RIJKSUNIVERSITEIT GRONINGEN

A Generalized Arithmetic Geometric Mean

Proefschrift

ter verkrijging van het doctoraat in de
Wiskunde en Natuurwetenschappen
aan de Rijksuniversiteit Groningen
op gezag van de
Rector Magnificus, dr. F. Zwarts,
in het openbaar te verdedigen op
vrijdag 26 november 2004
om 14.45 uur

door

Robert Carls

geboren op 9 juni 1971
te Frankfurt-Main, Duitsland

Promotores:	Prof. dr. H.W. Lenstra Prof. dr. M. van der Put
Copromotor:	Dr. J. Top
Beoordelingscommissie:	Prof. dr. S.J. Edixhoven Prof. dr. G. Frey Prof. dr. J.-F. Mestre

ISBN 90-367-2177-6

Contents

Chapter 1

Introduction

Figure 1.1 shows in which order one has to read the following chapters and sections depending on the individual interest. Readers who want to know about the abstract theory of a generalized arithmetic geometric mean are recommended to follow path A. If one is more interested in the applications, i.e., point counting, then one should consider option B. We remark that the Chapters 2–4 do not depend on each other.

Structure of Chapter 1:	
Section 1.1:	We recall some facts about the classical arithmetic geometric mean.
Section 1.2:	We survey point counting algorithms related to the generalized arithmetic geometric mean.
Section 1.3:	We outline a research program, which has as goal to make the generalized arithmetic geometric mean sequence explicit in higher dimensions.
Bibliography	

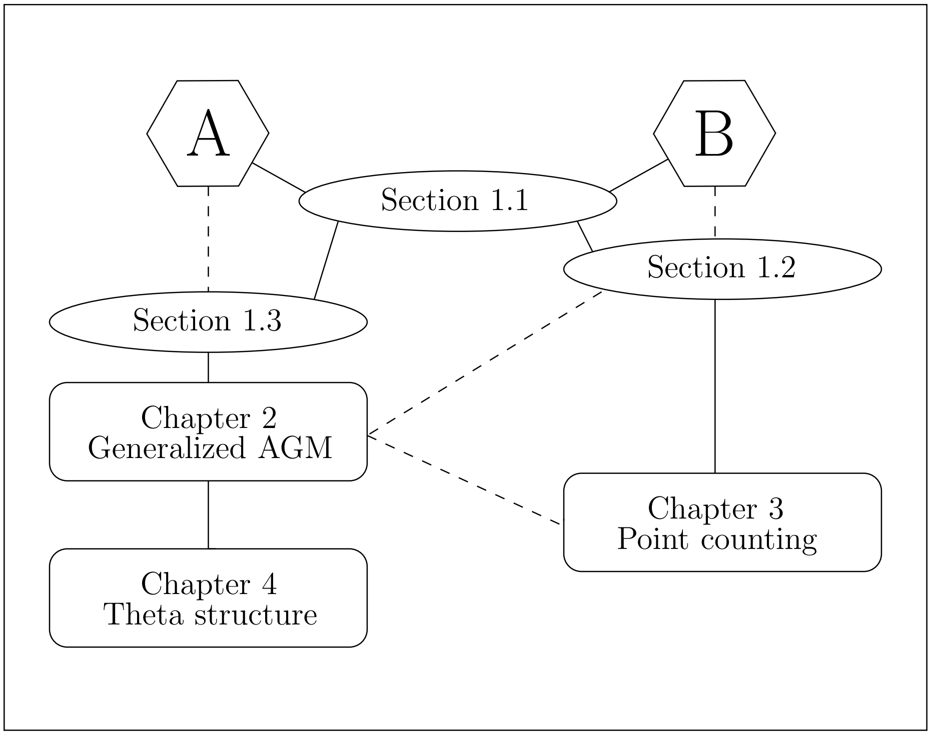

Figure 1.1: Leitfaden

1.1 The classical arithmetic geometric mean

At the end of the 18th century J.-L. Lagrange and C.F. Gauss became interested in the arithmetic geometric mean (AGM). Gauss worked on this subject in the period 1791 until 1828. For an exposition of Gauss' work on the AGM in a modern language and historical notes see [Cox84].

The AGM sequence is defined as follows. Given $a, b \in \mathbb{R}$ such that $a, b \geq 0$ one defines sequences of numbers by setting

$$a_{n+1} = \frac{a_n + b_n}{2} \quad \text{and} \quad b_{n+1} = \sqrt{a_n b_n} \tag{1.1}$$

for $n \geq 0$, where $a_0 = a$ and $b_0 = b$. The limits of the sequences a_n and b_n exist and

$$\lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n.$$

The common limit is called the *arithmetic geometric mean* of a and b.

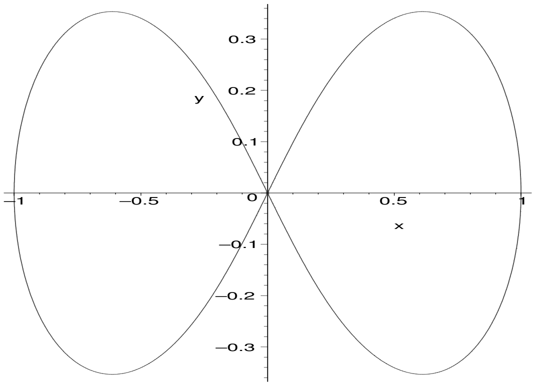

Figure 1.2: Lemniscate

Gauss discovered that elliptic integrals can be expressed in terms of the AGM. He approximated the arclength L of the *lemniscate* (see Figure 1.2), which is defined by the equation

$$(x^2 + y^2)^2 = a^2(x^2 - y^2),$$

using the formula

$$L = 4a \int_0^1 \frac{dt}{\sqrt{1 - t^4}} = \frac{2\pi a}{M(1, \sqrt{2})}.$$

For Gauss' proof of the right hand equality see [Cox84]. More details about the relation of the AGM with elliptic integrals can be found in [BM88].

In order to define an AGM sequence for complex numbers using the formulas (1.1) one has to make a choice for the square root. Let $a, b \in \mathbb{C}^*$ and $a \neq \pm b$. A square root c of ab is called the *right choice* if

$$\left|\frac{a+b}{2} - c\right| \leq \left|\frac{a+b}{2} + c\right|.$$

If equality holds in the latter inequality, then the right choice is the square root c of ab having the property, that the imaginary part of $c/(a+b)$ is strictly positive. If c is the right choice, then the angle between $(a+b)/2$ and c is at most half the angle between a and b (see Figure 1.3). Consequently, making the right choice for all but finitely many indices $n \geq 1$ forces the sequences a_n and b_n to converge to a common limit.

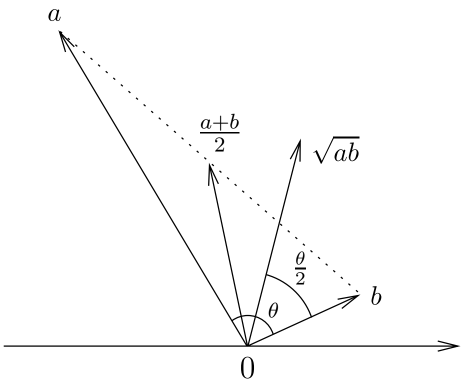

Figure 1.3: The arithmetic and the geometric mean

Given a prime number $p > 0$ one defines the AGM sequence for p-adic numbers $a, b \in \mathbb{Q}_p^*$ in the following way. To make sure that a square root of ab lies in $\mathbb{Q}_p$ one has to assume that

$$\frac{b}{a} \equiv 1 \bmod p^\alpha \quad \text{where} \quad \alpha = \begin{cases} 3 & \text{if } p = 2 \\ 1 & \text{if } p > 2. \end{cases}$$

We set

$$c = a \cdot \sum_{i=0}^{\infty} \binom{\frac{1}{2}}{i} \left(\frac{b}{a} - 1\right)^i.$$

By our assumption the power series converges to a p-adic integer. One verifies that $c^2 = ab$ and

$$\frac{2c}{a+b} \equiv 1 \bmod p^\alpha,$$

where α is as above. The latter implies that we can iterate the above construction and define an AGM sequence (a_n, b_n) with initial values $a_0 = a$ and $b_0 = b$. For $p > 2$ the sequences a_n and b_n converge to a common limit. The latter is true for $p = 2$ if and only if

$$\frac{b}{a} \equiv 1 \bmod 16.$$

The AGM sequence can be interpreted geometrically in the following way. Assume we are given an AGM sequence (a_n, b_n) with non-zero initial values a_0 and b_0 such that $a_0 \neq \pm b_0$. Consider the sequence of elliptic curves E_n defined by the equations

$$y^2 = x(x - a_n^2)(x - b_n^2), \quad n \geq 0.$$

There exists an isogeny $E_n \to E_{n+1}$ given by

$$(x, y) \mapsto \left(\frac{(x + a_n b_n)^2}{4x}, \frac{y(a_n b_n - x)(a_n b_n + x)}{8x^2} \right), \tag{1.2}$$

whose kernel is generated by the 2-torsion point $(0, 0)$ on E_n.

For the rest of this section we focus on the case where the coefficients a_n and b_n are 2-adic numbers. In [HM89] G. Henniart and J.-F. Mestre study the sequence E_n in the case of multiplicative reduction. In the following we will describe how to use the sequence E_n to approximate the canonical lift of an elliptic curve over a finite field of characteristic 2.

Let E be an elliptic curve over $\mathbb{Q}_2$ having ordinary good reduction and assume that $\#E[2](\mathbb{Q}_2) = 4$. Then E admits a model

$$y^2 = x(x - a^2)(x - b^2)$$

where $a, b \in \mathbb{Q}_2^*$ with $a \neq \pm b$, the point $(0, 0)$ is in the kernel of reduction,

$$\frac{b}{a} \equiv 1 \bmod 8 \quad \text{and} \quad \frac{b}{a} \not\equiv 1 \bmod 16.$$

This is proven in Section 2.2. We consider the 2-adic AGM sequence (a_n, b_n) with initial values $a_0 = a$ and $b_0 = b$. The associated sequence of elliptic curves E_n with $E_0 = E$ has the property that for all $n \geq 0$ the elliptic curve

E_n has ordinary good reduction and the point $(0,0)$ on E_n reduces to the point at infinity. Mestre pointed out that, despite the fact that the sequences a_n and b_n do not converge, the sequence of j-invariants

$$j_n = 2^8 \frac{(a_n^4 - a_n^2 b_n^2 + b_n^4)^3}{a_n^4 b_n^4 (a_n^2 - b_n^2)^2}$$

associated to the elliptic curves E_n converges, and

$$\lim_{n \to \infty} j_n \in \mathbb{Z}_2$$

is the j-invariant of the canonical lift of the reduction of E. The sequence E_n is characterized by the condition that the isogeny (1.2) is a lift of the relative 2-Frobenius. Mestre proposed also a higher dimensional analogue of the sequence E_n over the 2-adic numbers [Mes02].

Our contribution to the theory of the AGM is given by the following. We define a *generalized arithmetic geometric mean (GAGM) sequence* as a certain sequence of p-isogenous abelian schemes over a p-adic ring, which coincides in the 2-adic 1-dimensional case with the sequence E_n as defined above. In Chapter 2 we prove that the GAGM sequence converges p-adically. In Chapter 4 we show that the GAGM sequence admits a natural theta structure. As a consequence it can be endowed with canonical projective coordinates. Our results have to be seen in the context of our research program that we formulate in Section 1.3.

1.2 Point counting

In the following we will motivate our research on a generalization of the *arithmetic geometric mean (AGM)* by relating it to the point counting problem for abelian varieties over finite fields. The general point counting problem can be stated as follows.

Question 1.2.1 *Let V be a variety over a finite field $\mathbb{F}_q$. Is there an algorithm which computes the number $\#V(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points on V in a reasonable amount of time?*

Assume we are given a non-singular projective variety V over a finite field $\mathbb{F}_q$ of characteristic $p > 0$ and a projective embedding

$$V \hookrightarrow \mathbb{P}^n_{\mathbb{F}_q}.$$

The q-Frobenius endomorphism f on V is the morphism given by

$$(x_0 : \ldots : x_n) \mapsto (x_0^q : \ldots : x_n^q).$$

Let $i \geq 0$. The morphism f acts on the i-th cohomology space $H^i(V)$ of V as a linear map denoted by f^*. For H one can take a p-adic cohomology, e.g. the rigid or the crystalline cohomology, or the l-adic cohomology, where l is a prime different from p. The number of $\mathbb{F}_q$-rational points on V is related to the action of f^* on the cohomology by the Lefschetz trace formula

$$\#V(\mathbb{F}_q) = \sum_{i=0}^{2\cdot\dim(V)} (-1)^i \ \operatorname{tr}\big(f^*|H^i(V)\big).$$

Note that the cohomology spaces $H^i(V)$ are vector spaces defined over $\mathbb{Q}_q$ resp. $\mathbb{Q}_l$ if H is a p-adic resp. the l-adic cohomology. Here we denote by $\mathbb{Q}_q$ the field of fractions of the ring of p-Witt vectors with values in $\mathbb{F}_q$. One classifies point counting algorithms for varieties over finite fields into p-adic and l-adic methods depending on the cohomology theory that is used. In contrast to the l-adic ones the p-adic methods can only be applied if the characteristic p is small.

