \infty\}$ with Galois group equal to 16T915:

$$x^{16} - 6x^{12} + 72x^{10} + 198x^8 - 216x^6 + 1404x^4 - 1296x^2 + 324$$
$$x^{16} + 4x^{14} + 12x^{12} + 20x^{10} + 32x^8 + 44x^6 + 36x^4 + 28x^2 + 25$$
$$x^{16} - 4x^{14} + 4x^{12} - 8x^{10} + 48x^8 - 88x^6 + 88x^4 - 32x^2 + 4$$
$$x^{16} - 12x^{14} + 60x^{12} - 180x^{10} + 432x^8 - 972x^6 + 2052x^4 - 2916x^2 + 2025$$
$$x^{16} - 12x^{14} + 84x^{12} - 396x^{10} + 1296x^8 - 2916x^6 + 4428x^4 - 4212x^2 + 2025$$
$$x^{16} - 4x^{14} + 12x^{12} - 32x^{10} + 80x^8 - 104x^6 + 72x^4 - 16x^2 + 4$$
$$x^{16} + 12x^{14} + 60x^{12} + 144x^{10} + 144x^8 + 216x^6 + 1512x^4 + 1296x^2 + 324$$
$$x^{16} - 4x^{14} + 4x^{12} + 4x^{10} - 4x^6 - 20x^4 + 4x^2 + 25$$

6.6 Frobenius elements

Given a finite Galois extension K of $\mathbb{Q}$, we know by the Čhebotarev Density Theorem that every conjugacy class of $\mathrm{Gal}\,(K/\mathbb{Q})$ contains at least one automorphism obtained by lifting the Frobenius automorphism of the residue field corresponding to a prime in $\mathcal{O}_K$.

In this section we compute such a prime for every conjugacy class in the Galois group $G = G_{S,4}$ of the maximal exponent four extension $K = \mathbb{Q}_{S,4}$ of $\mathbb{Q}$ unramified outside 2, 3 and ∞. As K is the compositum of three fields, we choose the following polynomials

$$\begin{aligned} f_1 &= x^8 + 4x^6 + 4x^4 - 2, \\ f_2 &= x^{16} - 4x^{14} + 4x^{12} + 4x^{10} - 4x^6 - 20x^4 + 4x^2 + 25, \\ f_3 &= x^{16} - 20x^{12} + 84x^8 + 96x^6 - 128x^4 - 96x^2 - 8. \end{aligned}$$

from Tables 6.3, 6.5 and 6.8 respectively. Denote the splitting field of f_i by K_i. Let G_i be the Galois group of $K_i/\mathbb{Q}$.

Our first attempt to compute the Frobenius elements of K was as follows. For many primes compute the conjugacy class of Frobenius elements in G_i. This way

Table 6.6: Up to isomorphism all the number fields K unramified outside $S = \{2, 3, \infty\}$ with Galois group equal to 16T926:

$$x^{16} + 8x^{14} + 28x^{12} + 56x^{10} + 90x^8 + 136x^6 + 148x^4 + 88x^2 + 25$$
$$x^{16} - 12x^{14} + 60x^{12} - 216x^{10} + 504x^8 - 216x^6 + 216x^4 + 324$$
$$x^{16} + 8x^{14} + 10x^{12} - 40x^{10} - 54x^8 + 40x^6 + 76x^4 + 16x^2 + 4$$
$$x^{16} + 4x^{12} - 16x^{10} + 26x^8 - 32x^6 + 12x^4 + 16x^2 + 25$$
$$x^{16} - 12x^{14} + 66x^{12} - 216x^{10} + 450x^8 - 216x^6 + 756x^4 + 324$$
$$x^{16} - 24x^{12} - 72x^{10} + 126x^8 + 1296x^6 + 3672x^4 + 4536x^2 + 2025$$
$$x^{16} + 24x^{14} + 204x^{12} + 648x^{10} + 72x^8 - 2592x^6 + 2808x^4 - 1296x^2 + 324$$
$$x^{16} + 8x^{14} + 34x^{12} + 80x^{10} + 114x^8 + 88x^6 + 52x^4 + 16x^2 + 4$$

Table 6.7: Of the 16 number fields $M/\mathbb{Q}$ with Galois group 8T31 unramified outside $S = \{2, 3, \infty\}$ (up to isomorphism) listed in [29], only the following 8 fields contain $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

$$x^8 - 10x^4 - 12x^2 - 2$$
$$x^8 - 10x^4 + 12x^2 - 2$$
$$x^8 - 4x^6 + 2x^4 + 4x^2 - 2$$
$$x^8 + 4x^6 + 2x^4 - 4x^2 - 2$$
$$x^8 - 12x^6 + 42x^4 - 36x^2 - 18$$
$$x^8 + 12x^6 + 42x^4 + 36x^2 - 18$$
$$x^8 - 18x^4 - 36x^2 - 18$$
$$x^8 - 18x^4 + 36x^2 - 18$$

one obtains a triple of conjugacy classes at every prime. Unfortunately this fails to give as many triples as G has conjugacy classes, because some distinct conjugacy classes in G give identical triples of conjugacy classes in the G_i's.

Instead we use the method for computing Frobenius elements as described in [15]. Let $f = f_1 f_2 f_3$ and

$$f = (x - \alpha_1) \cdots (x - \alpha_n)$$

with $\alpha_i \in K$. Consider G as a subgroup of S_n by the action on the α_i. Every element from a given conjugacy class of G has the same cycle type, but an element from a different conjugacy class of G can have the same cycle type as well. In [15] for every conjugacy class C of G the following polynomials are introduced

$$\Gamma_C = \prod_{\sigma \in C} \left(x - \sum_{i=1}^{\deg f} h(\alpha_i)\sigma(\alpha_i) \right)$$

where $h \in \mathbb{Z}[x]$ is a fixed polynomial of $\deg h < \deg f$ such that the Γ_C's are coprime in $\mathbb{Q}[X]$ for different conjugacy classes C of G. Notice that $\Gamma_C \in \mathbb{Z}[x]$ and

Table 6.8: Up to isomorphism half of the number fields K unramified outside $S = \{2, 3, \infty\}$ with Galois group equal to 16T1468 are listed below. Substitute ix for x to obtain the other half.

$$x^{16} - 16x^{14} + 60x^{12} + 32x^{10} - 284x^{8} - 576x^{6} - 576x^{4} - 288x^{2} - 72$$
$$x^{16} - 16x^{14} + 92x^{12} - 208x^{10} + 106x^{8} + 184x^{6} - 268x^{4} + 592x^{2} - 1058$$
$$x^{16} - 20x^{12} + 42x^{8} - 264x^{6} + 340x^{4} - 528x^{2} - 2$$
$$x^{16} - 20x^{12} + 84x^{8} - 96x^{6} - 128x^{4} + 96x^{2} - 8$$
$$x^{16} - 24x^{14} + 220x^{12} - 1056x^{10} + 2874x^{8} - 4200x^{6} + 2380x^{4} + 672x^{2} - 1058$$
$$x^{16} - 28x^{12} - 240x^{10} - 686x^{8} - 888x^{6} - 540x^{4} - 144x^{2} - 18$$
$$x^{16} - 32x^{12} - 120x^{10} + 246x^{8} + 648x^{6} - 236x^{4} - 48x^{2} - 2$$
$$x^{16} - 40x^{12} - 120x^{10} - 2x^{8} + 312x^{6} + 180x^{4} - 144x^{2} - 18$$
$$x^{16} - 44x^{12} - 96x^{10} - 54x^{8} + 72x^{6} + 52x^{4} - 2$$
$$x^{16} - 4x^{12} + 4x^{8} - 96x^{6} - 288x^{4} - 288x^{2} - 72$$
$$x^{16} - 52x^{12} - 48x^{10} + 226x^{8} - 120x^{6} + 324x^{4} - 288x^{2} - 18$$
$$x^{16} - 56x^{12} - 168x^{10} + 6x^{8} + 216x^{6} + 52x^{4} - 2$$
$$x^{16} - 8x^{14} - 12x^{12} + 160x^{10} - 68x^{8} + 192x^{6} - 1872x^{4} - 864x^{2} - 72$$
$$x^{16} - 8x^{14} + 12x^{12} + 16x^{10} - 68x^{8} - 288x^{6} - 432x^{4} - 288x^{2} - 72$$
$$x^{16} - 8x^{14} - 12x^{12} + 256x^{10} - 686x^{8} + 360x^{6} + 396x^{4} - 288x^{2} - 18$$
$$x^{16} - 8x^{14} - 16x^{12} + 152x^{10} + 142x^{8} - 600x^{6} - 996x^{4} - 432x^{2} - 18$$
$$x^{16} - 8x^{14} - 16x^{12} + 88x^{10} + 118x^{8} - 88x^{6} - 4x^{4} + 32x^{2} - 2$$
$$x^{16} - 8x^{14} + 20x^{12} + 16x^{10} - 134x^{8} + 104x^{6} + 44x^{4} - 16x^{2} - 2$$
$$x^{16} - 8x^{14} + 20x^{12} - 16x^{10} - 302x^{8} + 456x^{6} + 1356x^{4} - 18$$
$$x^{16} - 8x^{14} + 20x^{12} - 16x^{10} + 34x^{8} - 120x^{6} + 60x^{4} - 18$$
$$x^{16} - 8x^{14} + 28x^{12} - 80x^{10} + 172x^{8} + 352x^{6} - 3152x^{4} + 6496x^{2} - 4232$$
$$x^{16} - 8x^{14} + 32x^{12} - 232x^{10} + 622x^{8} + 552x^{6} - 996x^{4} - 432x^{2} - 18$$
$$x^{16} - 8x^{14} + 32x^{12} - 40x^{10} - 50x^{8} + 360x^{6} - 372x^{4} + 144x^{2} - 18$$
$$x^{16} - 8x^{14} + 32x^{12} - 8x^{10} - 218x^{8} + 104x^{6} + 236x^{4} + 800x^{2} - 1250$$
$$x^{16} - 8x^{14} + 44x^{12} - 64x^{10} - 14x^{8} + 168x^{6} + 12x^{4} - 144x^{2} - 18$$
$$x^{16} - 8x^{14} - 4x^{12} + 32x^{10} - 110x^{8} + 360x^{6} + 924x^{4} - 720x^{2} - 18$$
$$x^{16} - 8x^{14} - 4x^{12} + 64x^{10} + 106x^{8} + 8x^{6} - 100x^{4} - 64x^{2} - 2$$
$$x^{16} - 8x^{14} - 52x^{12} - 176x^{10} - 500x^{8} - 1024x^{6} - 1264x^{4} - 736x^{2} - 8$$
$$x^{16} - 8x^{14} + 80x^{12} - 296x^{10} + 118x^{8} + 1256x^{6} - 244x^{4} - 2080x^{2} - 1058$$
$$x^{16} - 8x^{14} + 8x^{12} + 40x^{10} - 122x^{8} + 104x^{6} - 4x^{4} - 16x^{2} - 2$$
$$x^{16} - 8x^{14} - 8x^{12} - 8x^{10} + 262x^{8} - 440x^{6} + 268x^{4} - 272x^{2} - 2$$
$$x^{16} - 8x^{14} + 8x^{12} + 8x^{10} - 2x^{8} - 24x^{6} + 12x^{4} - 18$$

Γ_C is independent of the ordering of the α_i. In particular

$$\sigma \in C \Longleftrightarrow \Gamma_C\left(\sum_{i=1}^{\deg f} h(\alpha_i)\sigma(\alpha_i)\right) = 0.$$

To determine the conjugacy class of a Frobenius element at the prime p, it is sufficient to compute the roots of f in $K_p/\mathbb{Q}_p$ and use the equivalence above.