We briefly sum up some facts about l-adic methods for point counting. The following summary is not meant to be complete. An l-adic method is given by the so-called SEA method, named after its inventors R. Schoof, N.D. Elkies and A.O.L. Atkin. The SEA method is limited to elliptic curves. References for the SEA method are [Sch95] or [Elk98]. Contributions to the SEA package were made by J.-M. Couveignes [Cou94], M. Fouquet and F. Morain [FM02]. J. Pila succeeded to generalize Schoof's original algorithm, which underlies the SEA algorithm, to abelian varieties of higher dimension [Pil90]. The resulting algorithm is only of theoretical value. Partial results generalizing Atkin's ideas to Jacobians of curves of genus 2 and 3 were obtained by P. Gaudry [Gau00].

In the following we will focus on p-adic methods. The mile stones were set by

1. T. Satoh [Sat00],
2. K. Kedlaya [Ked01],
3. J.-F. Mestre [Mes00], [Mes02],
4. A. Lauder [Lau04b], [Lau04a].

There is a platoon of researchers working on extensions and generalizations of the above mentioned methods. In order to compare algorithms we will use the O- and $\tilde{O}$-notion. The latter will be explained in Section 3.2. We will state the complexities of the algorithms assuming that p is fixed.

1. *Satoh's canonical lift method*: The first p-adic method was proposed by T. Satoh. The original algorithm was designed for ordinary elliptic curves over a finite field of characteristic $p > 3$. Later on the algorithm was extended to $p = 2, 3$ by M. Fouquet, P. Gaudry, R. Harley [FGH00] and independently by B. Skjernaa [Skj03] for $p = 2$. Satoh's original method had running time $\tilde{O}(\log_p^3 q)$. F. Vercauteren, B. Preneel and J. Vandewalle showed in [PVV01] that there exists a memory efficient version of Satoh's algorithm having space complexity $O(\log_2^2 q)$. Combined efforts of the above mentioned mathematicians yielded an algorithm having running time $\tilde{O}(\log_p^2 q)$ [Har02].

In the following we briefly describe Satoh's algorithm. Let $\bar{E}$ be an ordinary elliptic curve over a finite field $\mathbb{F}_q$. The main part of Satoh's algorithm is the approximation of the canonical lift E over $\mathbb{Q}_q$ of $\bar{E}$. The canonical lift E has the defining property that it admits an endomorphism F lifting the q-Frobenius endomorphism f of $\bar{E}$. The approximation of E is done by a Newton iteration involving the p-th modular polynomial. After having computed a lift F of f up to a certain precision, one can compute the action of F on differentials. This gives the number of $\mathbb{F}_q$-rational points on $\bar{E}$ provided that one has computed all quantities with sufficiently high precision.

2. *Kedlaya's Monsky-Washnitzer method*: Kedlaya invented a p-adic method for counting points on hyperelliptic curves over a finite field $\mathbb{F}_q$ of characteristic $p > 2$. J. Denef and F. Vercauteren extended Kedlaya's method to $p = 2$ [DV02]. Other generalizations were proposed by F. Vercauteren [Ver03] and by N. Gurel and P. Gaudry [GG01]. The most general algorithm was obtained by R. Gerkmann [Ger03]. His method works for affine complete transversal intersections. Kedlaya's original method for a hyperelliptic curve of genus g has running time $\tilde{O}(g^4 \log_p^3 q)$.

Kedlaya's idea is to lift simultaneously a hyperelliptic curve $\bar{C}$ over $\mathbb{F}_q$ together with its q-Frobenius f to a hyperelliptic curve C over $\mathbb{Q}_q$ with endomorphism F reducing to f. The lifts C and F are formal in the sense that they exist in the category of rigid analytic spaces. There exists a natural explicit basis of $H^1(C')^-$ depending on the equation of C, where H denotes the Monsky-Washnitzer cohomology of the unramified locus C' of the degree 2 covering $C \to \mathbb{P}^1_{\mathbb{Q}_q}$. The minus sign indicates that one restricts to the subspace of the cohomology on which the hyperelliptic involution acts as minus the identity. One has to compute the matrix giving the action of F on the above basis of $H^1(C')^-$. This can be done using a reduction algorithm for differentials. The number of $\mathbb{F}_q$-rational points on $\bar{C}$ can be computed using a modified Lefschetz trace formula.

3. *Mestre's AGM method*: In the following we will cast a short glance on J.-F. Mestre's AGM method. First we consider Mestre's algorithm for ordinary elliptic curves over $\mathbb{F}_{2^d}$. The objects computed by the latter algorithm are the same as those computed in Satoh's algorithm, but the computation is done differently. The canonical lift is approximated using the AGM sequence (compare Section 1.1). The complexity of Mestre's AGM method for elliptic curves is $\tilde{O}(d^3)$. In [Koh03] D. Kohel proposed a generalization of Mestre's AGM algorithm for elliptic curves over a finite field of characteristic $p \in \{2, 3, 5, 7, 13\}$.

Mestre also proposed an AGM based algorithm for ordinary hyperelliptic curves over a finite field of characteristic 2 [Mes02]. This algorithm was implemented and improved by R. Lercier and D. Lubicz [LL03]. For a hyperelliptic curve of small genus they propose an AGM based algorithm having complexity essentially quadratic in the dimension of the finite field over its prime field. An extension of Mestre's algorithm to non-hyperelliptic curves of genus 3 was worked out by C. Ritzenthaler [Rit03].

4. *Lauder's deformation method*: Lauder proposed an algorithm for counting points on a smooth projective hypersurface defined over a finite field. The complexity of his algorithm is polynomial in $\log_p q$. The author is not aware of existing implementations of the so-called deformation method.

Lauder's algorithm consists of two parts, namely a deformation part and a counting part. The key idea is to deform the equation of the hypersurface into diagonal form by introducing an additional variable. The number of rational points on the variety given by the diagonal equation can be computed due to the fact that there are explicit formulas for the Frobenius matrix describing the action of Frobenius on cohomology. To relate this number to the number of rational points on the original hypersurface one uses the Gauss-Manin connection. For further details we refer to [Lau04b] and [Lau04a].

Our research fits into the above context in the following way. The results of Chapter 2 explain and generalize Mestre's convergence result for the geometric AGM sequence. In Chapter 3 we present a point counting algorithm for ordinary elliptic curves over finite fields of characteristic $p > 2$ based on a generalization of the AGM sequence. The latter algorithm has complexity

$\tilde{O}(\log_p^3 q)$. In Section 1.3 we outline a research program which has as goal a generalization of Mestre's higher dimensional AGM method to characteristic $p > 2$. An important part of the research program is already worked out and contained in Chapter 4.

1.3 A research program

In this section we formulate a research program consisting of some mathematical problems related to the GAGM sequence. In the center of the research program is the problem of making the generalized arithmetic geometric mean (GAGM) sequence explicit in the higher dimensional case. Our expectation is that one can find an algorithm computing the GAGM sequence as a sequence of points in some projective space. The latter projective space is expected to be a moduli space for abelian schemes with theta structure. A motivation for our research is that one probably will be able to use the above mentioned algorithm to compute the zeta function of an ordinary abelian variety over a finite field. A second goal is to provide a new conceptual basis for J.-F. Mestre's higher dimensional 2-adic AGM formulas [Mes02].

We intend to use the theory of theta functions over arbitrary rings to make the GAGM sequence explicit. The theory of algebraic theta functions was first introduced by D. Mumford in his series of articles [Mum66], [Mum67a] and [Mum67b]. Another source for the theory of theta functions, in the classical as well as in the algebraic setting, are the books [Mum83], [Mum84] and [Mum91]. Classically the theta functions of a fixed non-degenerate type on a complex abelian variety form an ample line bundle. Over an arbitrary ring one can evaluate sections of ample line bundles if one is given a rigidification and a theta structure for the line bundle. The resulting theory of theta functions is analogous with the classical theory.

Our setting for the rest of Section 1.3 is the following. Let R be a complete noetherian local ring with perfect residue field k of characteristic $p > 0$ and A an abelian scheme having ordinary reduction. The generalized arithmetic mean (GAGM) sequence is a sequence of abelian schemes

$$A \xrightarrow{F} A^{(p)} \xrightarrow{F} A^{(p^2)} \rightarrow \ldots$$

where F is an isogeny which is uniquely determined up to isomorphism by the condition that it reduces to the relative p-Frobenius. For a precise definition of the GAGM sequence see Section 2.1.

Let $\mathcal{L}$ be an ample line bundle of degree 1 on A and assume that we have trivialized the p-torsion of A_k, i.e., we are given an isomorphism

$$(\mathbb{Z}/p\mathbb{Z})_k^g \xrightarrow{\sim} A_k[p]^{\mathrm{et}}, \tag{1.3}$$

where $A_k[p]^{\mathrm{et}}$ denotes the maximal étale quotient of $A_k[p]$ and g is the relative dimension of A over R. We embed the GAGM sequence into projective space using the following theorem.

Theorem 1.3.1 *Let $p > 2$. For all $i \geq 1$ there exists a natural embedding*

$$A^{(p^i)} \hookrightarrow \mathbb{P}_R^{p^g-1}, \tag{1.4}$$

depending on the line bundle $\mathcal{L}$ and the isomorphism (1.3).

We will sketch the proof of Theorem 1.3.1 at the end of this section. Using Theorem 1.3.1 we associate to $A^{(p^i)}$ a point $P_i \in \mathbb{P}^{p^g-1}(R)$ by taking the image of the zero section under the embedding (1.4). This point is called the *theta null point* of $A^{(p^i)}$ (compare [Mum66]). As a result we get a sequence of points

$$\{P_i\}_{i\geq 1} \subseteq \mathbb{P}^{p^g-1}(R). \tag{1.5}$$

For algorithmic purposes it is convenient to assume that k is a finite field and $R = W_p(k)$ the ring of p-Witt vectors with values in k. The main goal of our research program is to find an algorithm, which computes the points of the sequence (1.5) over R up to a certain bound with a given precision in a reasonable amount of time. Beside that we want to relate the transformation on theta null points induced by F to the action of F on differentials. In the analytic theory of theta functions this is called a *transformation formula* (compare [Igu72] Ch.V, §1). D. Mumford remarked in his article [Mum66], p. 287, that such a transformation formula should also exist in the algebraic setting. An algorithm and a transformation formula as above will result in an algorithm for counting the number of points on the reduction A_k over the finite field k. This algorithm has as input the theta null point of $A^{(p)}$ and as output the number $\#A_k(k)$. In the case where A is the Jacobian of an explicitly given curve it should be possible to compute the theta null point of $A^{(p)}$.

Sketch of the proof of Theorem 1.3.1: The line bundle $\mathcal{L}$ descends along the GAGM sequence in a natural way, which means that there exists an ample line bundle $\mathcal{L}^{(p^i)}$ of degree 1 on $A^{(p^i)}$ for all $i \geq 1$ uniquely determined by some natural conditions (see Theorem 4.4.1). The following theorem is explained and proven in Chapter 4.

Theorem 1.3.2 *Suppose $p > 2$. Then for all $i \geq 1$ there exists a natural theta structure of type $(\mathbb{Z}/p\mathbb{Z})_R^g$ for the pair*

$$\left(A^{(p^i)}, \left(\mathcal{L}^{(p^i)}\right)^{\otimes p}\right)$$

depending on the isomorphism (1.3).

Let $i \geq 1$ and set $\mathcal{L}_i = \left(\mathcal{L}^{(p^i)}\right)^{\otimes p}$. We claim that the above theta structure for $\mathcal{L}_i$ induces an R-basis of $\mathcal{L}_i$, which is uniquely determined up to scalars. This is due to the simplicity of the representation theory of theta groups. The latter theory over an arbitrary base is written down in [MB85] Ch.V. There is a unique irreducible representation of the theta group of $\mathcal{L}_i$, which is given by $\mathcal{L}_i$ itself considered as an R-module. A theta structure induces an isomorphism of the latter representation with the standard representation of the standard theta group of type $(\mathbb{Z}/p\mathbb{Z})_R^g$ (compare Section 4.3.3). This isomorphism is unique up to scalars. Via the latter isomorphism the natural basis of the standard representation induces the basis of $\mathcal{L}_i$, whose existence was claimed above.