6.6.1 Computing the polynomials Γ_C

Suppose that we know the group G and its action on the α_i with the α_i as elements of $\mathbb{C}$. Given a polynomial h, to which precision do we need to compute the α_i in order to correctly compute the Γ_C's?

Consider α_i as an element in $\mathbb{C}$. If $n = |C|$ and $\Gamma_C = \sum_{i=0}^{n} c_i x^i$, then

$$|c_i| \le \binom{n}{i} M_C^{n-i},$$

where

$$M_C = \max_{\sigma \in C}\left|\sum_{i=1}^{\deg f} h(\alpha_i)\sigma(\alpha_i)\right| \le \deg f \cdot \max_i |h(\alpha_i)| \cdot \max_i |\alpha_i|.$$

This gives an upper bound on $\max|c_i|$ depending only on f, h, i and n.

6.6.2 Searching for a polynomial h

The choices $h = x$ and $h = x^2$ (as suggested in [15]) in our case both give Γ_C's with the resultant of some pairs equal to zero. The choice $h = x^3 - 3x$ does work. Below we explain how to obtained our h.

We need to find a polynomial h such that the resultant of every pair of Γ_C is nonzero. Moreover we would like the coefficients of the Γ_C's to be small.

Again take the α_i as elements in $\mathbb{C}$. Let $h = \sum_{i=0}^{\deg(f)-1} a_i x^i$. We consider h as an element $\left(a_0, \ldots, a_{\deg(f)-1}\right)$ from the lattice $\mathbb{Z}^{\deg f}$ with quadratic form $Q = M^\dagger M$, where the natural choice for M would be the matrix with rows

$$\left(\sigma(\alpha_i), \alpha_i\sigma(\alpha_i), \ldots, \alpha_i^{\deg(f)-1}\sigma(\alpha_i)\right)$$

for every $i = 1, \ldots, \deg f$ and every $\sigma \in G$. Unfortunately, at the time of writing Magma is unable to compute the Galois group of (reducible) f with $\alpha_i \in \mathbb{C}$. Instead we use the (sub)matrix M with rows for $i = 1, 2, 3$

$$\left(\sigma(\beta), \beta\sigma(\beta), \ldots, \beta^{\deg(f)-1}\sigma(\beta)\right)$$

where β runs over the roots of f_i and $\sigma \in G_i$. Starting from the shortest h we consider h of increasing length until we find a h whose Γ_C have pairwise non-zero resultants modulo a prime less than 100. This way we find

$$h = x^3 - 3x.$$

6.6.3 Computing the Frobenius elements

Given a prime $p \geq 5$ we now describe how to determine the conjugacy class of a Frobenius element σ at p. We need to determine the cycle type of σ, compute the sum $\sum_{i=1}^{\deg f} h(\alpha_i)\sigma(\alpha_i)$ and evaluate the Γ_C in this sum for all conjugacy classes C with the same cycle type as σ.

The cycle type of σ can be read off from the factorization of f over $\mathbb{Q}_p$, that is every irreducible factor corresponds to a cycle of length equal to its degree. Denote the set of irreducible factors by F.

As K_p is an unramified extension of $\mathbb{Q}_p$ of degree dividing 4, the polynomial f will certainly split completely over the unramified extension L_p of $\mathbb{Q}_p$ of degree 4.

Every α_i is the root of a unique $g \in F$. Using that $\sigma(\alpha_i)$ is also a root of g and $\sigma(\alpha_i) = \alpha_i^p \mod p$, we compute $\sigma(\alpha_i)$ with the Hensel Lemma. This gives the sum $\sum_{i=1}^{\deg f} h(\alpha_i)\sigma(\alpha_i)$ as an element of L_p.

This procedure works for every prime from 5 to 2999999 inclusive except for $p = 7$. For unclear reasons Magma fails to compute the Hensel lift at $p = 7$ for two irreducible polynomials in F of degree 2. However computing $\sigma(\alpha_i)$ is trivial for irreducible polynomials of degree 2.

6.6.4 The primes

Table 6.9 contains for every conjugacy class C of G the smallest prime p such that the Frobenius element at p is contained in C. If one is only interested in the primes such that every conjugacy class of G contains a power of a Frobenius element, then the primes in Table 6.10 can be *omitted*.

6.7 Consequences for the Faltings method

By combining the just computed list of primes with the Faltings method described in the previous chapter, we can easily derive two results concerning certain two-dimensional abelian varieties over $\mathbb{Q}$.

Theorem 6.1. *Let A_1 and A_2 be abelian varieties of dimension two defined over $\mathbb{Q}$. If A_1 and A_2 have good reduction at every prime $p \neq 2, 3$, the degree of $\mathbb{Q}(A_1[2], A_2[2])/\mathbb{Q}$ is a power of two and for every prime p in Table 6.9 the characteristic polynomials of Frobenius for A_1 and A_2 are equal, then A_1 and A_2 are isogeneous over $\mathbb{Q}$.*

Proof. Denote the absolute Galois group of $\mathbb{Q}$ by $G_{\mathbb{Q}}$. Let $\rho_i : G_{\mathbb{Q}} \to \mathrm{GL}_4(\mathbb{Z}_2)$ be the Galois representation on the Tate modules $\mathrm{T}_2 A_i \cong {\mathbb{Z}_2}^4$. Denote the residue representation by $\bar{\rho}_i$. Since the residue representation $\bar{\rho}_i$ factors as

$$G_{\mathbb{Q}} \longrightarrow \mathrm{Gal}\left(\mathbb{Q}(A_1[2], A_2[2])/\mathbb{Q}\right) \longrightarrow \mathrm{GL}_4(\mathbb{F}_2)$$

and the degree of $\mathbb{Q}(A_1[2], A_2[2])/\mathbb{Q}$ is a power of two, the image of $\bar{\rho}_i$ is a 2-group.

Table 6.9: Every conjugacy class of Gal$(K/\mathbb{Q})$ contains a Frobenius element at precisely one of the primes below. These primes are also the smallest possible.

5	167	563	1607	3529	7607	15887	65521
7	173	577	1609	3673	7873	16417	66841
11	179	593	1619	3719	7919	16631	69457
13	181	599	1657	3767	8161	18289	71233
17	191	601	1753	3769	8231	18433	71329
19	193	653	1777	3793	8641	18457	74353
23	199	659	1801	3889	8689	18481	101281
29	211	673	1823	3911	8737	18503	103969
31	229	719	1871	3947	9311	18793	118369
37	233	739	1873	4057	9601	19441	139921
41	239	743	1993	4127	9697	21001	149377
43	241	769	2017	4273	9721	21601	155569
47	257	839	2063	4297	9817	22441	161377
53	263	863	2087	4391	10007	22679	166417
59	269	881	2113	4441	10369	25969	168601
61	271	887	2137	4463	11447	26881	170353
67	283	937	2281	4561	11617	27529	186481
71	293	983	2351	4583	11689	29017	197233
73	311	1009	2377	4729	12049	29879	230977
79	313	1031	2393	4801	12241	30937	231169
83	331	1033	2521	4919	12409	33073	253681
89	337	1129	2593	5209	12743	34849	264289
97	347	1151	2617	5233	12841	34919	457153
103	359	1153	2663	5449	13249	36097	515041
107	373	1163	2687	5569	13417	37057	519553
109	379	1201	2689	5639	13633	38711	597697
113	409	1223	2713	5641	13921	39841	710641
127	431	1249	2833	5879	14087	40177	830497
131	433	1319	2999	6047	14449	42577	836833
139	449	1321	3119	6121	14737	48817	862417
149	457	1439	3167	6337	14929	49681	926977
151	479	1481	3313	6983	15121	54217	1484737
157	499	1487	3433	7393	15313	55681	1501009
163	521	1583	3499	7559	15649	57697	2977153

Table 6.10: The conjugacy class in Gal$(K/\mathbb{Q})$ of a Frobenius element at a prime below contains the power of a Frobenius element at a smaller prime.

3673	29017	155569	515041	862417
5209	30937	161377	597697	1501009
10369	101281	231169	830497	2977153

Let Σ be the set of Frobenius elements at the primes in Table 6.9 and $N = G_{\mathbb{Q}}$. The characters of the representations ρ_i are equal by Theorem 5.1. Since the ρ_i are semi-simple by [16, Satz 3], they are isomorphic by [6, §20, No. 6, Proposition 6]. From Corollary 1 to [16, Satz 4] follows that A_1 and A_2 are isogeneous over $\mathbb{Q}$. □

The theorem above can be strengthend a bit by excluding the primes in Table 6.10, because the Frobenius elements at these primes are conjugate to a power of a Frobenius element at the remaining primes in Table 6.9.

Theorem 6.2. *The number of isogeny classes of two-dimensional abelian varieties A over $\mathbb{Q}$ with good reduction at every prime $p \neq 2, 3$ and the degree of $\mathbb{Q}(A[2])/\mathbb{Q}$ a power of two is at most* $2.2 \cdot 10^{1783}$.

Proof. Let A be a two-dimensional abelian variety over $\mathbb{Q}$ and p a prime of good reduction. The characteristic polynomial of Frobenius at p is an example of a Weil polynomial, that is of the form

$$x^4 - a_1x^3 + \big(a_1^2 - a_2\big)x^2 - a_1px + p^2$$

with a_1, a_2 integers such that $|a_1| \leq 4\sqrt{p}$ and $|a_2| \leq 4p$. So there are at most $\big(8\sqrt{p}+1\big)(8p+1)$ such polynomials.