Every R-basis of $\mathcal{L}_i$ has cardinality p^g, since the degree of $\mathcal{L}_i$ equals p^g. The line bundle $\mathcal{L}_i$ is very ample, because we have assumed that $p > 2$. Thus the above basis determines in a unique way a closed immersion

$$A^{(p^i)} \hookrightarrow \mathbb{P}_R^{p^g-1}. \tag{1.6}$$

This finishes the sketch of the proof of Theorem 1.3.1. □

Bibliography

[BM88] Jean-Benoît Bost and Jean-François Mestre. Moyenne arithmético-géométrique et périodes des courbes de genre 1 et 2. Technical Report LMENS-88-13, Département de Mathématiques et d'Informatique Ecole Normale Supérieure, 1988.

[Cou94] Jean-Marc Couveignes. Schoof's algorithm and isogeny cycles. In *Proceedings Algorithmic Number Theory Symposium ANTS-I*, number 877 in Lecture Notes in Computer Science, pages 43–58, 1994.

[Cox84] David Cox. The arithmetic-geometric mean of Gauss. *Enseignement Mathématique (2)*, 30(3–4):275–330, 1984.

[DV02] Jan Denef and Frederik Vercauteren. An extension of Kedlaya's algorithm to Artin-Schreier curves in characteristic 2. In Claus Fieker and David Kohel, editors, *Proceedings Algorithmic Number Theory Symposium ANTS-V*, number 2369 in Lecture Notes in Computer Science, pages 308–323, 2002.

[Elk98] Noam David Elkies. Elliptic and modular curves over finite fields and related computational issues. In *Computational Perspectives on Number Theory: Proceedings of a conference in honor of A.O.L. Atkin*, pages 21–76. AMS/International Press, 1998.

[FGH00] Mireille Fouquet, Pierrick Gaudry, and Robert Harley. An extension of Satoh's algorithm and its implementation. *Journal of the Ramanujan Mathematical Society*, 15(4):281–318, 2000.

[FM02] Mireille Fouquet and François Morain. Isogeny volcanoes and the SEA algorithm. In *Proceedings Algorithmic Number Theory Symposium ANTS-V*, number 2369 in Lecture Notes in Computer Science, pages 276–291, 2002.

[Gau00] Pierrick Gaudry. *Algorithmique des courbes hyperelliptiques et applications à la cryptologie.* PhD thesis, École Polytechnique Paris, France, 2000.

[Ger03] Ralf Gerkmann. *The p-adic cohomology of varieties over finite fields and applications on the computation of zeta functions.* PhD thesis, Universität Essen, Germany, 2003.

[GG01] Nicolas Gurel and Pierrick Gaudry. An extension of Kedlaya's algorithm to superelliptic curves. In *Advances in Cryptology, Asiacrypt 2001*, number 2248 in Lecture Notes in Computer Science, pages 480–494, 2001.

[Har02] Robert Harley. Asymptotically optimal p-adic point-counting. Email to NMBRTHRY Archives, December 2002. http://listserv.nodak.edu/archives/nmbrthry.html.

[HM89] Guy Henniart and Jean-François Mestre. Moyenne arithmético-géométrique p-adique. *Comptes Rendus de l'Academie de Sciences Paris, Série I, Mathématiques*, 308(13):391–395, 1989.

[Igu72] Jun-Ichi Igusa. *Theta functions.* Number 194 in Grundlehren der mathematischen Wissenschaften. Springer-Verlag, 1972.

[Ked01] Kiran Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *Journal of the Ramanujan Mathematical Society*, 16(4):323–338, 2001.

[Koh03] David Kohel. The AGM-$X_0(N)$ Heegner point lifting algorithm and elliptic curve point counting. In *Proceedings of ASIACRYPT'03*, number 2894 in Lecture Notes in Computer Science, pages 124–136. Springer-Verlag, 2003.

[Lau04a] Alan Lauder. Counting solutions to equations in many variables over finite fields. *Foundations of Computational Mathematics*, 4(3):221–267, 2004.

[Lau04b] Alan Lauder. Deformation theory and the computation of zeta functions. *Proceedings of the London Mathematical Society*, 88(3):565–602, 2004.

[LL03] Reynald Lercier and David Lubicz. A quasi-quadratic time algorithm for hyperelliptic curve point counting. unpublished, available at http://www.math.u-bordeaux.fr/∼lubicz, 2003.

[MB85] Laurent Moret-Bailly. *Pinceaux de variétés abéliennes*, volume 129 of *Astérisque.* Société Mathématiques de France, 1985.

[Mes00] Jean François Mestre. Lettre adressée à Gaudry en Harley. unpublished, available at http://www.math.jussieu.fr/∼mestre, 2000.

[Mes02] Jean-François Mestre. Algorithmes pour compter des points en petite caractéristique en genre 1 et 2. unpublished, rédigé par D. Lubicz, available at http://www.maths.univ-rennes1.fr/crypto/2001-02/mestre.ps, 2002.

[Mum66] David Mumford. On the equations defining abelian varieties I. *Inventiones Mathematicae*, 1:287–354, 1966.

[Mum67a] David Mumford. On the equations defining abelian varieties II. *Inventiones Mathematicae*, 3:75–135, 1967.

[Mum67b] David Mumford. On the equations defining abelian varieties III. *Inventiones Mathematicae*, 3:215–244, 1967.

[Mum83] David Mumford. *Tata lectures on theta I*, volume 28 of *Progress in Mathematics*. Birkhäuser Verlag, 1983.

[Mum84] David Mumford. *Tata lectures on theta II*, volume 43 of *Progress in Mathematics*. Birkhäuser Verlag, 1984.

[Mum91] David Mumford. *Tata lectures on theta III*, volume 97 of *Progress in Mathematics*. Birkhäuser Verlag, 1991.

[Pil90] Jonathan Pila. Frobenius maps of abelian varieties and finding roots of unity in finite fields. *Mathematics of Computation*, 55(192):745–763, 1990.

[PVV01] Bart Preneel, Joos Vandewalle, and Frederik Vercauteren. A memory efficient version of Satoh's algorithm. In *Advances in Cryptology - Eurocrypt 2001*, number 2045 in Lecture Notes in Computer Science, pages 1–13, 2001.

[Rit03] Christophe Ritzenthaler. *Problèmes arithmétiques relatifs à certaines familles de courbes sur les corps finis*. PhD thesis, Université Paris 7, Denis-Diderot, France, 2003.

[Sat00] Takakazu Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *Journal of the Ramanujan Mathematical Society*, 15:247–270, 2000.

[Sch95] René Schoof. Counting points on elliptic curves over finite fields. *Journal de Théorie des Nombres de Bordeaux*, 7:219–254, 1995.

[Skj03] Berit Skjernaa. Satoh's algorithm in characteristic 2. *Mathematics of Computation*, 72:477–487, 2003.

[Ver03] Frederik Vercauteren. *Computing zeta functions of curves over finite fields.* PhD thesis, Katholieke Universiteit Leuven, Belgium, 2003.

Chapter 2

The Convergence Theorem

In this chapter we introduce a generalized arithmetic geometric mean sequence as a certain sequence of p-isogenous abelian schemes over a p-adic ring. We prove the p-adic convergence of the latter sequence by means of Serre-Tate theory. The convergence is implicitly used in J.-F. Mestre's point counting algorithm for ordinary hyperelliptic curves (see [Mes02] and [LL03]) and in its extension by C. Ritzenthaler (see [Rit03]). The author is aware of the fact that the Convergence Theorem (see Corollary 2.1.4) is known to the experts. We remark that it is not contained in the literature.

Structure of Chapter 2:	
Section 2.1:	We give a definition of a generalized arithmetic geometric mean sequence and state the Convergence Theorem.
Section 2.2:	We explain the link with the classical arithmetic geometric mean which is due to C.F. Gauss.
Section 2.3:	We make some general remarks about the notation that is used in this chapter.
Section 2.4:	We describe the deformation theory of abelian varieties over a field of positive characteristic, i.e. Serre-Tate theory, that we use in the proof the Convergence Theorem.
Section 2.5:	This section contains the proof of the Convergence Theorem and the proofs of the statements made in Section 2.2.
Acknowledgments	
Bibliography	

2.1 A generalized arithmetic geometric mean

Let R be a complete noetherian local ring. We assume R to have perfect residue field k of characteristic $p > 0$. By $\mathfrak{m}$ we denote the maximal ideal of R. Let $\pi : A \to \operatorname{Spec}(R)$ be an abelian scheme having ordinary reduction.

Proposition 2.1.1 *There exists an abelian scheme $\pi^{(p)} : A^{(p)} \to \operatorname{Spec}(R)$ and a commutative diagram of isogenies*

$$\begin{tikzcd}
A \arrow[r, "F"] \arrow[d, "{[p]}"'] & A^{(p)} \arrow[dl, "V"] \\
A &
\end{tikzcd}$$

such that F_k equals relative Frobenius. The latter condition determines F uniquely in the sense that

$$\operatorname{Ker}(F) = A[p]^{\mathrm{loc}}.$$

This will be proven in Section 2.5.1. By 'F_k equals relative Frobenius' we mean that there exists a morphism $\mathrm{pr} : A_k^{(p)} \to A_k$ such that the diagram

$$\begin{tikzcd}
A_k \arrow[dr, "F_k"] \arrow[drr, bend left, "f_p"] \arrow[ddr, bend right, "\pi_k"'] & & \\
& A_k^{(p)} \arrow[r, "\mathrm{pr}"] \arrow[d, "\pi_k^{(p)}"] & A_k \arrow[d, "\pi_k"] \\
& \operatorname{Spec}(k) \arrow[r, "f_p"] & \operatorname{Spec}(k)
\end{tikzcd}$$

is commutative and the square is Cartesian. Here f_p denotes the absolute p-Frobenius. For the definition of $A[p]^{\mathrm{loc}}$ see Section 2.4.3.

Theorem 2.1.2 *Let B be an abelian scheme over R and I an open ideal of R. If*

$$A \cong B \bmod I$$

then

$$A^{(p)} \cong B^{(p)} \bmod pI + \langle I \rangle_p$$

where $\langle I \rangle_p$ denotes the ideal generated by the p-th powers of elements in I.

The above Theorem will be proven in Section 2.5.2.

Definition 2.1.3 *The sequence*

$$A \xrightarrow{F} A^{(p)} \xrightarrow{F} A^{(p^2)} \to \dots$$

is called the generalized arithmetic geometric mean (GAGM) sequence.

Here we denote by $A^{(p^i)}$ $(i \geq 1)$ the abelian scheme that one gets by iterating i times the construction of Proposition 2.1.1. Our name giving is justified by the remarks made in Section 2.2. Let (A^*, φ) be the canonical lift of A_k. For a definition see Section 2.4.7.

Corollary 2.1.4 (Convergence Theorem) *Let $q = \#k < \infty$. One has*

$$\lim_{n \to \infty} A^{(q^n)} = A^*,$$

i.e.

$$(\forall i \geq 0)(\exists N \geq 0)(\forall n \geq N) \quad A^{(q^n)} \cong A^* \bmod \mathfrak{m}^i.$$

This Corollary is proven in Section 2.5.3. We can reformulate Corollary 2.1.4 by saying that the sequence $\left(A^{(q^n)}\right)$ converges with respect to the natural topology on the deformation space $\mathrm{Defo}_{A_k}(R)$ of A_k over R. For a definition of $\mathrm{Defo}_{A_k}(R)$ see Section 2.4.4.

Assume now that R admits an automorphism σ lifting the p-th power Frobenius of k. Let $n \geq 0$ and $A^{(\wp^n)}$ be the pull-back of $A^{(p^n)}$ via the morphism $\mathrm{Spec}(\sigma^{-n})$. Consider the composed isomorphism

$$\left(A^{(\wp^n)}\right)_k \xrightarrow{\sim} A_k \xrightarrow{\varphi^{-1}} A_k^* \tag{2.1}$$

where the left hand isomorphism is the natural one and the right hand isomorphism is the inverse of the structure morphism of the lift (A^*, φ).

Corollary 2.1.5 *For all $n \geq 0$ there exists an isomorphism*

$$A^{(\wp^n)} \xrightarrow{\sim} A^*$$

over $R/\mathfrak{m}^{n+1}$ which is uniquely determined by the condition that it induces the isomorphism (2.1).

This Corollary is proven in Section 2.5.3.

2.2 The link with the classical AGM sequence

In this section we state some results due to J.-F. Mestre. For lack of reference we will prove them in Section 2.5. Let k be a finite field of characteristic 2 and $R = W_2(k)$ the ring of 2-Witt vectors with values in k. The field of fractions of R will be denoted by K. Let E be a smooth elliptic curve over R, i.e. an abelian scheme over R of relative dimension 1.