The upper bound on the number of isogeny classes follows by computing

$$\prod_p (8\sqrt{p}+1)(8p+1)$$

where p ranges over the primes in Table 6.9 excluding those in Table 6.10. □

6.7.1 The case $S = \{2, \infty\}$

In the case of $\mathbb{Q}$ and $S = \{2, \infty\}$ a stronger version of Theorem 6.1 is essentially described in [22]. Since the degree of $\mathbb{Q}_{S,4}/\mathbb{Q}$ is lower than in the case of $\{2, 3, \infty\}$, less primes need to be checked. More importantly the image of $G_{\mathbb{Q}} \to \mathrm{GL}_4(\mathbb{F}_2)$ is in fact a 2-group, because of the non-existence of number fields unramified outside S of degree $d \leq 15$ not a power of 2, see [28] and its references. This results in:

Theorem 6.3 (Grenié [22])**.** *Let A_1 and A_2 be abelian varieties of dimension two defined over $\mathbb{Q}$. If A_1 and A_2 have good reduction at every prime $p \neq 2$ and for every prime p in*

$$\{5, 7, 11, 17, 23, 31\}$$

the characteristic polynomials of Frobenius for A_1 and A_2 are equal, then A_1 and A_2 are isogeneous over $\mathbb{Q}$.

Also Theorem 6.2 can be strengthend in this case:

Theorem 6.4. *The number of isogeny classes of two-dimensional abelian varieties A over $\mathbb{Q}$ with good reduction at every prime $p \neq 2$ is at most* $9.3 \cdot 10^{20}$.

6.8 Other exponent 4 extensions

Let K be a number field and S a finite set of places of K including the primes above 2 and the real infinite places. Suppose that A_1 and A_2 are two-dimensional abelian varieties defined over K with good reduction at the finite primes not in S. Denote the Galois representation on the Tate module of A_i by $\rho_i : G_K \to \operatorname{Aut}(\mathrm{T}_2 A_i)$.

In order to use the Faltings method to compare the Galois representations we could compute the maximal exponent four extension of $L = K(A_1[2], A_2[2])$ unramified outside S. Then the deviation map δ factors as

$$G_K \longrightarrow \operatorname{Gal}(L_{S,4}/K) \longrightarrow \delta(G_K).$$

However, based on Section 6.2 we expect the degree of $L_{S,4}/K$ to be much bigger than the order of the deviation group $\delta(G_K)$. Recall from the previous chapter that the order of the latter group is less than 2^{32}.

Instead of computing $L_{S,4}$ consider the field M such that G_M is the kernel of $\rho_1 \times \rho_2$. Denote the maximal exponent four extension of L in M by L_M. The deviation map δ factors as

$$G_K \longrightarrow \operatorname{Gal}(L_M/K) \longrightarrow \delta(G_K).$$

Define $M_i = K(A_i[2^\infty])$. Notice that $G_{M_i} = \ker \rho_i$ and $M = M_1 \cdot M_2$. Observe that M is a subfield of the maximal 2-extension of L unramified outside S. On the other hand the field M_i and therefore also M contains $K(\zeta_{2^\infty})$.

We can study L_M using the arithmetic of A_i, namely: What is $A_i(L_M)[2^\infty]$? By adjoining the points in this group to L we obtain a subfield of L_M.

6.8.1 Elliptic curve example

Let $K = \mathbb{Q}$. Recall

$$E_1 : y^2 = x^3 - 39x - 70 = (x-7)(x+2)(x+5)$$

with $\Delta(E_1) = 2^8 3^8$ and $j(E_1) = \frac{2^4 13^3}{3^2}$. It has good reduction at $p \geq 5$ and potential multiplicative reduction at $p = 3$. Now we will study $E_1(L_M)[2^\infty]$.

First we show that $E_1(L_M)[2^\infty]$ contains $E_1[8]$. The induced map

$$\tilde{\rho} : \operatorname{Gal}(\mathbb{Q}(E_1[8])/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$$

is injective. Since the two-torsion points of E_1 are rational, $\tilde{\rho}(\sigma) = 1 + 2A_\sigma$ with $A_\sigma \in \mathrm{M}_2(\mathbb{Z}/8\mathbb{Z})$. So $\operatorname{Gal}(\mathbb{Q}(E_1[8])/\mathbb{Q})$ has exponent 4, because $(1+2A_\sigma)^4 = 1$. Hence $\mathbb{Q}(E_1[8]) \subset L_M$ and the claim follows.

Let $p \geq 5$. Since L_M/K is of exponent 4 and unramified at p, the degree of the residue field of $\mathcal{O}_{L_M}$ at p over $\mathbb{F}_p$ divides 4. As E_1 has good reduction p we obtain an injective homomorphism

$$E_1(L_M)[2^\infty] \longrightarrow \bar{E}_1\big(\mathbb{F}_{p^4}\big)[2^\infty].$$

Thus $|E_1(L_M)[2^\infty]|$ divides $\left|\bar{E}_1\big(\mathbb{F}_{p^4}\big)\right|$. The latter is easily derived from $\left|\bar{E}_1(\mathbb{F}_p)\right|$ and $\bar{E}_1(\mathbb{F}_{q^n}) = q^n + 1 - a_n$ with $a_2 = a_1^2 - 2q$.

Suppose that $p = 5$, then $\bar{E}_1 : y^2 = x^3 + x$ and $\bar{E}_1(\mathbb{F}_5) = 4$. Now $\bar{E}_1(\mathbb{F}_{25}) = 32$ and $\bar{E}_1(\mathbb{F}_{625}) = 640 = 128 \cdot 5$. Therefore $|E_1(L_M)[2^\infty]|$ divides 128. Similar if $p = 7$, then $\left|\bar{E}_1(\mathbb{F}_{7^4})\right| = 256 \cdot 9$. Hence $E_1(L_M)[2^\infty]$ is isomorphic to either $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ or $\mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.

Alternatively we can use the potential multiplicative reduction of E_1 at $p = 3$. The elliptic curve E_1 is isomorphic over $\mathbb{Q}\big(\sqrt{3}\big)$ to

$$E_1' : {y'}^2 = (x' + 1)x'(x' - 3)$$

with the isomorphism given by $x' = \frac{x+2}{3}$ and $y' = \frac{y}{3\sqrt{3}}$. The latter curve has split multiplicative reduction at 3, because the tangent lines at the node $(0,0)$ of $\bar{E}_1'$ are defined over $\mathbb{F}_3$. Thus E_1' is isomorphic over $\mathbb{Q}_3$ to the Tate curve E_q with $q \in \mathbb{Q}_3$ such that

$$j(E_q) = \frac{1}{q} + 744 + \dots.$$

In fact $q = u \cdot 3^2$ with $u \in \mathbb{Z}_3^*$ and $u \equiv 13 \mod 81$. Moreover $E_q\big(\bar{\mathbb{Q}}_3\big) \cong \bar{\mathbb{Q}}_3^*/q^{\mathbb{Z}}$ as Galois modules. Observe that the x-coordinate of a point on E_1 of order 4 satisfies

$$0 = 2(x-1)(x+11)\big(x^2 - 14x - 59\big)\big(x^2 + 4x + 31\big)$$

and that the discriminant of the degree 2 terms are $2^4 3^3$ and $-2^2 3^3$ respectively. So $\sqrt{3} \in L_M$. Hence

$$E_1(L_M) \cong E_1'(L_M) \longrightarrow E_1'(\mathbb{Q}_{3,4}) \cong \mathbb{Q}_{3,4}^*/q^{\mathbb{Z}},$$

where $\mathbb{Q}_{3,4} = \mathbb{Q}_3\big(\zeta_{16}, \sqrt[4]{3}\big)$ is the maximal exponent four extension of $\mathbb{Q}_3$. Since $E_1'[2^\infty]$ is rational over the maximal 2-extension $\hat{\mathbb{Q}}_3$ of $\mathbb{Q}_3$, we can deduce the subgroup $\mathbb{Q}_{3,4}^*/q^{\mathbb{Z}}[2^\infty]$ from the Galois action on $\hat{\mathbb{Q}}_3^*/q^{\mathbb{Z}}[2^\infty]$. Recall that

$$\left\langle s, t : t^2\left[t^{-1}, s^{-1}\right]\right\rangle$$

is a pro-2 presentation of $\mathrm{Gal}\left(\hat{\mathbb{Q}}_3/\mathbb{Q}\right)$ and the subgroup $\left\langle s^4, t^4\right\rangle$ corresponds to $\mathbb{Q}_{3,4}$. Suppose that $n = 2^k$, then $\hat{\mathbb{Q}}_3^*/q^{\mathbb{Z}}[n] = \left\langle \zeta_n \cdot q^{\mathbb{Z}},\ \sqrt[n]{q} \cdot q^{\mathbb{Z}}\right\rangle$ where $q = v\,\sqrt[n]{3}^2$ with $v^n = u$. Hensel's lemma implies that $v \in \mathbb{Q}_3$, because $u \equiv 1 \mod 3$. With respect to the basis $\left\{\zeta_n \cdot q^{\mathbb{Z}},\ \sqrt[n]{q} \cdot q^{\mathbb{Z}}\right\}$

$$[\rho(s)] = \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad [\rho(t)] = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}.$$

The vector $(a,b)^T$ is fixed by $\left[\rho\big(s^4\big)\right]$ and $\left[\rho\big(t^4\big)\right]$ if and only if $16a \equiv 0 \mod n$ and $8b \equiv 0 \mod n$. Hence

$$\mathbb{Q}_{3,4}^*/q^{\mathbb{Z}}[2^\infty] = \left\langle \zeta_{16} \cdot q^{\mathbb{Z}},\ \sqrt[8]{q} \cdot q^{\mathbb{Z}}\right\rangle \cong \mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}.$$

Using the good reduction at $p = 5$ or the potential multiplicative reduction at $p = 3$ we now know that $E_1(L_M)[2^\infty]$ is isomorphic to either $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ or $\mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. With Magma we show that $E_1(L_M)[2^\infty]$ has a point of order 16: Let ψ_8 and ψ_{16} be the 8- and 16-division polynomials of E_1. Factor $\frac{\psi_{16}}{\psi_8}$ over $\mathbb{Q}(E_1[8])$ as $f_1 \cdots f_{24}$ with f_i irreducible of degree 4. Let k be the residue field of $\mathcal{O}_{\mathbb{Q}(E_1[8])}$ at a prime above 5, then $k \cong \mathbb{F}_{5^4}$. If $E_1(L_M)$ contains a point of order 16, then its x-coordinate is a zero of f_j for some j and f_j factors into linear terms over k as L_M has exponent 4. Precisely 8 of the f_i's factor completely over k, say $f_1, \ldots, f_8$. Let N be an extension of $\mathbb{Q}(E_1[8])$ obtained by adding a root x_{16} of f_1. Using Magma one verifies that over N the equation $y^2 = x_{16}^3 - 39x_{16} - 70$ has two roots, that is $E_1(N)$ has a point[1] of order 16. Let g_1 be the minimal polynomial over $\mathbb{Q}$ of a primitive element of $\mathbb{Q}(E_1[8])$ and g_2 be the minimal polynomial of x_{16} over $\mathbb{Q}$. Now N is the splitting field of g_1g_2. Compute the Galois group of g_1g_2 and verify that the exponent of $\mathrm{Gal}\,(N/\mathbb{Q})$ is indeed 4. Hence $N \subset L_M$ and $E_1(L_M)$ contains a point of order 16. The computation also shows that $[\mathbb{Q}(E_1[8]) : \mathbb{Q}] = 16$ and $[N : \mathbb{Q}] = 64$.

Remark 6.5. This subsection is related to determining the image of the Galois representation on the 2-adic Tate module of E_1. According to [52] (obtained via [11]) the image is generated by

$$\begin{pmatrix} 1 & 0 \\ 0 & 7 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 4 & 5 \end{pmatrix}, \begin{pmatrix} 3 & 6 \\ 4 & 7 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_2).$$

Using Magma we find that the exponent four quotient of the image has order 128. Therefore the subfield N of L_M computed above is a proper subfield.

6.9 Open questions

We determined the field $\mathbb{Q}_{S,4}$ for $S = \{2, 3, \infty\}$ by carefully selecting subgroups of $G_{S,4}$ and searching for the fields corresponding to these subgroups. Here we used the images of s_3, t_3 and t_∞ in the abelian exponent two quotient of $G_{S,4}$ and Kummer theory to limit the search for the number fields. This raises the following question: Is it possible to further limit the search by using that s_3 is a Frobenius element above 3 and similar for t_3 and t_∞?

As mentioned in the introduction, this chapter is motivated by applying the Faltings method to $\mathrm{Jac}\,(C)$ of a genus two curve C and $E_1 \times E_2$. Since the two-torsion points of E_2 are not rational, it appears infeasible to compute the maximal exponent four extension of $\mathbb{Q}(\mathrm{Jac}\,(C)[2], E_1[2], E_2[2])$. We ask: Is it feasible to compute the maximal exponent four subfield of

$$\mathbb{Q}(\mathrm{Jac}\,(C)[2^\infty], E_1[2^\infty], E_2[2^\infty])?$$

[1] Notice that $E_1(N)$ has in fact 64 points of order 16 (by adding a point of order 8), so f_i splits completely over N for $i = 1, \ldots, 8$.

A (partial) description of the Galois group of the maximal 2-extension is also available for global function fields. A natural question therefore is: Can one compute the maximal exponent four extension of a global function field?

Chapter 7

Van Wamelen method

In this chapter we compute morphisms from a genus two curve to an elliptic curve using the complex uniformization of the associated Jacobian varieties. The method is essentially the same as the one described in [72, 73], where it is used to compute endomorphisms of a Jacobian variety and morphisms between genus two curves, respectively. The p-adic analog of this method is introduced in [30] without explicit computation of morphisms.

We describe the complex uniformization method in Section 7.1 and give an application in Section 7.2.

7.1 Theory

We describe the method from [72] in the context of determining a morphism between curves.

Let K be a number field. Consider two curves C_i defined over K with rational points $O_i \in C_i(K)$ for $i = 1, 2$ and a morphism $\phi : C_1 \to C_2$ defined over a finite extension L of K sending O_1 to O_2. Denote the Jacobian variety of C_i by $\mathrm{Jac}\,(C_i)$. By [46, Section 6],

$$\begin{tikzcd} C_1 \arrow[r] \arrow[d, "\phi"'] & \mathrm{Jac}\,(C_1) \arrow[d, "\phi_*"] \\ C_2 \arrow[r] & \mathrm{Jac}\,(C_2) \end{tikzcd}$$

is a commutative diagram of varieties over K. Associate to each of the algebraic varieties and morphisms their analytic versions. Recall that the underlying set of C_i^{an} is equal to $C_i(\mathbb{C})$ and that $\phi : C_1 \to C_2$ is completely determined by the induced map $C_1(\mathbb{C}) \to C_2(\mathbb{C})$. So ϕ is actually determined by ϕ^{an}.

The analytic Jacobian variety $\mathrm{Jac}\,(C_i)^{\mathrm{an}}$ has a simple description in terms of the dual of the $\mathbb{C}$-vector space $\Omega^1_{C_i^{\mathrm{an}}}$ of regular one forms and the first homology group $\mathrm{H}_1\left(C_i^{\mathrm{an}}, \mathbb{Z}\right)$. Write Λ_i for the image of the homomorphism

$$\begin{aligned} \mathrm{H}_1\left(C_i^{\mathrm{an}}, \mathbb{Z}\right) &\longrightarrow {\Omega^1_{C_i^{\mathrm{an}}}}^* \\ \gamma &\longmapsto \left(\omega \mapsto \int_\gamma \omega\right). \end{aligned}$$

The analytic Jacobian variety $\mathrm{Jac}\left(C_i\right)^{\mathrm{an}}$ is isomorphic to ${\Omega^1_{C_i^{\mathrm{an}}}}^*/\Lambda_i$ and the morphism $C_i \to \mathrm{Jac}\left(C_i\right)$ becomes the morphism

$$\begin{aligned} C_i^{\mathrm{an}} &\longrightarrow {\Omega^1_{C_i^{\mathrm{an}}}}^*/\Lambda_i \\ P &\longmapsto \left(\omega \mapsto \int_{O_i}^P \omega\right) + \Lambda_i. \end{aligned}$$

The morphism $\phi_*^{\mathrm{an}} : \mathrm{Jac}\left(C_1\right)^{\mathrm{an}} \to \mathrm{Jac}\left(C_2\right)^{\mathrm{an}}$ is induced by the dual of the linear map $\phi^{\mathrm{an}*} : \Omega^1_{C_2^{\mathrm{an}}} \to \Omega^1_{C_1^{\mathrm{an}}}$.

We can determine ϕ_*^{an} by solving a linear system as follows. Choose a set of generators $\alpha_i = \{\gamma_{i1}, \ldots, \gamma_{i2g_i}\}$ of $\mathrm{H}_1\left(C_i^{\mathrm{an}}, \mathbb{Z}\right)$ and a basis $\beta_i = \{\omega_{i1}, \ldots, \omega_{ig_i}\}$ of $\Omega^1_{C_i/K}$ with g_i the genus of C_i. Since β_i is a basis of $\Omega^1_{C_i^{\mathrm{an}}}$ too, this induces an isomorphism ${\Omega^1_{C_i^{\mathrm{an}}}}^* \to \mathbb{C}^{g_i}$. The lattice Λ_i considered as a subgroup of $\mathbb{C}^{g_i}$ is generated by the *period matrix*

$$[\Lambda_i] = \begin{pmatrix} \int_{\gamma_{i1}} \omega_{i1} & \cdots & \int_{\gamma_{i2g_i}} \omega_{i1} \\ \vdots & & \vdots \\ \int_{\gamma_{i1}} \omega_{ig_i} & \cdots & \int_{\gamma_{i2g_i}} \omega_{ig_i} \end{pmatrix} \in \mathrm{M}_{g_i \times 2g_i}(\mathbb{C}).$$

Since $\phi^{\mathrm{an}*}$ is the $\mathbb{C}$-linear extension of $\phi^* : \Omega^1_{C_2/L} \to \Omega^1_{C_1/L}$, with respect to the bases β_i we have $[\phi^{\mathrm{an}*}] \in \mathrm{M}_{g_1 \times g_2}(L)$. The dual map $\phi^{\mathrm{an}**}$ induces a map between the analytic Jacobians if and only if $\phi^{\mathrm{an}**}(\Lambda_1) \subset \Lambda_2$, that is

$$[\phi^{\mathrm{an}*}]^{\mathrm{T}}[\Lambda_1] = [\Lambda_2]B$$

with $B \in \mathrm{M}_{2g_2 \times 2g_1}(\mathbb{Z})$. Notice that by scaling this system by some integer and choosing a basis of $\mathcal{O}_L$ the problem reduces to computing integer solutions of a linear system.

We can reconstruct $\phi : C_1 \to C_2$ from ${\phi_*}^{\mathrm{an}}$ as follows. Consider C_i as a curve in $\mathbb{A}^2$ with coordinates x_i, y_i. The rational map ϕ is defined by two rational functions in x_1, y_1 with coefficients in $\mathcal{O}_L$. Take the coefficients as variables. If ϕ is regular at $P \in C_1(\mathbb{C})$, then evaluating ϕ at P gives linear equations. To compute $\phi(P)$ use the following commutative diagram

$$\begin{tikzcd} C_1(\mathbb{C}) \arrow[r] \arrow[d, "\phi"'] & \mathrm{Jac}\left(C_1\right)(\mathbb{C}) \arrow[d, "\phi_*"'] & {\Omega^1_{C_1^{\mathrm{an}}}}^*/\Lambda_1 \arrow[l, "\cong"'] \arrow[d, "\phi^{\mathrm{an}**}"'] \\ C_2(\mathbb{C}) \arrow[r] & \mathrm{Jac}\left(C_2\right)(\mathbb{C}) & {\Omega^1_{C_2^{\mathrm{an}}}}^*/\Lambda_2 \arrow[l, "\cong"'] \end{tikzcd}$$

Given sufficiently many distinct points, the coefficients can be obtained by solving the linear system of equations.

7.2 Application

Consider the hyperelliptic curve C defined by

$$y^2 = \bigl(x^3 + 60x + 20\bigr)(60x + 20)(60x - 60),$$

the elliptic curve E_1 defined by

$$y_1^2 = x_1^3 - 39x_1 - 70$$

and the elliptic curve E_2 defined by

$$y_2^2 = x_2^3 - 52500x_2 - 5537500.$$

As mentioned in Section 4.5, we expect $\operatorname{Jac}(C)$ and $E_1 \times E_2$ to be isogeneous. Using the method described in the previous section, we will compute morphisms $\phi_i : C \to E_i$ defined over $\mathbb{Q}$ for $i = 1, 2$ using Magma.

We first compute the homomorphisms $\operatorname{Jac}(C)^{\mathrm{an}} \to E_i^{\mathrm{an}}$ for $i = 1, 2$ by the following steps.