Proposition 2.2.1 *We have $E[2] \cong \mu_{2,R} \times_R (\mathbb{Z}/2\mathbb{Z})_R$ if and only if E_K can be given by an equation of the form*

$$y^2 = x(x-a^2)(x-b^2), \tag{2.2}$$

where $a, b \in K^*$ such that $a \neq \pm b$, the point $(0,0)$ generates $E[2]^{\mathrm{loc}}(K)$ and $\frac{b}{a} \in 1+8R$.

This proposition is proven in Section 2.5.4. Assume from now on until the end of this section that E satisfies the equivalent conditions of Proposition 2.2.1 and let E_K be given by equation (2.2). By our assumption E has ordinary reduction. The condition $\frac{b}{a} \in 1+8R$ implies that $\frac{b}{a}$ is a square in R. We set in analogy to the classical AGM formulas

$$\tilde{a} = \frac{a+b}{2}, \ \tilde{b} = \sqrt{ab} = a\sqrt{\frac{b}{a}}, \tag{2.3}$$

where we choose $\sqrt{\frac{b}{a}} \in 1+4R$.

Proposition 2.2.2 *Let $E^{(2)}$ be as in Section 2.1. The curve $E_K^{(2)}$ admits the model*

$$y^2 = x(x-\tilde{a}^2)(x-\tilde{b}^2) \tag{2.4}$$

where the point $(0,0)$ generates $E^{(2)}[2]^{\mathrm{loc}}(K)$ and $\frac{\tilde{b}}{\tilde{a}} \in 1+8R$.

A proof of the Proposition and formulas for the isogeny F_K (compare Proposition 2.1.1) can be found in Section 2.5.5. For more details about the classical AGM sequence we refer to [Cox84].

2.3 Notation

Let R be a ring. By the *fppf-topology* on R we mean the category of R-schemes together with surjective coverings consisting of morphisms which are flat and locally of finite presentation. One can embed the category of R-schemes in the category of fppf-sheaves by setting

$$X \mapsto \mathrm{Hom}_R(\cdot, X).$$

By the Yoneda Lemma the above functor is fully faithful. We use the same symbol for a scheme and the fppf-sheaf represented by it. By a *group* we mean an abelian fppf-sheaf, which is not necessarily representable. Let G be a group and C an R-algebra. By G_C we denote the group that one gets by pulling back via the ring homomorphism $R \to C$. Let $I : G \to H$ be a morphism of groups over R. Then I_C denotes the morphism that is induced by I via base extension with C. If G and H are groups over R then $\underline{\mathrm{Hom}}(G, H)$ denotes the sheaf of homomorphisms from G to H, i.e.

$$\underline{\mathrm{Hom}}(G, H)(C) = \mathrm{Hom}_C(G_C, H_C).$$

If a representing object of a group has the property of being finite (resp. flat, étale, connected, etc.) then we simply say that it is a finite (resp. flat, étale, connected, etc.) group. Similarly we will say that a map of groups is finite (resp. faithfully flat, smooth, etc.) if the groups are representable and the induced map of schemes has the corresponding property. A morphism is called *finite locally free* if it is finite flat and of finite presentation. We will denote the zero section of a group G by 0_G.

2.4 Deformation theory

In this Section we give the theoretical background for the proof of the statements of Section 2.1. Some of the proofs can also be found in the literature. We will indicate this by giving a reference. We give a proof of all statements using our notation in order to make the theory coherent.

2.4.1 Abelian schemes

Let R be a ring. An *abelian scheme* over R of relative dimension g is a proper smooth group scheme over R whose geometric fibers are connected and of dimension g. The fibers of an abelian scheme are abelian varieties, i.e. projective group varieties. A finite locally free and surjective morphism of abelian schemes is called an *isogeny*. A morphism of abelian schemes is an isogeny if and only if the maps induced on fibers are isogenies. The multiplication-by-n map $[n]$ $(0 \neq n \in \mathbb{Z})$ is an isogeny. Isogenies are epimorphisms in the category of fppf-sheaves. The category of abelian schemes over R admits a duality. If A is an abelian scheme over R then we denote its dual by $\check{A}$. The dual $\check{A}$ is given by the sheaf $\mathrm{Pic}^0_{A/R}$. Note that $\mathrm{Pic}^0_{A/R}$ is representable by a scheme (see [BLR90] Ch. 8, Theorem 1 and [FC90] Ch. I, Theorem 1.9). A line bundle $\mathcal{L}$ on A determines a map $A \to \check{A}$ by setting $x \mapsto t_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$ where t_x denotes the translation by x. This map is an isogeny if the line bundle $\mathcal{L}$ is relative ample.

2.4.2 Barsotti-Tate groups

Let R be a ring. The following definition of a Barsotti-Tate group is the one of Grothendieck [Gro74] and Messing [Mes72].

Definition 2.4.1 *A* Barsotti-Tate group *G over R is a group satisfying the following conditions:*

1. *G is p-divisible, i.e. $[p]_G$ is an epimorphism,*
2. *G is p-torsion, i.e.*
$$G = \lim_{n\to\infty} G[p^n]$$
3. *$G[p^n]$ is a finite locally free group.*

The Barsotti-Tate groups over R form a full subcategory of the category of abelian fppf-sheaves over R. The latter category is known to be abelian and has enough injectives. This enables us to apply methods of homological algebra. To an abelian scheme A over a ring R we can associate the Barsotti-Tate group
$$A[p^\infty] = \lim_{n\to\infty} A[p^n].$$
The p-divisibility of $A[p^\infty]$ follows from the p-divisibility of A. In fact $(\cdot)[p^\infty]$ gives a functor from abelian schemes to Barsotti-Tate groups. One can define the dual Barsotti-Tate group of G as

$$G^D = \lim_{n\to\infty} G[p^n]^D$$

where $G[p^n]^D = \underline{\mathrm{Hom}}(G[p^n], \mathbb{G}_{m,R})$. The bonding morphisms of the dual group G^D are obtained by dualizing the exact sequence

$$0 \to G[p] \to G[p^{m+1}] \to G[p^m] \to 0.$$

We call a Barsotti-Tate group G *ind-étale* if $G[p^n]$ is étale for all $n \geq 1$. A Barsotti-Tate group is called *toroidal* if it is the Cartier dual of an ind-étale

Barsotti-Tate group. The standard example for an ind-étale Barsotti-Tate group is

$$(\mathbb{Q}_p/\mathbb{Z}_p)_R = \lim_{n\to\infty} (\mathbb{Z}/p^n\mathbb{Z})_R.$$

Its Cartier dual is equal to

$$\mu_R = \lim_{n\to\infty} \mu_{p^n,R}$$

where $\mu_{p^n,R}$ denotes the kernel of the morphism $\mathbb{G}_{m,R} \to \mathbb{G}_{m,R}$ given on points by $x \mapsto x^{p^n}$. Obviously μ_R is toroidal.

2.4.3 The connected-étale sequence

Let R be a henselian noetherian local ring with perfect residue field k of characteristic $p > 0$ and maximal ideal $\mathfrak{m}$. Let G be a finite flat group over R and G^{loc} the connected component of G containing the zero section. The closed and open subscheme G^{loc} is finite flat. Since R is henselian the number of connected components of a finite R-scheme is invariant under reduction. The reduction of $G^{\mathrm{loc}} \times_R G^{\mathrm{loc}}$ consists of one point because G_k^{loc} is connected. Hence $G^{\mathrm{loc}} \times_R G^{\mathrm{loc}}$ is connected. As a consequence the composition law restricted to $G^{\mathrm{loc}} \times_R G^{\mathrm{loc}}$ factors over G^{loc}. Also inversion restricted to G^{loc} factors over G^{loc}. This makes G^{loc} a subgroup of G. We can form a quotient $G^{\mathrm{et}} = G/G^{\mathrm{loc}}$ (see [Ray67] §5, Théorème 1) which is a finite flat group over R. The quotient map $\pi : G \to G^{\mathrm{et}}$ is finite faithfully flat and hence open (see [GD67] Théorème 2.4.6). The zero section of G^{et} is an open immersion since it is the image of G^{loc} under the quotient map π. This implies that G^{et} is an étale group. Recall that a finite flat group over R is étale if and only if its zero section is an open immersion. The sequence

$$0 \to G^{\mathrm{loc}} \to G \xrightarrow{\pi} G^{\mathrm{et}} \to 0 \tag{2.5}$$

is exact in the category of groups over R. It is called the *connected-étale sequence*. For another account see [Tat97] (3.7). Now let G be a Barsotti-Tate group over R. Obviously there is a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & G[p^n]^{\mathrm{loc}} \arrow[r] \arrow[d] & G[p^n] \arrow[r] \arrow[d] & G[p^n]^{\mathrm{et}} \arrow[r] \arrow[d, dashed] & 0 \\
0 \arrow[r] & G[p^{n+1}]^{\mathrm{loc}} \arrow[r] & G[p^{n+1}] \arrow[r] & G[p^{n+1}]^{\mathrm{et}} \arrow[r] & 0.
\end{tikzcd}$$

The limits

$$G^{\mathrm{et}} = \lim_{n\to\infty} G[p^n]^{\mathrm{et}} \quad \text{and} \quad G^{\mathrm{loc}} = \lim_{n\to\infty} G[p^n]^{\mathrm{loc}}$$

are Barsotti-Tate groups. We get an exact sequence of groups

$$0 \to G^{\mathrm{loc}} \to G \to G^{\mathrm{et}} \to 0. \tag{2.6}$$

Splitting of the connected-étale sequence

Let R and k be as above and G be a Barsotti-Tate group over k. We set

$$G^{\mathrm{red}} = \lim_{n\to\infty} G[p^n]^{\mathrm{red}}.$$

We claim that G^{red} is a Barsotti-Tate group. We have for every finite scheme X over k that

$$X^{\mathrm{red}} \times_k X^{\mathrm{red}} = (X \times_k X)^{\mathrm{red}}.$$

This comes from the fact that X^{red} is the spectrum of a product of finite field extensions. Consequently $G[p^n]^{\mathrm{red}}$ forms a subgroup of $G[p^n]$ because the group law of $G[p^n]$ as well as the inversion map factor over $G[p^n]^{\mathrm{red}}$. The p-divisibility of G^{red} follows from that of G.

Lemma 2.4.2 *Let G be a Barsotti-Tate group over a perfect field k. Then the sequence* (2.6) splits.

Proof. The group G^{red} is ind-étale since for all $n \geq 1$ the scheme $G[p^n]^{\mathrm{red}}$ is the spectrum of a product of finite separable field extensions of k. Let $\bar{k}$ be an algebraic closure of k. Since

$$G^{\mathrm{loc}}(\bar{k}) \cap G^{\mathrm{red}}(\bar{k}) = \{0\}$$

it follows that

$$G^{\mathrm{red}}(\bar{k}) = G(\bar{k}) \xrightarrow{\sim} G^{\mathrm{et}}(\bar{k}) \tag{2.7}$$

where the right hand isomorphism is induced by the quotient map $G \to G^{\mathrm{et}}$ which is surjective. The isomorphism (2.7) induces an isomorphism

$$G^{\mathrm{red}} \to G^{\mathrm{et}},$$

because the category of finite étale k-schemes is equivalent to the category of finite π-sets where $\pi = \mathrm{Gal}(\bar{k}/k)$. □

2.4.4 The Serre-Tate Theorem

Let R be a complete noetherian local ring with perfect residue class field of characteristic $p > 0$ and maximal ideal $\mathfrak{m}$. Let X be an abelian variety resp. a Barsotti-Tate group over k. A *lift* (Y, φ) of X over R is an abelian scheme resp. a Barsotti-Tate group Y over R together with an isomorphism $\varphi : Y_k \overset{\sim}{\to} X$. The lifts of X form a category if we define an arrow

$$(Y, \varphi) \to (Z, \tau)$$

to be a morphism of groups $\beta : Y \to Z$ such that $\tau \circ \beta_k = \varphi$. We denote this category by $\mathfrak{L}_X(R)$.

Theorem 2.4.3 (Serre-Tate) *Let R be artinian local and let X be an abelian variety over its residue field k which we assume to be of characteristic $p > 0$. The functor*

$$\mathfrak{L}_X(R) \to \mathfrak{L}_{X[p^\infty]}(R)$$

given by

$$(A, \varphi) \mapsto (A[p^\infty], \varphi[p^\infty])$$

gives an equivalence of categories.

For a proof see [Kat81], Th.1.2.1. Let X be an abelian variety resp. a Barsotti-Tate group over k. If R is artinian, then we denote the set of isomorphism classes of $\mathfrak{L}_X(R)$ by $\mathrm{Defo}_X(R)$.

Definition 2.4.4 *For a complete noetherian local ring R we set*

$$\mathrm{Defo}_X(R) = \lim_{\leftarrow_i} \mathrm{Defo}_X(R/\mathfrak{m}^i).$$

$\mathrm{Defo}_X(R)$ *is called the* formal deformation space *of X over R.*

The space $\mathrm{Defo}_X(R)$ has a natural topology, i.e. the limit topology with respect to the discrete topology on $\mathrm{Defo}_X(R/\mathfrak{m}^i)$ for all $i \geq 1$.

2.4.5 Barsotti-Tate groups of ordinary abelian schemes

Recall that a local ring R is *henselian* if and only if every finite R-algebra splits into a product of local rings. Let R be a complete noetherian local ring with perfect residue field k of characteristic $p > 0$. Note that R is henselian since it is complete. There exists a functor L from the category of ind-étale

Barsotti-Tate groups over k to the category of ind-étale Barsotti-Tate groups over R and natural equivalences η and δ such that

$$(\cdot)_k \circ L = \eta \quad \text{and} \quad L \circ (\cdot)_k = \delta$$

where $(\cdot)_k$ denotes the reduction functor. This follows from [Ray70a] Ch.VIII, Corollary of Proposition 1. Using Cartier duality one can extend this functor to the category of toroidal Barsotti-Tate groups.

Lemma 2.4.5 *Let A be an abelian scheme over R having ordinary reduction. Then $A[p^\infty]^{\mathrm{loc}}$ is the Cartier dual of $\check{A}[p^\infty]^{\mathrm{et}}$.*

Proof. By the equivalence given by the functor L it suffices to prove the Lemma over k. The Cartier dual of $A[p^\infty]$ is given by $\check{A}[p^\infty]$. It suffices to prove that the Cartier dual of $A[p^\infty]^{\mathrm{et}}$ is equal to $\check{A}[p^\infty]^{\mathrm{loc}}$. The Lemma follows by dualizing the connected-étale sequence. We will show that the Cartier dual of $A[p^n]^{\mathrm{et}}$ is connected. As a consequence the dual of $A[p^\infty]^{\mathrm{et}}$ is contained in $\check{A}[p^\infty]^{\mathrm{loc}}$. Equality follows by comparing ranks. Note that $\check{A}$ is ordinary. In general the Cartier dual $G^D = \underline{\mathrm{Hom}}(G, \mathbb{G}_{m,k})$ of a finite étale group G of order p^l over k is connected. Note that a finite group over k is connected if and only if it has no non-zero points over an algebraic closure $\bar{k}$ of k. Every morphism $G \to \mathbb{G}_{m,k}$ factors over the connected scheme $\mu(p^l)_k$ and hence must be equal zero. This means that $G^D(\bar{k}) = \{0\}$ and hence G^D is connected. □

Let R^{sh} be the *strict henselization* of R. First of all R^{sh} is a noetherian local ring which is henselian. Secondly its residue field is a separable closure of k. A finite scheme over a field is étale if and only if it is constant over a separable closure of this field. Since R and R^{sh} are henselian we can lift idempotents of finite algebras (see [Ray70a] Ch. I, §2). This implies that a finite flat scheme over R is étale if and only if it is constant over R^{sh}. The following corollary follows by the above discussion and Lemma 2.4.5.

Corollary 2.4.6 *Let A be an abelian scheme over R having ordinary reduction. Then*

$$(A[p^\infty]^{\mathrm{et}})_{R^{\mathrm{sh}}} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^g_{R^{\mathrm{sh}}} \quad \textit{and} \quad (A[p^\infty]^{\mathrm{loc}})_{R^{\mathrm{sh}}} \cong \mu^g_{R^{\mathrm{sh}}}$$

where g is the relative dimension of A over R.

2.4.6 Deformations as 1-extensions

Next we want to describe the elements in the deformation space of an ordinary abelian variety as 1-extensions. The extension $R \hookrightarrow R^{\mathrm{sh}}$ is faithfully flat and

$$\mathfrak{m}_{\mathrm{sh}} = R^{\mathrm{sh}}\mathfrak{m}$$

where $\mathfrak{m}_{\mathrm{sh}}$ denotes the maximal ideal of R^{sh}. As a consequence R^{sh} is artinian if and only if R is. If R be artinian and $l \geq 1$ an integer such that $\mathfrak{m}^l = 0$ then

$$\big(1+\mathfrak{m}\big)^{p^{l-1}} = \big(1+\mathfrak{m}_{\mathrm{sh}}\big)^{p^{l-1}} = \{1\}. \tag{2.8}$$

Here $\mathfrak{m}^l$ denotes the usual product of ideals and

$$\big(1+\mathfrak{m}\big)^{p^{l-1}} \quad = \quad \Big\{ \ (1+m)^{p^{l-1}} \ \mid \ m \in \mathfrak{m} \ \Big\}.$$

Lemma 2.4.7 *Let R be a complete noetherian local ring and A an abelian scheme over R having ordinary reduction. If the connected-étale sequence*

$$0 \to A[p^\infty]^{\mathrm{loc}} \to A[p^\infty] \to A[p^\infty]^{\mathrm{et}} \to 0 \tag{2.9}$$

splits then the splitting is unique.

Proof. By [GD71] Ch. I, Théorème 10.12.3 it suffices to check uniqueness over $R/\mathfrak{m}^i$ for all $i \geq 1$. The difference of two sections of (2.9) is an element of $\mathrm{Hom}_R(A[p^\infty]^{\mathrm{et}}, A[p^\infty]^{\mathrm{loc}})$. By the sheaf property of the functor

$$\underline{\mathrm{Hom}}(A[p^\infty]^{\mathrm{et}}, A[p^\infty]^{\mathrm{loc}})$$

and Corollary 2.4.6 we have an injective map

$$\mathrm{Hom}_R(A[p^\infty]^{\mathrm{et}}, A[p^\infty]^{\mathrm{loc}}) \to \mathrm{Hom}_{R^{\mathrm{sh}}}\big((\mathbb{Q}_p/\mathbb{Z}_p)^g, \mu^g\big) \cong \mathrm{Hom}_{R^{\mathrm{sh}}}(\mathbb{Q}_p/\mathbb{Z}_p, \mu)^{g^2}.$$

As usual g denotes the relative dimension of A over R. We claim that the right hand side equals zero. It suffices to prove that

$$\mathrm{Hom}_{R^{\mathrm{sh}}}(\mathbb{Q}_p/\mathbb{Z}_p, \mu) = 0.$$

An R^{sh}-morphism $\mathbb{Q}_p/\mathbb{Z}_p \to \mu$ corresponds to an infinite sequence $(x_1, x_2, \ldots)$ of roots of unity in $1+\mathfrak{m}_{\mathrm{sh}}$, such that $x_{i+1}^p = x_i$. Let $l \geq 1$ such that $\mathfrak{m}^l = 0$. By (2.8) it follows that $x_i = x_{i+l-1}^{p^{l-1}} = 1$ for $i \geq 1$. □

Now we are ready to state the main result of this section.

Theorem 2.4.8 *Let R be artinian and X an ordinary abelian variety over k. Then there is a natural bijection of sets*

$$\mathrm{Defo}_X(R) \overset{\sim}{\longrightarrow} \mathrm{Ext}^1_R\Big(L\big(X[p^\infty]^{\mathrm{et}}\big), L\big(X[p^\infty]^{\mathrm{loc}}\big)\Big) \tag{2.10}$$

which is functorial in R. In particular, the set $\mathrm{Defo}_X(R)$ carries the structure of an abelian group.

Proof. Let L, η and δ be as in Section 2.4.5. By Theorem 2.4.3 it suffices to define a map

$$\mathrm{Defo}_{X[p^\infty]}(R) \longrightarrow \mathrm{Ext}^1_R\Big(L\big(X[p^\infty]^{\mathrm{et}}\big), L\big(X[p^\infty]^{\mathrm{loc}}\big)\Big)$$

having the desired properties. Let (G, φ) be a lift of $X[p^\infty]$. The isomorphism φ induces isomorphisms

$$\varphi^{\mathrm{loc}} : G_k^{\mathrm{loc}} \overset{\sim}{\to} X[p^\infty]^{\mathrm{loc}} \quad \text{and} \quad \varphi^{\mathrm{et}} : G_k^{\mathrm{et}} \overset{\sim}{\to} X[p^\infty]^{\mathrm{et}}.$$

Consider the isomorphisms

$$L(\varphi^{\mathrm{loc}}) \circ \delta(G^{\mathrm{loc}}) : G^{\mathrm{loc}} \overset{\sim}{\to} L(X[p^\infty]^{\mathrm{loc}})$$

and

$$L(\varphi^{\mathrm{et}}) \circ \delta(G^{\mathrm{et}}) : G^{\mathrm{et}} \overset{\sim}{\to} L(X[p^\infty]^{\mathrm{et}}).$$

Via these isomorphisms the connected-étale sequence (2.6) of G induces an extension of $L\big(X[p^\infty]^{\mathrm{et}}\big)$ by $L\big(X[p^\infty]^{\mathrm{loc}}\big)$. Conversely, assume we are given an extension

$$0 \to L(X[p^\infty]^{\mathrm{loc}}) \to G \to L(X[p^\infty]^{\mathrm{et}}) \to 0. \tag{2.11}$$

There exist natural isomorphisms

$$\eta(X[p^\infty]^{\mathrm{loc}})^{-1} : \big(L(X[p^\infty]^{\mathrm{loc}})\big)_k \overset{\sim}{\to} X[p^\infty]^{\mathrm{loc}}$$

and

$$\eta(X[p^\infty]^{\mathrm{et}})^{-1} : \big(L(X[p^\infty]^{\mathrm{et}})\big)_k \overset{\sim}{\to} X[p^\infty]^{\mathrm{et}}.$$

These two isomorphisms uniquely determine an isomorphism

$$\varphi : G_k \overset{\sim}{\to} X[p^\infty]$$

via the unique section of (2.11) over k (see Lemma 2.4.2 and Lemma 2.4.7). We map (2.11) to the lift (G, φ). The two constructions are compatible with isomorphism classes and inverse to each other. □

2.4.7 The canonical lift

In this Section we assume R to be a complete noetherian local ring. Let X be an ordinary abelian variety over k and (A, φ) a lift of X. Recall from Section 2.4.4 that φ is an isomorphism $A_k \xrightarrow{\sim} X$.

Definition 2.4.9 *We say that (A, φ) is a* canonical lift *of X if the connected-étale sequence*

$$0 \to A[p^\infty]^{\mathrm{loc}} \to A[p^\infty] \to A[p^\infty]^{\mathrm{et}} \to 0$$

is split.

As one can see the isomorphism φ does not play a role in the above definition. By Lemma 2.4.7 the canonical lift is, as a lift, unique up to unique isomorphism. Next we will discuss the existence of a canonical lift. We remark that the elements of $\mathrm{Defo}_X(R)$ correspond to (not necessarily algebraic!) formal abelian schemes lifting X.

Theorem 2.4.10 *The zero element of* $\mathrm{Defo}_X(R)$ *is the completion of a projective abelian scheme. It satisfies the condition formulated in Definition 2.4.9, i.e. it is a canonical lift of X.*

Proof. Any element of $\mathrm{Defo}_X(R)$ is given by a compatible system of lifts (A_i, φ_i) $(i \geq 1)$ of X where A_i is an abelian scheme over $R_i = R/\mathfrak{m}^i$. The Barsotti-Tate group $X[p^\infty]$ is by Lemma 2.4.2 isomorphic to the product of its connected and étale part. A lift of $X[p^\infty]$ to R_i is given by

$$G_i = L\big(X[p^\infty]^{\mathrm{loc}}\big) \times L\big(X[p^\infty]^{\mathrm{et}}\big)$$

where L is the functor introduced in Section 2.4.5. This yields a compatible system of Barsotti-Tate groups lifting $X[p^\infty]$. By Theorem 2.4.3 there exists a compatible system (A_i, φ_i) as above such that $A_i[p^\infty] \cong G_i$.