1. Compute the period matrices P_C and P_E of C and E

$$P_C = \begin{pmatrix} p_{11} & p_{12} & p_{13} & p_{14} \\ p_{21} & p_{22} & p_{23} & p_{24} \end{pmatrix} \quad \text{and} \quad P_E = \begin{pmatrix} q_{11} & q_{12} \end{pmatrix}$$

2. Rewrite the linear system $A^{\mathrm{T}} P_C = P_E B$ as $Mv = 0$ with

$$M = \begin{pmatrix} p_{11} & p_{21} & -q_{11} & 0 & 0 & 0 & -q_{12} & 0 & 0 & 0 \\ p_{12} & p_{22} & 0 & -q_{11} & 0 & 0 & 0 & -q_{12} & 0 & 0 \\ p_{13} & p_{23} & 0 & 0 & -q_{11} & 0 & 0 & 0 & -q_{12} & 0 \\ p_{14} & p_{24} & 0 & 0 & 0 & -q_{11} & 0 & 0 & 0 & -q_{12} \end{pmatrix}$$

and

$$v = \begin{pmatrix} a_{11} & a_{21} & b_{11} & b_{12} & \dots & b_{24} \end{pmatrix}^{\mathrm{T}}$$

3. Find integer solutions using the LLL method as suggested by [72]. The lattice is the one with the standard basis of $\mathbb{R}^{10}$ as generators and with the quadratic form given by the matrix

$$I + \frac{1}{\varepsilon}\Bigl(M^{\dagger}M + \bigl(M^{\dagger}M\bigr)^{\mathrm{T}}\Bigr)$$

where ε is the precision.

We find for E_1 and E_2 respectively that

$$A_1 = \begin{pmatrix} 200 \\ 100 \end{pmatrix} \cdot n_1, \quad B_1 = \begin{pmatrix} -3 & 0 & 0 & 1 \\ -3 & -2 & -1 & 0 \end{pmatrix} \cdot n_1$$

and

$$A_2 = \begin{pmatrix} -20 \\ 20 \end{pmatrix} \cdot n_2, \quad B_2 = \begin{pmatrix} 2 & 0 & 0 & 1 \\ -1 & -3 & 1 & -2 \end{pmatrix} \cdot n_2$$

for $n_1, n_2 \in \mathbb{Z}$.

Recall from Section 4.5 that we expected $\operatorname{Jac}(C)$ and $E_1 \times E_2$ are $(5,5)$-isogeneous. This is supported by the above computation as the degree of the isogeny is equal to the index of the lattice of C in the lattice of $E_1 \times E_2$, and this index is equal to the absolute value of

$$\det \begin{pmatrix} B_1 \\ B_2 \end{pmatrix} = -25 n_1^2 n_2^2.$$

We continue by computing the x_i-coordinate of the morphism $C \to E_i$ and assume that the morphism is compatible with the hyperelliptic involution. In this case x_i is a function of x only.

1. Suppose that the x_i is a rational function in x of degree at most 5 defined over $\mathbb{Q}$, that is

$$x_i = \frac{c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0}{d_5x^5 + d_4x^4 + d_3x^3 + d_2x^2 + d_1x + d_0}$$

with $c_i, d_i \in \mathbb{Z}$.

2. Choose 12 points from $C(\mathbb{C})$ with distinct x-coordinates and compute the image on $E_i(\mathbb{C})$ by chasing the diagram

$$\begin{tikzcd} C(\mathbb{C}) \arrow[r] & {\Omega^1_{C^{\mathrm{an}}}}^{*}/\Lambda_C \arrow[d, "\bar{A}^{\mathrm{T}}"] \\ E_i(\mathbb{C}) \arrow[r] & {\Omega^1_{E_i^{\mathrm{an}}}}^{*}/\Lambda_{E_i} \end{tikzcd}$$

3. Find integer solutions to the resulting linear system as above.

Following these steps we obtain

$$x_1 = \frac{9x^5 - 50x^4 + 740x^3 + 60x^2 - 160x - 32}{25x^4 - 100x^3 + 60x^2 + 80x + 16}$$

and

$$x_2 = \frac{27x^5 - 60x^4 + 3850x^3 + 17700x^2 + 11475x + 2000}{3x^4 - 8x^3 + 6x^2 - 1}.$$

We still need to compute the y_i as a function of x, y. Instead of using the same method as above, we solve the defining equation for E_i in the function field $\mathbb{Q}(C)$. As a bonus this proves the computation is correct. Since the mentioned equation has two solutions, we choose the one that is compatible with the matrix A_i. The functions are

$$y_1 = \frac{9}{20} \frac{x^5 - 8x^4 - 48x^3 - 64x^2 - 16x}{125x^6 - 750x^5 + 1200x^4 + 200x^3 - 960x^2 - 480x - 64} y$$

and

$$y_2 = \frac{27}{20} \frac{3x^6 - 10x^5 - 415x^4 - 4780x^3 - 6875x^2 - 3050x - 425}{9x^7 - 39x^6 + 61x^5 - 35x^4 - 5x^3 + 11x^2 - x - 1} y.$$

Hence we obtain explicit morphisms $\phi_i : C \to E_i$ defined over $\mathbb{Q}$ for $i = 1, 2$ that together induce a $(5, 5)$-isogeny $\mathrm{Jac}\,(C) \to E_1 \times E_2$. This confirms the expectation from Section 4.5.

Conclusion

We conclude this thesis by briefly discussing the results and a number of open questions for each of the chapters.

In Chapter 1 we studied elliptic curves E over $\mathbb{F}_q$ such that E is maximal over a finite extension of $\mathbb{F}_q$. The discussion is separated in two cases, namely E is supersingular and E is ordinary. In the former case we extended the work of [14] to provide a complete picture. Our main contribution is to the latter case of ordinary elliptic curves. Lower bounds on linear forms in logarithms proved to be the key ingredients to explicitly limit the degree of the field extensions over which E may be maximal. However this limit is not strict as is shown by ineffective methods. Indeed computer experiments suggest that the degree of such extensions is at most 5 for $q > 5$. We believe different techniques are necessary to improve the effective and ineffective upper bounds on the degree of the field extension. A result from sieve theory allowed us to prove an observation made in [65] on elliptic curves over $\mathbb{F}_p$ maximal over a cubic extension. It is unknown to us if a similar proof also works in the quintic case.

In Chapter 2 we constructed from a pair of elliptic curves with complex multiplication a genus 2 curves over $\mathbb{Q}$ or over quadratic number fields, and gave a precise description of when their reduction modulo a prime above p is maximal over $\mathbb{F}_{p^2}$. This showed that the technique used in [35] for genus $g = 3$ can also be applied in the case $g = 2$. For some pairs of complex multiplication our method does not work over $\mathbb{Q}$. It is unknown to us if this is due to our construction of the genus 2 curve or that such curves simply do not exist over $\mathbb{Q}$. We considered only 4 out of the 13 possible endomorphism rings of elliptic curves over $\mathbb{Q}$ with complex multiplication. This leaves the question open whether or not our construction also works for the remaining endomorphism rings.

In Chapter 3 we constructed a family of elliptic curves of which every elliptic curve has the same Galois representation on their 3-torsion subgroup. Although such families are not new, we used the Hesse pencil to obtain an elementary proof of its universal property. It complements earlier proofs in [53] using the theory of modular curves and in [17] using invariant theory.

In Chapter 4 we studied the Jacobian variety of the Mestre curve $C_{a,b}$ for various a, b. We found that $\operatorname{Jac}(C_{a,b})$ is isogeneous to $E_{a,b}^2 \times \operatorname{Jac}(D_{a,b})^2$ with $E_{a,b}$ an elliptic curve and $D_{a,b}$ a genus 2 curve. Since $\operatorname{Jac}(D_{a,b})$ is in general simple, it is not possible to improve the lower bound on the rank of the elliptic curves in the family from [67, Theorem 3]. A computer experiment suggested that for some values of a, b the $\mathrm{Jac}\,(D_{a,b})$ is isogeneous to a product of elliptic curves, but $E_{a,b}$ is not one of those factors. It is unknown to us if there are any a, b such that $E_{a,b}$ is a factor of $\mathrm{Jac}\,(D_{a,b})$.

In Chapter 5 we extended the explicit version of the Faltings method described in [10] for the special case of 2-dimensional 2-adic representations to arbitrary finite dimensional p-adic representations of a profinite group. This is closely related to [22], although our version puts more emphasis on the residue representations.

In Chapter 6 we analysed maximal Galois extensions of number fields unramified outside a given finite set of places with Galois group of exponent 4. We succeeded in computing such an extension of $\mathbb{Q}$ unramified outside 2, 3 and ∞ as the splitting field of a degree 40 polynomial over $\mathbb{Q}$, and adapted the method in [15] to compute a Frobenius element for every conjugacy class in the Galois group. In general these extensions are currently too large to compute explicitly. Therefore it is impossible to apply our explicit version of the Faltings method to the Jacobian variety of the curve $D_{a,b}$ with $a = 60$ and $b = 20$ from Chapter 4. Possibly an improved explicit version can be obtained by studying subfields of $\mathbb{Q}(A_1[2^\infty], A_2[2^\infty])$ for given abelian surfaces A_1 and A_2 over $\mathbb{Q}$. Another open question is how many of the primes in Table 6.9 are necessary for Theorem 6.1 to be true. A partial answer would follow from an extension of [64] to genus 2 curves over $\mathbb{Q}$ with good reduction outside 2 and 3 such that the field of definition of the Weierstrass points of the curve has degree a power of 2.

In Chapter 7 we applied complex uniformation as in [72, 73] in the slightly different context of a morphism from a genus 2 curve to an elliptic curve. We explicitly computed a morphism from the curve $D_{a,b}$ with $a = 60$ and $b = 20$ from Chapter 4 to each of the elliptic factors of its Jacobian variety. It would be interesting to see if the same could be achieved with 3-adic uniformization, because both elliptic curves have potential multiplicative reduction at 3.

Samenvatting

De Nederlandse titel van het voorliggende proefschrift luidt:

De arithmetiek van maximale krommen, het Hessepenceel en de Mestrekromme

Dit proefschrift is het resultaat van het bestuderen van vragen binnen drie onderwerpen uit de arithmetische meetkunde. Hieronder geven wij per onderwerp een beknopte wetenschappelijke beschrijving van de vragen en de resultaten, en noemen wij kort enkele nieuwe problemen die uit dit werk voortkomen.

Maximale krommen

Het eerste onderwerp gaat over krommen over eindige lichamen met veel rationale punten op de kromme. Het aantal rationale punten op een kromme C van geslacht g over een eindig lichaam $\mathbb{F}_q$ met q elementen voldoet aan de bekende Hasse-Weil-Serre-grens

$$q+1-g\lfloor 2\sqrt{q}\rfloor \le |C(\mathbb{F}_q)| \le q+1+g\lfloor 2\sqrt{q}\rfloor.$$

We noemen de kromme C *maximaal* over $\mathbb{F}_q$ indien de bovengrens wordt bereikt.

In hoofdstuk 1 beschouwen wij elliptische krommen E over $\mathbb{F}_q$ en stellen wij de vraag: Bestaat er een eindige uitbreiding van $\mathbb{F}_q$ waarover E maximaal is? Het antwoord is afhankelijk van het supersingulier dan wel gewoon zijn van E. Schrijf

$$a_1 = q+1-|E(\mathbb{F}_q)|.$$

Als E supersingulier is, oftewel $\operatorname{ggd}(a_1, q) \neq 1$, dan bestaan er in het geval $a_1 \neq -\sqrt{q}, 2\sqrt{q}$ oneindig veel uitbreidingen van $\mathbb{F}_q$ waarover E maximaal is, maar in het geval $a_1 = -\sqrt{q}, 2\sqrt{q}$ komen deze uitbreidingen in zijn geheel niet voor. Het antwoord voor gewone E is minder volledig. Met behulp van de theorie van lineaire vormen in logaritmen verkrijgen wij een expliciete bovengrens op de graad van de uitbreiding waarover E maximaal is. Vervolgens verbeteren wij met ineffectieve methoden de bovengrens tot 11 voor voldoende grote q. Een computerberekening laat voor priemmachten $q < 10^6$ zien dat enkel de graden 3 (zie tabel 1.2 voor $q < 10^3$), 5 (zie tabel 1.3), 7 (bij $q = 5$ en $a_1 = 1$) en 13 (bij $q = 2$ en $a_1 = 1$)

daadwerkelijk voorkomen; de graden 3 en 5 lijken oneindig vaak voor te komen. Een resultaat uit de zeeftheorie bevestigt het bestaan van oneindig veel priemgetallen p met een elliptische kromme over $\mathbb{F}_p$ die maximaal is over $\mathbb{F}_{p^3}$. Het is bij ons onbekend of eenzelfde resultaat mogelijk is voor graad 5.

In hoofdstuk 2 maken wij geslacht-2-krommen C over $\mathbb{Q}$ en over kwadratische getallenlichamen doormiddel van een vezelproduct van twee elliptische krommen E_1 en E_2 elk met complexe vermenigvuldiging. Hierbij kiezen wij krommen E_i met endomorfismenring $\mathbb{Z}[\zeta_3]$, $\mathbb{Z}[i]$, $\mathbb{Z}\left[\frac{1}{2}+\frac{1}{2}\sqrt{-7}\right]$ of $\mathbb{Z}\left[\sqrt{-2}\right]$. Voor alle mogelijke paren van deze ringen vinden wij een kromme C die in 7 gevallen is gedefinieerd over $\mathbb{Q}$ en in de resterende 3 gevallen is gedefinieerd over een kwadratisch getallenlichaam. Vanwege de complexe vermenigvuldiging van E_1 en E_2 hebben wij een nauwkeurige beschrijving (via een congruentierelatie) van de priemen $\mathfrak{p}$ waarvoor de reductie $E_{i,\mathfrak{p}}$ van E_i bij $\mathfrak{p}$ supersingulier is. In het bijzonder weten wij de priemgetallen p, waarvan de reducties $E_{1,\mathfrak{p}}$ en $E_{2,\mathfrak{p}}$ bij priemen $\mathfrak{p}$ boven p maximaal zijn over $\mathbb{F}_{p^2}$. Per constructie is de Jacobivariëteit $\mathrm{Jac}\,(C)$ van C isogeen met $E_1 \times E_2$. Dus weten wij hetzelfde voor de reducties van C. De bovengenoemde endomorfismenringen zijn slechts 4 van de 13 mogelijkheden in het geval van elliptische krommen over $\mathbb{Q}$ met complexe vermenigvuldiging. Er resteert de vraag of onze constructie ook werkt voor de overige ringen.

Het Hessepenceel

Het tweede onderwerp betreft een familie van elliptische krommen over een perfect lichaam k van karakteristiek ongelijk aan 2 en 3, waarbij de Galoisvoorstelling op de 3-torsieondergroep hetzelfde is voor alle elliptische krommen in de familie. De constructie van de familie van krommen gaat als volgt: Zij E een elliptische kromme over k met vergelijking $F = 0$ en $F \in k[X, Y, Z]$ een homogeen kubisch polynoom. Schrijf

$$\mathrm{Hess}\,(F) = \det \begin{pmatrix} \frac{\partial^2 F}{\partial X^2} & \frac{\partial^2 F}{\partial X \partial Y} & \frac{\partial^2 F}{\partial X \partial Z} \\ \frac{\partial^2 F}{\partial X \partial Y} & \frac{\partial^2 F}{\partial Y^2} & \frac{\partial^2 F}{\partial Y \partial Z} \\ \frac{\partial^2 F}{\partial X \partial Z} & \frac{\partial^2 F}{\partial Y \partial Z} & \frac{\partial^2 F}{\partial Z^2} \end{pmatrix}.$$

Het *Hessepenceel* van E is de kromme $\mathcal{E}$ over $k(t)$ met vergelijking

$$tF + \mathrm{Hess}\,(F) = 0.$$

Wij vatten $k(t)$ op als het functielichaam van $\mathbb{P}^1$. Daardoor kunnen wij spreken van een vezel E_{t_0} van $\mathcal{E}$ boven $t_0 \in \mathbb{P}^1(k)$. Merk op dat $E_\infty = E$.

Zij ook E' een elliptische kromme over k. Een isomorfisme $\phi : E[3] \to E'[3]$ van de voorstellingen $\rho : G_k \to \mathrm{Aut}\,(E[3])$ en $\rho' : G_k \to \mathrm{Aut}\,(E'[3])$ heet *symplectisch* als ϕ compatibel is met de Weilparingen op de 3-torsieondergroepen.

In hoofdstuk 3 laten wij zien dat alle elliptische krommen in de bovenstaande familie dezelfde Galoisvoorstelling hebben op de 3-torsieondergroep en geven wij een eenvoudig bewijs van de universele eigenschap van deze familie: Als E en E'

zijn beschreven door middel van een Weierstrassvergelijking over k, dan is E' over k isomorf met een vezel E_{t_0} voor een zekere t_0 in $\mathbb{P}^1(k)$ dan en slechts dan als er een symplectisch isomorfisme $\phi : E[3] \to E'[3]$ bestaat. Wij laten zien dat de buigpunten van E precies de punten zijn die alle krommen E_{t_0} in het Hessepenceel $\mathcal{E}$ gemeenschappelijk hebben. Voor een elliptische kromme met een Weierstrassvergelijking is een buigpunt hetzelfde als een punt van orde 1 of 3. Ook is de Weilparing op $E_{t_0}[3]$ hetzelfde voor alle elliptische krommen E_{t_0}. Dus $E_{t_0}[3] = E[3]$ als groepen en voor de Weilparing. Wij bepalen een Weierstrassvergelijking voor $\mathcal{E}$ en daarmee ook voor E_{t_0}. Een isomorfisme tussen E_{t_0} met Weierstrassvergelijking en E' is nu een projectieve lineaire afbeelding die volledig vast ligt door zijn beperking tot de 3-torsieondergroepen. Er zijn precies 24 groepsisomorfismen $E[3] \to E'[3]$ die compatibel zijn met de Weilparing, en er zijn evenzoveel isomorfismen $E_{t_0} \to E'$ met variërende t_0 in $\mathbb{P}^1\big(\overline{k}\big)$. Oftewel als er een symplectisch isomorfisme tussen $E[3]$ en $E'[3]$ bestaat, dan bestaat er ook een t_0 zo dat E_{t_0} over $\overline{k}$ isomorf is met E'. De universele eigenschap van het Hessepenceel $\mathcal{E}$ volgt nu uit een toepassing van stelling 90 van Hilbert.

De Mestrekromme

Het derde en laatste onderwerp bestaat eigenlijk uit een aantal verschillende deelonderwerpen, maar allemaal zijn zij gemotiveerd door de volgende vraag: Hoe ziet de ontbinding van de Jacobivariëteit van de Mestrekromme er op isogenie na uit?

In hoofdstuk 4 beginnen wij met de vergelijking van de *Mestrekromme* $C_{a,b}$

$$v^2 = g_{ab}(u) := -ab\big(u^2+1\big)\Big[b^2\big(u^4+u^2+1\big)^3 + a^3\big(u^2+1\big)^2u^4\Big],$$

over een lichaam k. Deze kromme heeft de eigenschap, dat er twee onafhankelijke morfismen $C_{a,b} \to E_{a,b}$ bestaan, waarbij $E_{a,b}$ de elliptische kromme over k is met vergelijking

$$y^2 = x^3 + ax + b.$$

Door automorfismen van $C_{a,b}$ te bepalen en de correspondentie tussen krommen en functielichamen te benutten, vinden wij quotiëntkrommen van $C_{a,b}$. Dit herhalen wij voor de quotiënten. De automorfismen van een kromme induceren idempotentrelaties op zijn Jacobivariëteit. Zodoende vinden wij de ontbinding

$$\operatorname{Jac}(C_{a,b}) \sim_k E_{a,b}^2 \times \operatorname{Jac}(D_{a,b})^2,$$

waarbij $D_{a,b}$ de geslacht-2-kromme is met vergelijking

$$y^2 = \big(x^3+ax+b\big)(ax+b)(ax-3b).$$

Het bestuderen van het karakteristieke polynoom van Frobenius bij $p = 17$ voor $a = 1$, $b = 1$ laat zien dat $\operatorname{Jac}(D_{1,1})$ geometrisch enkelvoudig is over $\mathbb{Q}$. Daarmee is ook $\operatorname{Jac}(D_{a,b})$ geometrisch enkelvoudig over $\mathbb{Q}(a,b)$. Hieruit concluderen wij, dat er voor algemene a, b niet nog een derde onafhankelijk morfisme $C_{a,b} \to E_{a,b}$

bestaat. Een computerberekening suggereert dat voor enkele concrete waarden $a_0, b_0 \in \mathbb{Q}$ de $\mathrm{Jac}\,(D_{a_0,b_0})$ over $\mathbb{Q}$ isogeen is met een product van elliptische krommen. In tabel 4.1 staan de resultaten voor $-1000 \leq a_0, b_0 \leq 1000$ met $a_0 b_0 \bigl(4a_0^3 + 27b_0^2\bigr) \neq 0$. In geen van de gevonden gevallen is E_{a_0,b_0} een factor van $\mathrm{Jac}\,(D_{a_0,b_0})$. Het is ons onbekend of er $a_0, b_0 \in \mathbb{Q}$ voorkomen met E_{a_0,b_0} wel een factor van $\mathrm{Jac}\,(D_{a_0,b_0})$. Verder suggereert de berekening dat $\mathrm{Jac}\,(D_{60,20})$ isogeen is met $E'_{60,20} \times E''_{60,20}$, waarbij

$$y^2 = x^3 - 52500x - 5537500$$

de vergelijking van de elliptische kromme $E''_{60,20}$ is en

$$y^2 = x^3 - 39x - 70 \qquad \text{of} \qquad y^2 = x^3 - 219x + 1190$$

de vergelijking van de elliptische kromme $E'_{60,20}$ is.