We claim that the compatible system (A_i, φ_i) is induced by an abelian scheme over R. Taking limits one gets a proper formal group scheme A over R lifting X (see [GD71] Ch. I, Proposition 10.12.3.1 and [GD67] Ch. III, Section 3.4.1). In the following we will prove that A is algebraic. The abelian variety X is projective and hence there exists an ample line bundle $\mathcal{L}$ on X. We will construct a compatible system of line bundles $\mathcal{L}_i$ on the compatible system (A_i, φ_i) lifting $\mathcal{L}$. Let $\check{X}$ denote the dual abelian variety of X. There exists a compatible system of lifts of $\check{X}$ given by $(\check{A}_i, \check{\varphi}_i^{-1})$ where $\check{A}_i$ denotes the dual of A_i and $\check{\varphi}_i$ the dual of the morphism φ_i. The line bundle $\mathcal{L}$ determines an isogeny $\lambda : X \to \check{X}$. Next we prove that there exists a compatible system of isogenies $\lambda_i : A_i \to \check{A}_i$ lifting λ. By Theorem 2.4.3 it suffices to prove that there exists a unique lift of $\lambda[p^\infty]$ (the map induced by λ on Barsotti-Tate groups) to R_i for $i \geq 1$. Note that $\check{A}_i[p^\infty]$ decomposes as a product of its connected and étale part. This follows from Lemma 2.4.5. The morphism

$$L\big(\lambda[p^\infty]^{\mathrm{loc}}\big) \times L\big(\lambda[p^\infty]^{\mathrm{et}}\big) \tag{2.12}$$

over R_i lifts $\lambda[p^\infty]$. By Theorem 2.4.3 there exists a morphism λ_i inducing the morphism (2.12). The morphism λ_i is an isogeny since it is an isogeny on the special fiber. One can prove that λ_i is induced by an ample line bundle $\mathcal{L}_i$ on A_i (see [Oor71] §2, Lemma 2.3.2). We can assume that $\mathcal{L}_i$ is induced by $\mathcal{L}_{i+1}$ via base extension. By [GD67] Ch. III, Théorème 5.4.5 it follows that A is projective algebraic.

We finish the proof of the claim by proving that A is an abelian scheme. By [GD67] Ch. III, Théorème 5.4.1 we conclude that A is a group scheme. Since R is local it follows by [GD67] Ch. IV, Théorème 12.2.4 that the scheme A has geometrically integral fibers. The geometric fibers of A are complete group varieties and hence non-singular. The scheme A is flat over R (compare [Bou89] Ch. III, §5.2, Theorem 1). Hence it follows by [GD67] Ch. IV, Théorème 17.5.1 that A is smooth over R. This proves our claim. Finally we claim that the connected-étale sequence of $A[p^\infty]$ splits. This follows from the fact that over R_i the connected-étale sequence splits by construction and the splitting is unique by Lemma 2.4.7. As a consequence one gets a compatible system of sections of connected-étale sequences which by [GD71] Ch. I, Proposition 10.12.3.1 induces a section of the connected-étale sequence over R. □

The above proof is essentially the one presented in [Mes72] Ch.V, Th.3.3, generalized to the case where R is a complete noetherian local ring.

Lemma 2.4.11 *Let k be a finite field. The pair (A, φ) is a canonical lift of X if and only if the ring homomorphism*

$$\mathrm{End}(A) \to \mathrm{End}(X) \tag{2.13}$$

induced by reduction via φ is bijective.

Proof. Assume we are given a canonical lift (A, φ) of X. The method described in the proof of Theorem 2.4.10 that we used to lift the polarization

λ to R can also be used to lift endomorphisms of X to A. Hence the natural map (2.13) is surjective. It is also injective by the Rigidity Lemma (see [FMK94] Ch. 6, §1, Proposition 6.1).

Conversely, suppose that (A, φ) is a lift of X and the natural map (2.13) is bijective. Then there exists a lift F of the q-th power Frobenius on X where $q = \#k$. By Lemma 2.5.3 the kernel of F^i is equal to $A[q^i]^{\text{loc}}$. It follows by Lemma 2.5.2 that the connected-étale sequence of $A[p^\infty]$ has a section. □

More details about the canonical lift can be found in [Moo95] Ch. III, §1.

2.4.8 The torsion structure of the deformation space

Suppose R is artinian and X is an ordinary abelian variety over k. Let $l \in \mathbb{N}$ be the smallest natural number such that $\mathfrak{m}^l = 0$. We have already seen (see Theorem 2.4.8) that $\text{Defo}_X(R)$ is an abelian group.

Theorem 2.4.12 *We have*

$$p^{l-1} \cdot x = 0, \ \forall x \in \text{Defo}_X(R).$$

In the remainder of this Section we will give a proof of this Theorem. By Theorem 2.4.8 and Corollary 2.4.6 we have

$$\text{Defo}_{X_{\bar{k}}}(R^{\text{sh}}) = \text{Ext}^1_{R^{\text{sh}}}((\mathbb{Q}_p/\mathbb{Z}_p)^g, \mu^g) \cong \text{Ext}^1_{R^{\text{sh}}}(\mathbb{Q}_p/\mathbb{Z}_p, \mu)^{g^2}$$

where $\bar{k}$ denotes the residue field of R^{sh} (an algebraic closure of k) and g is the dimension of X. The following sheaf computation (compare [Mes72] Appendix, Prop.2.5) reveals the structure of the deformation space of $X_{\bar{k}}$ over R^{sh}.

Proposition 2.4.13 *Let R be an Artin local ring with perfect residue field of characteristic $p > 0$ and maximal ideal $\mathfrak{m}$. Then there is a natural isomorphism*

$$1 + \mathfrak{m} = \mu_R(R) \xrightarrow{\sim} \text{Ext}^1_R(\mathbb{Q}_p/\mathbb{Z}_p, \mu) \tag{2.14}$$

which is functorial in R.

Proof. We have an exact sequence of groups

$$0 \to \mathbb{Z} \to \mathbb{Z}[1/p] \to \mathbb{Q}_p/\mathbb{Z}_p \to 0, \tag{2.15}$$

which is the limit of the direct system of exact sequences of groups

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z} \arrow[r, "{[p^{n+1}]}"] & \mathbb{Z} \arrow[r] & \mathbb{Z}/p^{n+1}\mathbb{Z} \arrow[r] & 0 \\
0 \arrow[r] & \mathbb{Z} \arrow[r, "{[p^n]}"] \arrow[u, "\mathrm{id}"] & \mathbb{Z} \arrow[r] \arrow[u, "{[p]}"] & \mathbb{Z}/p^n\mathbb{Z} \arrow[r] \arrow[u] & 0.
\end{tikzcd}$$

The short exact sequence (2.15) induces a long exact sequence (we only write down the relevant terms)

$$\begin{aligned}\ldots \to \mathrm{Hom}_R(\mathbb{Z}[1/p], \mu) \xrightarrow{\gamma} \mathrm{Hom}_R(\mathbb{Z}, \mu) \xrightarrow{\delta} \mathrm{Ext}^1_R(\mathbb{Q}_p/\mathbb{Z}_p, \mu) \\ \to \mathrm{Ext}^1_R(\mathbb{Z}[1/p], \mu) \to \ldots\end{aligned}$$

We claim that δ is an isomorphism. First we prove injectivity. The map γ factors as

$$\mathrm{Hom}_R(\mathbb{Z}[1/p], \mu) \to \varprojlim \mathrm{Hom}_R(\mathbb{Z}, \mu) \to \mathrm{Hom}_R(\mathbb{Z}, \mu),$$

where the first map is the natural map and the second one is the projection onto the lowest factor. We have $\mathrm{Hom}_R(\mathbb{Z}, \mu) = \mu(R) = 1 + \mathfrak{m}$ and because of (2.8) it follows that

$$\varprojlim \mathrm{Hom}_R(\mathbb{Z}, \mu) = 0.$$

This shows that γ is the zero map and consequently δ is injective. Next we will prove that $\mathrm{Ext}^1_R(\mathbb{Z}[1/p], \mu) = 0$ which implies that δ is bijective. The functor $\mathrm{Hom}_R(\mathbb{Z}[1/p], \cdot)$ is the composition of the functor

$$F \mapsto (\mathrm{Hom}_R(\mathbb{Z}, F))_{i\in\mathbb{N}} \tag{2.16}$$

from the category of fppf-groups to the category of inverse systems of abelian groups, where the bonding morphisms are given by the multiplication-by-p map, with the inverse limit functor

$$(F_i)_{i\in\mathbb{N}} \mapsto \varprojlim_i F_i.$$

We claim that the functor (2.16) maps injectives to $\lim_{\leftarrow}$-acyclic inverse systems. Let I be an injective fppf-group. Since $[p]$ is a monomorphism on $\mathbb{Z}$ we conclude by the injectivity of I that the inverse system

$$\big(\mathrm{Hom}_R(\mathbb{Z}, I)\big)_{i\in\mathbb{N}}$$

has surjective transition morphisms. It follows by [GD67] Ch. 0, §13, Proposition 13.2.1 and Proposition 13.2.2 that it is $\lim_{\leftarrow}$-acyclic. By Grothendieck's Theorem [Mil80] App.B, Theo.1, there exists a spectral sequence

$$\Big(R^p \lim_{\leftarrow_i}\Big)\Big(\big(\mathrm{Ext}^q_R(\mathbb{Z},\mu)\big)_{i\in\mathbb{N}}\Big) \implies \mathrm{Ext}^{p+q}_R(\mathbb{Z}[1/p],\mu).$$

We get an exact sequence of lower terms

$$\begin{aligned} 0 \to R^1 \lim_{\leftarrow_i}\Big(\big(1+\mathfrak{m}\big)_{i\in\mathbb{N}}\Big) &\to \mathrm{Ext}^1_R(\mathbb{Z}[1/p],\mu) \\ \xrightarrow{\beta} \lim_{\leftarrow}\mathrm{Ext}^1_R(\mathbb{Z},\mu) &\to R^2 \lim_{\leftarrow_i}\Big(\big(1+\mathfrak{m}\big)_{i\in\mathbb{N}}\Big) \to \dots \end{aligned}$$

The inverse system $(1+\mathfrak{m})_{i\in\mathbb{N}}$ satisfies the Mittag-Leffler condition and as above it follows that $(1+\mathfrak{m})_{i\in\mathbb{N}}$ is $\lim_{\to}$ -acyclic. Thus the map β is bijective. We complete the proof of the Theorem by showing that

$$\lim_{\leftarrow}\mathrm{Ext}^1_R(\mathbb{Z},\mu) = 0. \tag{2.17}$$

The Kummer exact sequence

$$0 \to \mu_{p^n,R} \to \mathbb{G}_{m,R} \overset{[p^n]}{\to} \mathbb{G}_{m,R} \to 0$$

induces a long exact sequence of cohomology

$$\begin{aligned} 0 \to \mu(p^n)(R) \to R^* \to R^* \to \mathrm{H}^1\big(\mathrm{Spec}(R),\mu(p^n)\big) \\ \to \mathrm{H}^1(\mathrm{Spec}(R),\mathbb{G}_m) \to \dots \end{aligned}$$

Hilbert's Theorem 90 states that $\mathrm{H}^1(\mathrm{Spec}(R),\mathbb{G}_m) = \mathrm{Pic}(R) = 0$. This implies

$$\mathrm{H}^1\big(\mathrm{Spec}(R),\mu(p^n)\big) \cong R^*/(R^*)^{p^n} = (1+\mathfrak{m})/(1+\mathfrak{m})^{p^n}$$

for $n \geq 1$. The latter equality follows from the fact that k is perfect. Consequently $\mathrm{H}^1\big(\mathrm{Spec}(R),\mu(p^n)\big) = 1+\mathfrak{m}$ for sufficiently large n. It follows that

$$\mathrm{H}^1(\mathrm{Spec}(R),\mu) = \mathrm{H}^1\big(\mathrm{Spec}(R),\lim_{\to}\mu(p^n)\big) = \lim_{\to}\mathrm{H}^1\big(\mathrm{Spec}(R),\mu(p^n)\big) = 0.$$

Note that $\mathrm{Hom}_R(\mathbb{Z},F) = \Gamma(\mathrm{Spec}(R),F)$ for every abelian fppf-sheaf F. As a consequence $\mathrm{Ext}^1_R(\mathbb{Z},\mu) = 0$ which implies (2.17). □

The proof of Theorem 2.4.12 is completed by the following

Lemma 2.4.14 *The natural R-functorial group homomorphism*

$$\mathrm{Defo}_X(R) \to \mathrm{Defo}_{X_{\bar{k}}}(R^{\mathrm{sh}}) \tag{2.18}$$

given by base extension is injective.

Proof. We have to show that the natural map

$$\mathrm{Ext}^1_R\Big(L\big(X[p^\infty]^{\mathrm{et}}\big), L\big(X[p^\infty]^{\mathrm{loc}}\big)\Big) \to \mathrm{Ext}^1_{R^{\mathrm{sh}}}\big((\mathbb{Q}_p/\mathbb{Z}_p)^g, \mu^g\big)$$

induced by base extension is injective. Here g denotes the dimension of X. Suppose an extension defined over R splits over R^{sh}. Then it was already split over R because a section over R^{sh} is unique and hence descends to R. The obstruction for a section to be unique is given by $\mathrm{Hom}_{R^{\mathrm{sh}}}\big((\mathbb{Q}_p/\mathbb{Z}_p)^g, \mu^g\big)$. The latter is equal to zero since $\mathrm{Hom}_{R^{\mathrm{sh}}}(\mathbb{Q}_p/\mathbb{Z}_p, \mu) = 0$ as explained in Lemma 2.4.7. □

2.5 The proofs

In this Section we prove the statements presented in Section 2.1 and Section 2.2. We use the notation of the corresponding sections.