In hoofdstuk 5 beschrijven wij een expliciete variant van de Faltingsmethode. Zij G een pro-eindige groep, K een lokaal lichaam, R de ring van gehelen van K en k het restklassenlichaam van R met karakteristiek p. De methode is een criterium om te beslissen of gegeven continue voorstellingen $\rho_1 : G \to \mathrm{GL}_d(R)$ en $\rho_2 : G \to \mathrm{GL}_d(R)$ isomorf zijn. Het hart wordt gevormd door de *afwijkingsafbeelding* $\delta : G \to \delta(G)$ en de *afwijkingsgroep* $\delta(G)$ horende bij de voorstellingen ρ_1 en ρ_2, waarbij $\delta(G)$ het verschil tussen de karakters van ρ_1 en ρ_2 meet. In onze variant benaderen wij $\delta(G)$ aan de hand van de kern N van het product van de restvoorstellingen

$$\bar{\rho} = \bar{\rho}_1 \times \bar{\rho}_2 : G \longrightarrow \mathrm{GL}_d(k) \times \mathrm{GL}_d(k).$$

Onder geschikte voorwaarden heeft de groep $\delta(N)$ exponent p^e met e een geheel getal zo dat $d \leq p^e$. Daarmee kunnen wij onder dezelfde voorwaarden de groep $\delta(N)$ benaderen door G/N^{p^e}, waarbij N^{p^e} de topologische afsluiting is van de groep voortgebracht door alle h^{p^e} met $h \in N$. Ook laten wij zien dat de groep G/N^{p^e} eindig is dan en slechts dan als het pro-p-quotiënt van N eindig voortgebracht is.

In hoofdstuk 6 bestuderen wij de maximale Galoisuitbreiding $K_{S,4}$ van een getallenlichaam K onvertakt buiten een eindig aantal plaatsen S met een Galoisgroep $G_{S,4}$ van exponent 4, waarbij $K = \mathbb{Q}$ of $\mathbb{Q}\bigl(\sqrt[3]{10}\bigr)$ en S een verzameling van plaatsen van K met daarin een aantal priemen boven 2, 3 en 5 en de reële oneindige plaats. Bij de volgende resultaten spelen computerberekeningen met Magma een belangrijke rol. In het algemeen (zie tabel 6.1 voor $|G_{S,4}|$) is $K_{S,4}$ te groot is om uit te rekenen, maar in speciale gevallen is het wel mogelijk: Voor $S = \{2, \infty\}$ is $\mathbb{Q}_{S,4}$ het ontbindingslichaam van een polynoom van graad 8 uit tabel 6.3; voor $S = \{2, 3, \infty\}$ is $\mathbb{Q}_{S,4}$ het compositum van $\mathbb{Q}_{\{2,\infty\},4}$ en de ontbindingslichamen van een polynoom van graad 16 uit tabel 6.5 of 6.6 en een polynoom van graad 16 uit tabel 6.8. In het laatste geval bepalen wij voor elke conjugatieklasse C in $G_{S,4}$ een priem $p \geq 5$ met zijn Frobeniuselement boven p in C, zie tabel 6.9. Hiermee maken wij onze variant van de Faltingsmethode in hoofdstuk 5 volledig expliciet voor abelse oppervlakken A over $\mathbb{Q}$ met goede reductie buiten 2 en 3 en met $\mathbb{Q}(A[2])/\mathbb{Q}$ een 2-uitbreiding, en vinden wij dat er ten hoogstens $2.2 \cdot 10^{1783}$ isogenieklassen van zulke abelse oppervlakken bestaan. Soortgelijke uitspraken doen wij voor abelse oppervlakken over $\mathbb{Q}$ onvertakt buiten 2. Het lijkt op dit moment onmogelijk via de Faltingsmethode aan te tonen dat $\mathrm{Jac}\,(D_{60,20})$ over $\mathbb{Q}$ isogeen is met $E'_{60,20} \times E''_{60,20}$, omdat $K_{S,4}$ in dit geval ($K = \mathbb{Q}\big(\zeta_3, \sqrt[3]{10}\big)$ en S bevat de priemen boven 2, 3 en 5) te groot is om uit te rekenen. Een mogelijke verbetering is het bestuderen van de maximale exponent-4-uitbreiding van $\mathbb{Q}(A_1[2], A_2[2])$ binnen $\mathbb{Q}(A_1[2^\infty], A_2[2^\infty])$ voor abelse oppervlakken A_i in plaats van $K_{S,4}$. Wij geven een eerste aanzet voor een elliptische kromme E over $\mathbb{Q}$ met rationale 2-torsieondergroep door gebruik te maken van de arithmetiek van E.

In hoofdstuk 7 passen wij complexe uniformizatie van abelse variëteiten toe op $\mathrm{Jac}\,(D_{60,20})$, $E'_{60,20}$ en $E''_{60,20}$ om algebraïsche morfismen $D_{60,20} \to E'_{60,20}$ en $D_{60,20} \to E''_{60,20}$ te vinden en expliciet uit te rekenen, waarbij in dit hoofdstuk de elliptische kromme $E'_{60,20}$ de volgende vergelijking heeft:

$$y^2 = x^3 - 39x - 70.$$

De morfismen zijn $D_{60,20} \to E'_{60,20}$ waarbij $(x, y) \mapsto (x_1, y_1)$ met

$$\begin{aligned} x_1 &= \frac{9x^5 - 50x^4 + 740x^3 + 60x^2 - 160x - 32}{25x^4 - 100x^3 + 60x^2 + 80x + 16} \\ y_1 &= \frac{9}{20}\,\frac{x^5 - 8x^4 - 48x^3 - 64x^2 - 16x}{125x^6 - 750x^5 + 1200x^4 + 200x^3 - 960x^2 - 480x - 64}\,y \end{aligned}$$

en $D_{60,20} \to E''_{60,20}$ waarbij $(x, y) \mapsto (x_2, y_2)$ met

$$\begin{aligned} x_2 &= \frac{27x^5 - 60x^4 + 3850x^3 + 17700x^2 + 11475x + 2000}{3x^4 - 8x^3 + 6x^2 - 1} \\ y_2 &= \frac{27}{20}\,\frac{3x^6 - 10x^5 - 415x^4 - 4780x^3 - 6875x^2 - 3050x - 425}{9x^7 - 39x^6 + 61x^5 - 35x^4 - 5x^3 + 11x^2 - x - 1}\,y. \end{aligned}$$

Hiermee volgt dat $\mathrm{Jac}\,(D_{60,20})$ over $\mathbb{Q}$ isogeen is met $E'_{60,20} \times E''_{60,20}$. Een interessante vraag is of de morfismen ook via 3-adische uniformizatie te bepalen zijn, omdat in dit geval beide elliptische krommen potentiële multiplicatieve reductie bij de priem 3 hebben.

Bibliography

[1] M. Artebani and I.V. Dolgachev. The Hesse pencil of plane cubic curves. *L'Enseignement Mathématique*, 55(3-4):235–273, 2009.

[2] A. Baker. The Theory of Linear Forms in Logarithms. In A. Baker and D.W. Masser, editors, *Transcendence Theory: Advances and Applications*, pages 1–27. Academic Press, 1977.

[3] M. Bhargava and A. Shankar. Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. *Annals of Mathematics. Second Series*, 181(1):191–242, 2015.

[4] W. Bosma, J. Cannon, and C. Playoust. The Magma Algebra System I: The User Language. *Journal of Symbolic Computation*, 24(3-4):235–265, 1997.

[5] N. Boston. Galois p-groups unramified at p - a survey. In *Primes and Knots*, volume 416 of *Contemporary Mathematics*, pages 31–40. American Mathematical Society, 2006.

[6] N. Bourbaki. *Algèbre: Chapitre 8, Modules et anneaux semi-simples.* Éléments de mathématique. Springer, new edition, 2012.

[7] C. Breuil, B. Conrad, F. Diamond, and R. Taylor. On the modularity of elliptic curves over $\mathbb{Q}$: Wild 3-adic exercises. *Journal of the American Mathematical Society*, 14(4):843–939, 2001.

[8] Y. Bugeaud. *Approximation by Algebraic Numbers*, volume 160 of *Cambridge tracts in mathematics.* Cambridge University Press, 2004.

[9] J.W.S. Cassels. Diophantine equations with special reference to elliptic curves. *Journal of the London Mathematical Society*, 41(1):193–291, 1966.

[10] G. Chênevert. *Exponential sums, hypersurfaces with many symmetries and Galois representations.* PhD thesis, McGill University, 2008.

[11] J. Cremona. Elliptic Curve Data, September 2015. `doi:10.5281/zenodo.30569`.

[12] F. Diamond and J. Shurman. *A First Course in Modular Forms*, volume 228 of *Graduate Texts in Mathematics.* Springer, 2005.

[13] J.D. Dixon, M.P.F. du Sautoy, A. Mann, and D. Segal. *Analytic Pro-p Groups*, volume 61 of *Cambridge studies in advanced mathematics.* Cambridge University Press, 2nd edition, 2003.

[14] P. Doetjes. Maximale elliptische krommen over eindige lichamen. Bachelor's thesis, Rijksuniversiteit Groningen, 2009. URL: `http://irs.ub.rug.nl/dbi/4a9d2d8a403dc`.

[15] T. Dokchitser and V. Dokchitser. Identify Frobenius elements in Galois groups. *Algebra & Number Theory*, 7(6):1325–1352, 2013.

[16] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Inventiones mathematicae*, 73(3):349–366, 1983.

[17] T.A. Fisher. The Hessian of a genus one curve. *Proceedings of the London Mathematical Society*, 104(3):613–648, 2012.

[18] W. Fulton. Algebraic Curves: An Introduction to Algebraic Geometry. 2008. URL: `http://www.math.lsa.umich.edu/~wfulton/`.

[19] G. van der Geer, E.W. Howe, K.E. Lauter, and C. Ritzenthaler. Tables of curves with many points. Retrieved on 22 September 2016. URL: `http://www.manypoints.org`.

[20] G. van der Geer and M. van der Vlugt. Tables of curves with many points. *Mathematics of Computing*, 69(230):797–810, 2000.

[21] D.R. Grant. A curve for which Coleman's effective Chabauty bound is sharp. *Proceedings of the American Mathematical Society*, 122(1):317–319, 1994.

[22] L. Grenié. Comparison of semi-simplifications of Galois representations. *Journal of Algebra*, 316(2):608–618, 2007.

[23] G.H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers.* Oxford University Press, 4th edition, 1975.

[24] G. Harman and P. Lewis. Gaussian primes in narrow sectors. *Mathematika*, 48(1-2):119–135, 2001.

[25] R. Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate Texts in Mathematics.* Springer, 1977.

[26] E.W. Howe and K.E. Lauter. Improved upper bounds for the number of points on curves over finite fields. *Annales de l'Institut Fourier*, 53(6):1677–1737, 2003.

[27] E.W. Howe and K.E. Lauter. New methods for bounding the number of points on curves over finite fields. In C. Faber, G. Farkas, and R. de Jong, editors, *Geometry and Arithmetic*, EMS Series of Congress Reports, pages 173–212. European Mathematical Society, 2012.

[28] J.W. Jones. Number fields unramified away from 2. *Journal of Number Theory*, 130(6):1282–1291, 2010.

[29] J.W. Jones and D.P. Roberts. A database of number fields. *London Mathematical Society Journal of Computation and Mathematics*, 17(1):595–618, 2014.

[30] S. Kadziela. Rigid analytic uniformization of curves and the study of isogenies. *Acta Applicandae Mathematicae*, 99(2):185–204, 2007.

[31] E. Kani. The number of curves of genus two with elliptic differentials. *Journal für die reine und angewandte Mathematik*, 485:93–121, 1997.

[32] E. Kani and M. Rosen. Idempotent relations and factors of Jacobians. *Mathematische Annalen*, 284(2):307–327, 1989.

[33] H. Koch. l-Erweiterungen mit vorgegebenen Verzweigungsstellen. *Journal für die reine und angewandte Mathematik*, 219:30–61, 1965.

[34] H. Koch. *Galois Theory of p-Extensions.* Springer Monographs in Mathematics. Springer, 2002.

[35] T. Kodama, J. Top, and T. Washio. Maximal hyperelliptic curves of genus three. *Finite Fields and Their Applications*, 15(3):392–403, 2009.

[36] A. Kumar. Hilbert modular surfaces for square discriminants and elliptic subfields of genus 2 function fields. *Research in the Mathematical Sciences*, 2(1):1–46, 2015.

[37] M. Kuwata. Constructing families of elliptic curves with prescribed mod 3 representation via Hessian and Cayleyan curves. 2012. `arXiv:1112.6317v2`.

[38] S. Lang. *Elliptic Functions*, volume 112 of *Graduate Texts in Mathematics.* Springer, second edition, 1987.

[39] M. Laurent, M. Mignotte, and Y. Nesterenko. Formes linéaires en deux logarithmes et déterminants d'interpolation. *Journal of Number Theory*, 55(2):285–321, 1995.

[40] Q. Liu. *Algebraic Geometry and Arithmetic Curves*, volume 6 of *Oxford Graduate Texts in Mathematics.* Oxford University Press, 2002.

[41] R. Livné. Cubic Exponential Sums and Galois Representations. In *Current Trends in Arithmetical Algebraic Geometry*, volume 67 of *Contemporary Mathematics*, pages 247–261. American Mathematical Society, 1987.

[42] A.J.S. Mann. On the orders of groups of exponent four. *Journal of the Londen Mathematical Society. Second Series*, 26(1):64–76, 1982.

[43] G. N. Markšaĭtis. On p-extensions with one critical number. *Izvestiya Akademii Nauk SSSR. Seriya Matematicheskaya*, 27(2):463–466, 1963.

[44] J-F. Mestre. Rang de courbes elliptiques d'invariant donné. *Comptes Rendus de l'Académie des sciences. Série I: Mathématique*, 314:919–922, 1992.

[45] J.S. Milne. Abelian Varieties. In G. Cornell and J.H. Silverman, editors, *Arithmetic Geometry*, pages 103–150. Springer, 1986.

[46] J.S. Milne. Jacobian Varieties. In G. Cornell and J.H. Silverman, editors, *Arithmetic Geometry*, pages 167–212. Springer, 1986.

[47] J.S. Milne. Algebraic geometry, 2015. URL: `http://www.jmilne.org/math/`.

[48] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of Number Fields*. Grundlehren der mathematischen Wissenschaften. Springer, second edition, 2013.

[49] R. Pannekoek. *Topological aspects of rational points on K3 surfaces*. PhD thesis, Universiteit Leiden, 2013. URL: `http://hdl.handle.net/1887/21743`.

[50] The PARI Group. *PARI/GP version 2.7.5*, 2015. URL: `http://pari.math.u-bordeaux.fr/`.

[51] E. Pascal. *Repertorium der Höheren Mathematik: II. Theil: Die Geometrie*. B.G. Teubner, 1902.

[52] J. Rouse and D. Zureick-Brown. Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois. *Research in Number Theory*, 1(1):1–34, 2015.

[53] K. Rubin and A. Silverberg. Families of elliptic curves with constant mod p representations. In J.H. Coates and S.-T. Yau, editors, *Elliptic Curves, Modular Forms and Fermat's Last Theorem*, pages 148–161. International Press, 1993.

[54] J-P. Serre. Nombres de points des courbes algébriques sur $\mathbb{F}_q$. In *Séminaire de Théorie des Nombres de Bordeaux. Année 1982–1983.* Exposé No. 22.

[55] J-P. Serre. Rational points on curves over finite fields. Lectures given at Harvard University. Notes by F.Q. Gouvéa, December 1985.

[56] J-P. Serre. *Lectures on the Mordell-Weil Theorem*, volume 15 of *Aspects of Mathematics: E.* Vieweg, third edition, 1997.

[57] J-P. Serre. Résumé des cours de 1984–1985. In *Œuvres, Collected Papers*, volume IV, 1985–1998. Springer, 2000.

[58] J-P. Serre. *Galois Cohomology.* Springer Monographs in Mathematics. Springer, 2002. Corrected Second Printing.

[59] A. Silverberg. Ranks “cheat sheet”. In C. David, M. Lalín, and M. Manes, editors, *Women in numbers 2: research directions in number theory*, volume 606 of *Contemporary Mathematics*, pages 101–110. American Mathematical Society, 2013.

[60] J.H. Silverman. Heights and the specialization map for families of abelian varieties. *Journal für die reine und angewandte Mathematik*, 342:197–211, 1983.

[61] J.H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics.* Springer, 1985.

[62] J.H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 151 of *Graduate Texts in Mathematics.* Springer, 1994.

[63] J.H. Silverman and J. Tate. *Rational Points on Elliptic Curves.* Undergraduate Texts in Mathematics. Springer, 1992.

[64] N.G. Smart. S-unit equations, binary forms and curves of genus 2. *Proceedings of the London Mathematical Society*, 75(2):271–307, 1997.

[65] M.A. Soomro. *Algebraic curves over finite fields.* PhD thesis, Rijksuniversiteit Groningen, 2013. URL: `http://irs.ub.rug.nl/ppn/35797039X`.

[66] The Stacks Project Authors. Stacks Project, 2015. URL: `http://stacks.math.columbia.edu`.

[67] C.L. Stewart and J. Top. On ranks of twists of elliptic curves and power-free values of binary forms. *Journal of the American Mathematical Society*, 8(4):943–973, 1995.

[68] H. Stichtenoth. *Algebraic Function Fields and Codes*, volume 254 of *Graduate Texts in Mathematics.* Springer, second edition, 2009.

[69] J. Tate. Endomorphisms of abelian varieties over finite fields. *Inventiones mathematicae*, 2(2):134–144, 1966.

[70] A. Tuijp. Hesse pencil in characteristic two. Bachelor’s thesis, Rijksuniversiteit Groningen, 2015. URL: `http://irs.ub.rug.nl/dbi/55a7a856bac9a`.

[71] M. Vaughan-Lee. *The restricted Burnside problem*, volume 8 of *London Mathematical Society monographs. New series.* Oxford University Press, second edition, 1993.

[72] P. van Wamelen. Proving that a genus 2 curve has complex multiplication. *Mathematics of Computation*, 68(228):1663–1677, 1999.

[73] P. van Wamelen. Poonen's question concerning isogenies between Smart's genus 2 curves. *Mathematics of Computation*, 69(232):1685–1697, 2000.

[74] L.C. Washington. *Elliptic Curves: Number Theory and Cryptography*. Discrete Mathematics and its Applications. Chapman & Hall/CRC, second edition, 2008.

[75] W.C. Waterhouse. Abelian varieties over finite fields. *Annales scientifiques de l'École Normale Supérieure*, 2(4):521–560, 1969.

[76] A. Wiles. Modular elliptic curves and Fermat's Last Theorem. *Annals of Mathematics*, 141(3):443–551, 1995.

[77] J.S. Wilson. *Profinite groups*, volume 19 of *London Mathematical Society monographs. New series.* Oxford University Press, 1998.

[78] K. Wingberg. On Galois groups of p-closed algebraic number fields with restricted ramification II. *Journal für die reine und angewandte Mathematik*, 416:187–194, 1991.

[79] E.I. Zel'manov. Solution of the restricted Burnside problem for groups of odd exponent. *Izvestiya Akademii Nauk SSSR. Seriya Matematicheskaya*, 54(1):42–59, 1990.

[80] E.I. Zel'manov. Solution of the restricted Burnside problem for 2-groups. *Matematicheskiĭ Sbornik*, 182(4):568–592, 1991.

Index

complex multiplication, 19
coset action, 62

deviation group, 51
deviation map, 51

flex point, 30

height, 5
    logarithmic, 7
Hesse pencil, 29
Hessian, 29
Hessian curve, 30
homomorphism
    symplectic, 29

maximal, 1, 19
maximal 2-extension, 60
Mestre curve, 41

ordinary, 2

period matrix, 80

supersingular, 2

transitive group, 62
    degree, 62
twist, 39

Curriculum Vitae

Ane Anema was born on 17 January 1986 in Sneek, the Netherlands. In 2009 he obtained his bachelor's degrees in mathematics and in physics from the University of Groningen. In 2011 he completed his master's in mathematics. During the years 2012–2016 he was a PhD student in mathematics at the University of Groningen under the supervision of Jaap Top.

He maintains a professional website at: `http://22gd7.nl/a.s.i.anema`.