2.5.1 Proof of Proposition 2.1.1

In order to prove Proposition 2.1.1 we need the following proposition.

Proposition 2.5.1 *Let A be an abelian scheme over a noetherian ring R and G a finite flat subgroup of A. Then the quotient sheaf A/G is representable by an abelian scheme. The quotient map $A \to A/G$ is an isogeny.*

Proof. We sketch the proof. First assume that R is integral and normal. Then A is projective (see [Ray70b] Ch. XI, Théorème 1.4). Projectivity implies that every G-orbit lies in some open affine. As a consequence the quotient A/G is representable (compare [Ray67] §5, Théorème 1). The general case can be deduced from the above special case proceeding as in [FC90] Ch. I, Proof of Theorem 1.9. □

We switch to the notation of Proposition 2.1.1, i.e. A is an abelian scheme over R having ordinary reduction. By Proposition 2.5.1 there exists an isogeny

$$F : A \to A/A[p]^{\mathrm{loc}}.$$

There exists a commutative diagram

$$\begin{tikzcd}
A \arrow[r, "F"] \arrow[d, "{[p]}"'] & A^{(p)} \arrow[dl, "V"] \\
A &
\end{tikzcd}$$

since

$$\mathrm{Ker}(F) = A[p]^{\mathrm{loc}} \subseteq \mathrm{Ker}([p]_A).$$

The morphism V is an isogeny. This can be checked fiber-wise. The connected-étale sequence is well-behaved under reduction, i.e.

$$A_k[p]^{\mathrm{loc}} = \left(A[p]^{\mathrm{loc}}\right)_k.$$

This is due to the following. Let $A[p]^{\mathrm{loc}} = \mathrm{Spec}(C)$. The finite R-algebra C is connected, i.e. has only the trivial idempotents 0 and 1. This is also true for $C \otimes_R k$, since R is henselian and one can lift the idempotents of $C \otimes_R k$ to C (compare [Ray70a] Ch. I, §1).

The kernel K of relative Frobenius $A_k \to A_k^{(p)}$ has no non-zero points over an algebraic closure of k and hence is connected. Its order equals p^g where g is the relative dimension of A over R. Since $K \subseteq A_k[p]$ we get by comparing ranks

$$K = A_k[p]^{\mathrm{loc}} = (A[p]^{\mathrm{loc}})_k.$$

This proves Proposition 2.1.1.

2.5.2 Proof of Theorem 2.1.2

We use the same notation as in Section 2.1. The map F induces a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & A[p^\infty]^{\mathrm{loc}} \arrow[r] \arrow[d, "{F[p^\infty]^{\mathrm{loc}}}"] & A[p^\infty] \arrow[r] \arrow[d, "{F[p^\infty]}"] & A[p^\infty]^{\mathrm{et}} \arrow[r] \arrow[d, "{F[p^\infty]^{\mathrm{et}}}"] & 0 \\
0 \arrow[r] & A^{(p)}[p^\infty]^{\mathrm{loc}} \arrow[r] & A^{(p)}[p^\infty] \arrow[r] & A^{(p)}[p^\infty]^{\mathrm{et}} \arrow[r] & 0.
\end{tikzcd}$$

Lemma 2.5.2 *We have:*

1. *$F[p^\infty]$ is an epimorphism.*

2. *$F[p^\infty]^{\mathrm{et}}$ is an isomorphism.*

3. *$F[p^\infty]^{\mathrm{loc}}$ is an epimorphism.*

Proof. First consider the exact sequence of sheaves

$$0 \to A[p]^{\mathrm{loc}} \to A \xrightarrow{F} A^{(p)} \to 0.$$

Let S be an R-scheme and $s \in A^{(p)}[p^i](S)$ for some $i \geq 1$. Since F is an epimorphism there exists an fppf-covering $T \to S$ and $t \in A(T)$ such that $F(t)$ is induced by s. We must have $t \in A[p^\infty](T)$ because the order of the kernel $A[p]^{\mathrm{loc}}$ is p^g. Hence $F[p^\infty]$ is an epimorphism of fppf-sheaves. It follows that $F[p^\infty]^{\mathrm{et}}$ is an epimorphism. Since $\mathrm{Ker}(F[p^\infty]^{\mathrm{loc}}) = \mathrm{Ker}(F[p^\infty])$ we conclude by the Snake Lemma that there is a monomorphism

$$\delta : \mathrm{Ker}(F[p^\infty]^{\mathrm{et}}) \to \mathrm{Coker}(F[p^\infty]^{\mathrm{loc}}).$$

Suppose $\mathrm{Ker}(F[p^\infty]^{\mathrm{et}}) \neq 0$. The map δ_k is a closed immersion. Since R is henselian the map δ_k embeds a non-trivial finite étale group into a finite connected one. This is a contradiction. □

Consider the map $A \to A^{(p^j)}$ defined recursively by $F^j = F \circ F^{j-1}$, where $j \geq 1$ and $F^0 = \mathrm{id}$.

Lemma 2.5.3 *The map F^j has kernel $A[p^j]^{\mathrm{loc}}$.*

Proof. We prove this by induction on j. By Proposition 2.1.1 it is true for $j = 1$. Repeated pulling back yields a commutative diagram

$$\begin{tikzcd}
\mathrm{Ker}(F^{j-1}) \arrow[r] \arrow[d, "\epsilon"] & 0 \arrow[d] & \\
\mathrm{Ker}(F^j) \arrow[r, "\mu"] \arrow[d] & \mathrm{Ker}(F) \arrow[r] \arrow[d] & 0 \arrow[d] \\
A \arrow[r, "F^{j-1}"] & A^{(p^{j-1})} \arrow[r, "F"] & A^{(p^j)}
\end{tikzcd}$$

with all square subdiagrams Cartesian. The vertical and horizontal sequences

$$\begin{tikzcd}
 & & 0 \arrow[d] & & \\
 & & \mathrm{Ker}(F^j)^{\mathrm{loc}} \arrow[d] & & \\
0 \arrow[r] & \mathrm{Ker}(F^{j-1}) \arrow[r, "\epsilon"] & \mathrm{Ker}(F^j) \arrow[r, "\mu"] \arrow[d, "\beta"] & \mathrm{Ker}(F) \arrow[r] \arrow[dl, dashed, "\psi"] & 0 \\
 & & \mathrm{Ker}(F^j)^{\mathrm{et}} \arrow[d] & & \\
 & & 0 & &
\end{tikzcd}$$

are exact. The group $\mathrm{Ker}(F^{j-1})$ is connected (by assumption). As a consequence $\beta \circ \epsilon = 0$ and there exists a map ψ making the above diagram commutative. Since $\mathrm{Ker}(F)$ is connected it follows that $\psi = 0$. We conclude that $\mathrm{Ker}(F^j)$ is connected. □

Consider the map

$$\mathrm{Frob}(R) \quad : \quad \mathrm{Defo}_{A_k}(R) \to \mathrm{Defo}_{A_k^{(p)}}(R)$$

induced by the map

$$A \mapsto A^{(p)}. \tag{2.19}$$

Lemma 2.5.4 *The map* $\mathrm{Frob}(R)$ *is a homomorphism of groups and its kernel is equal to* $\mathrm{Defo}_{A_k}(R)[p]$*, i.e. the set of elements of order* p *in* $\mathrm{Defo}_{A_k}(R)$.

Proof. Let R be artinian. Then the map $\mathrm{Frob}(R)$ is equal to the map

$$\mathrm{Ext}^1_R(A[p^\infty]^{\mathrm{et}}, A[p^\infty]^{\mathrm{loc}}) \to \mathrm{Ext}^1_R(A^{(p)}[p^\infty]^{\mathrm{et}}, A^{(p)}[p^\infty]^{\mathrm{loc}})$$

given by

$$\mathrm{Ext}^1_R\big((F[p^\infty]^{\mathrm{et}})^{-1}, F[p^\infty]^{\mathrm{loc}}\big).$$

This map is a homomorphism of groups. By Lemma 2.5.2 and Lemma 2.5.3 the map $F[p^\infty]^{\mathrm{loc}}$ factors over the multiplication-by-p map on

$$\mathrm{Ext}^1_R(A[p^\infty]^{\mathrm{et}}, A[p^\infty]^{\mathrm{loc}})$$

followed by an isomorphism. For general R the claim follows by taking limits. □

After these preparatory remarks we are able to prove Theorem 2.1.2. Let R, A, B and I be as in the Theorem. Suppose $A \cong B \bmod I$. This means that $A - B$ is the zero element in $\mathrm{Defo}_{A_k}(R/I)$. We have

$$(R/I)^{\mathrm{sh}} = R^{\mathrm{sh}}/I_{\mathrm{sh}}$$

where by definition $I_{\mathrm{sh}} = R^{\mathrm{sh}}I$. Let $J = pI + \langle I\rangle_p$ and $J_{\mathrm{sh}} = R^{\mathrm{sh}}J$. With $\mathfrak{m}_{\mathrm{sh}}$ we denote the maximal ideal of R^{sh}. Then there is a commutative diagram

$$\begin{tikzcd}
\mathrm{Defo}_{A_k}(R/J) \arrow[r] \arrow[d] & 1 + (\mathfrak{m}_{\mathrm{sh}}/J_{\mathrm{sh}}) \arrow[d] \\
\mathrm{Defo}_{A_k}(R/I) \arrow[r] & 1 + (\mathfrak{m}_{\mathrm{sh}}/I_{\mathrm{sh}})
\end{tikzcd}$$

where the horizontal arrows are injective. The diagram is due to the functoriality of the maps (2.10), (2.14) and (2.18). The vertical map on the right hand side has kernel $1 + (I_{\mathrm{sh}}/J_{\mathrm{sh}})$. The inclusion

$$(1 + I_{\mathrm{sh}})^p \subseteq 1 + J_{\mathrm{sh}}$$

implies that the elements in the kernel of the vertical map on the left hand side have order p. Thus $A - B$ has order p in $\mathrm{Defo}_{A_k}(R/J)$. By Lemma 2.5.4 it follows that $A^{(p)} - B^{(p)}$ is the zero element in

$$\mathrm{Defo}_{A_k^{(p)}}(R/J).$$

This proves Theorem 2.1.2.

2.5.3 Proof of Corollary 2.1.4 and Corollary 2.1.5

We use the notation of Section 2.1. We claim that Corollary 2.1.4 and Corollary 2.1.5 follow from Theorem 2.1.2 by taking $B = A^*$ and $I = \mathfrak{m}^i$ where $i \geq 1$. Note that we have $pI + \langle I\rangle_p \subseteq \mathfrak{m}^{i+1}$. In order to prove the convergence of the sequences

$$\left(A^{(q^n)}\right) \quad \text{and} \quad \left(A^{(\wp^n)}\right)$$

in $\mathrm{Defo}_{A_k}(R)$ it remains to show that

$$\left(A^*\right)^{(q)} \cong A^* \quad \text{and} \left(A^*\right)^{(\wp)} \cong A^*. \tag{2.20}$$

By Lemma 2.5.2 the splitting of the connected-étale sequence for A^* implies the splitting of the connected-étale sequence for $(A^*)^{(p)}$ and hence also for $(A^*)^{(q)}$. The connected-étale sequence on $(A^*)^{(\wp)}$ is obtained by base-extending the one for $(A^*)^{(p)}$ via the automorphism $\mathrm{Spec}(\sigma^{-1})$. Hence it is split as well. The existence of the isomorphisms (2.20) follows from the uniqueness of the canonical lift.

2.5.4 Proof of Proposition 2.2.1

We use the notation of Section 2.2. In order to prove Proposition 2.2.1 we state the following lemma.

Lemma 2.5.5 *Let E be an elliptic curve over R with $E[2] \cong \mu_{2,R} \times_R (\mathbb{Z}/2\mathbb{Z})_R$. Then E_K can be given by a model*

$$y^2 = x(x-\alpha)(x-\beta), \;\; \alpha, \beta \in K^*, \;\; \alpha \neq \beta, \tag{2.21}$$

where $(0,0)$ generates $E[2]^{\mathrm{loc}}(K)$ and $\frac{\beta}{\alpha} \in 1 + 16R$.

Proof. We can assume that E is given by the equation (2.21) and $(0,0)$ generates $E[2]^{\mathrm{loc}}(K)$. We set $\lambda = \frac{\beta}{\alpha}$. Then

$$j(E) = j(E_K) = 2^8 \frac{\left((\lambda-1)^2 + \lambda\right)^3}{\lambda^2(\lambda-1)^2}. \tag{2.22}$$

Let v be the discrete additive valuation of K satisfying $v(2) = 1$. Since E has ordinary good reduction it follows that $j(E) \not\equiv 0 \bmod 2$. Hence equation (2.22) implies

$$0 = 8 + 3v((\lambda-1)^2 + \lambda) - 2v(\lambda) - 2v(\lambda - 1). \tag{2.23}$$

An isomorphism to a minimal model is of the form

$$(x, y) \rightarrow (u^2 x + r, \ldots).$$

We can assume that the discriminant of the given model is a unit and hence $u \in R^*$. Since $(0,0)$ is in the kernel of reduction it follows that $v(r) < 0$. Also we have $v(u^2\alpha + r) \geq 0$ and $v(u^2\beta + r) \geq 0$ since the points $(\alpha, 0)$ and $(\beta, 0)$ are not in the kernel of reduction. We conclude that $v(\alpha) = v(\beta) = v(r)$ which implies $v(\lambda) = 0$. By (2.23) we cannot have $v(\lambda - 1) = 0$. Hence $v(\lambda - 1) > 0$, and it follows again by (2.23) that $v(\lambda - 1) = 4$. This implies the Lemma. □

Now we prove Proposition 2.2.1. Let E be as in the Proposition and let

$$y^2 = x(x-\alpha)(x-\beta), \;\; \alpha, \beta \in K^*, \;\; \alpha \neq \beta,$$

be a model for E having the properties listed in Lemma 2.5.5. Over $L = K(i)$ the above curve is isomorphic to the twisted curve E^t given by

$$y^2 = x(x+\alpha)(x+\beta)$$

via the isomorphism

$$(x,y) \mapsto (-x, iy). \tag{2.24}$$

Now by [Sil86] Ch.X, Prop.1.4 we have an equivalence

$$\alpha, \beta \in K^{*2} \Leftrightarrow [2]_{E^t}^{-1}(0,0)(K) \neq \emptyset. \tag{2.25}$$

We claim that the right hand side of (2.25) holds. Let $G_L = \mathrm{Gal}(L/K)$. The isomorphism (2.24) induces an isomorphism of groups $E[4](L) \xrightarrow{\sim} E^t[4](L)$. One computes $\sigma(P^t) = -(\sigma(P))^t$ for $\mathrm{id} \neq \sigma \in G_L$. As a consequence $\sigma(P^t) = P^t$ if and only if $\sigma(P) = -P$. Hence

$$[2]_E^{-1}(0,0)(K) = \emptyset \implies [2]_{E^t}^{-1}(0,0)(K) \neq \emptyset. \tag{2.26}$$

Suppose $P \in [2]_E^{-1}(0,0)(K)$. Let Q be a point of order 2 which does not lie in the kernel of reduction. Then

$$[2]_E^{-1}(0,0)(K) = \{P, -P, P+Q, -(P+Q)\}.$$

Two of these four points have to be in the kernel of reduction. Thus the points of $E[4]^{\mathrm{loc}}$ are rational over K. We have $E[4]^{\mathrm{loc}}_{\bar{K}} \cong \mu_{4,\bar{K}}$ over $\bar{K}$. This implies $i \in K$ which is a contradiction. Since the converse direction in Proposition 2.2.1 is trivial this finishes the proof.

2.5.5 Proof of Proposition 2.2.2

We use the notation of Section 2.2 and Section 2.5.4. The curve E_K is isogenous with the elliptic curve

$$y^2 = x\left(x - \left(\frac{a-b}{2}\right)^2\right)\left(x - \left(\frac{a+b}{2}\right)^2\right) \tag{2.27}$$

via the isogeny

$$(x,y) \mapsto \left(\frac{y^2}{4x^2}, \frac{y(ab-x)(ab+x)}{8x^2}\right)$$

which has kernel equal to

$$E[p]^{\mathrm{loc}}(\bar{K}) = \langle (0,0) \rangle.$$

The point $(0,0)$ on the curve defined by (2.27) is not in the kernel of reduction since it is the image of the point $(a^2,0)$ or $(b^2,0)$ which induce a non-trivial point in $E[p]^{\mathrm{et}}(K)$. It follows by Lemma 2.5.2 that $(0,0)$ on the curve (2.27) has non-zero image in the étale part of the p-torsion. Consider the x-coordinates

$$\left(\frac{a-b}{2}\right)^2 \quad \text{and} \quad \left(\frac{a+b}{2}\right)^2$$

of the other two 2-torsion points. The one with the smaller valuation is the x-coordinate of the 2-torsion point in the kernel of reduction, because an isomorphism over K to a minimal model preserves the ordering given by the valuations. Let v be a discrete additive valuation of K such that $v(2) = 1$. Since $b/a \in 1 + 8R$ it follows that

$$v(a+b) = v(a) + v(1 + \frac{b}{a}) = v(a) + 1 < v(a) + v(1 - \frac{b}{a}) = v(a-b).$$

Mapping

$$(x, y) \mapsto \left(x - \left(\frac{a+b}{2}\right)^2, y\right)$$

yields the model (2.4). The isogeny $F_K : E_K \to E_K^{(2)}$ is given by

$$(x, y) \mapsto \left(\frac{(x+ab)^2}{4x}, \frac{y(ab-x)(ab+x)}{8x^2}\right).$$

Bibliography

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron models.* Number 21 in Ergebnisse der Mathemathik, 3. Folge. Springer-Verlag, 1990.

[Bou89] Nicolas Bourbaki. *Commutative algebra, Chapters 1-7.* Elements of Mathematics. Springer-Verlag, second edition, 1989.

[Cox84] David Cox. The arithmetic-geometric mean of Gauss. *Enseignement Mathématique (2)*, 30(3–4):275–330, 1984.

[FC90] Gerd Faltings and Ching-Li Chai. *Degeneration of abelian varieties.* Number 22 in Ergebnisse der Mathematik, 3. Folge. Springer-Verlag, 1990.

[FMK94] John Fogarty, David Mumford, and Frances Kirwan. *Geometric invariant theory.* Number 32 in Ergebnisse der Mathemathik, 2. Folge. Springer-Verlag, third edition, 1994.

[GD67] Alexander Grothendieck and Jean Dieudonné. *Éléments de géométrie algébrique I-IV.* Number 4,8,11,17,20,24,28,32 in Publications Mathématiques. Institut des Hautes Études Scientifiques, 1960–1967.

[GD71] Alexander Grothendieck and Jean Dieudonné. *Éléments de géométrie algébrique I.* Springer-Verlag, 1971.

[Gro74] Alexander Grothendieck. *Groupes de Barsotti-Tate et cristaux de Dieudonné.* Les presses de l'université de Montréal, 1974.

[Kat81] Nicholas Katz. Serre-Tate local moduli. In Jean Giraud, Luc Illusie, and Michel Raynaud, editors, *Surfaces algébriques*, number 868 in Lecture Notes in Mathematics, pages 138–202. Springer-Verlag, 1981.

[LL03] Reynald Lercier and David Lubicz. A quasi-quadratic time algorithm for hyperelliptic curve point counting. unpublished, available at http://www.math.u-bordeaux.fr/∼lubicz, 2003.

[Mes72] William Messing. *The crystals associated to Barsotti-Tate groups.* Number 264 in Lecture Notes in Mathematics. Springer-Verlag, 1972.

[Mes02] Jean-François Mestre. Algorithmes pour compter des points en petite caractéristique en genre 1 et 2. unpublished, rédigé par D. Lubicz, available at http://www.maths.univ-rennes1.fr/crypto/2001-02/mestre.ps, 2002.

[Mil80] John Milne. *Étale cohomology.* Princeton University Press, 1980.

[Moo95] Ben Moonen. *Special points and linearity properties of Shimura varieties.* PhD thesis, Universiteit Utrecht, The Netherlands, 1995.

[Oor71] Frans Oort. Finite group schemes, local moduli for abelian varieties, and lifting problems. *Compositio Mathematica*, 23:265–296, 1971.

[Ray67] Michel Raynaud. Passage au quotient par une relation d'équivalence plate. In Tonny A. Springer, editor, *Local fields, Proceedings of a Conference held at Driebergen, The Netherlands.* Springer-Verlag, 1967.

[Ray70a] Michel Raynaud. *Anneaux locaux henséliens.* Number 169 in Lecture Notes in Mathematics. Springer-Verlag, 1970.

[Ray70b] Michel Raynaud. *Faisceaux amples sur les schémas en groupes et les espaces homogènes.* Number 119 in Lecture Notes in Mathematics. Springer-Verlag, 1970.

[Rit03] Christophe Ritzenthaler. *Problèmes arithmétiques relatifs à certaines familles de courbes sur les corps finis.* PhD thesis, Université Paris 7, Denis-Diderot, France, 2003.

[Sil86] Joseph H. Silverman. *The arithmetic of elliptic curves.* Number 106 in Graduate Texts in Mathematics. Springer-Verlag, 1986.

[Tat97] John Tate. Finite flat group schemes. In Gary Cornell, Joseph H. Silverman, and Glenn Stevens, editors, *Modular forms and Fermat's last theorem.* Springer-Verlag, 1997.

Chapter 3

Point counting on elliptic curves

In this chapter we provide an algorithm for computing the generalized arithmetic geometric mean (GAGM) sequence in the case of an elliptic curve and $p > 2$. For the definition of the GAGM sequence see Section 2.1. A basic step in our algorithm is to compute an explicit Frobenius lift. We show how to use the algorithm in order to count points on an ordinary elliptic curve over a finite field of characteristic $p > 2$.

Structure of Chapter 3:	
Section 3.1:	We provide explicit formulas describing a lift of the relative Frobenius assuming that the defining polynomial of a lift of the kernel of the relative Frobenius is given. These formulas are not restricted to the ordinary case.
Section 3.2:	We describe an algorithm for computing a lift of relative Frobenius in the ordinary case. We give a complexity bound for an algorithm, which approximates the lift of the relative Frobenius with given precision.
Section 3.3:	We present a point counting algorithm for ordinary elliptic curves over a finite field of characteristic $p > 2$, based on the computation of the GAGM sequence.
Section 3.4:	We collect some facts about division polynomials, which are used in the proof of correctness of Algorithm 3.2.2.
Section 3.5:	We complete the proofs of the statements made in Section 3.1, Section 3.2 and Section 3.3.
Perspectives	
Acknowledgments	
Bibliography	

3.1 An explicit lift of relative Frobenius

Let R denote a complete discrete valuation ring with perfect residue field k of characteristic $p > 2$ and K its field of fractions. Let π be a uniformizer of R and $\bar{K}$ an algebraic closure of K. We assume K to have characteristic 0.

Consider an elliptic curve E over K having good reduction. Also we assume that $\#E[2](K) = 4$. The curve E admits a model

$$y^2 = x(x-a)(x-b) \tag{3.1}$$

where $a, b \in R^*$ and $a \not\equiv b \bmod \pi$. Let $\bar{E}$ be the reduction of E, which is given by

$$y^2 = x(x-\bar{a})(x-\bar{b}),$$

where the coefficients

$$\bar{a} \equiv a \bmod \pi \quad \text{and} \quad \bar{b} \equiv b \bmod \pi$$

are in k. Let $\bar{E}^{(p)}$ over k be the elliptic curve with equation

$$y^2 = x(x-\bar{a}^p)(x-\bar{b}^p).$$

The isogeny $\bar{F} : \bar{E} \to \bar{E}^{(p)}$ over k defined by $(x,y) \mapsto (x^p, y^p)$ is called the *relative Frobenius*. In the following we will discuss necessary conditions for a lift of the relative Frobenius to exist.

Assume we are given a subgroup $G \leq E[p](\bar{K})$ of order p being defined over K, i.e. $\sigma(G) = G$ for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$. Let $S \subseteq G$ such that $S \cap -S = \emptyset$ and $G = S \cup -S \cup \{0_E\}$, where 0_E denotes the zero section of E. We set

$$P_1 = (0,0), \quad P_2 = (a,0) \quad \text{and} \quad P_3 = (b,0).$$

Let $x(Q)$ denote the x-coordinate of a point $0_E \neq Q \in E(\bar{K})$. We define

$$h(x) = \prod_{Q \in S} \left(\frac{x}{x(Q)} - 1 \right)$$

and

$$g_i(x) = \prod_{Q \in S} \big(x - x(Q + P_i) \big), \quad i = 1,2,3.$$

Note that $x(Q) \neq 0$ for $Q \in S$, since $p > 2$. Since G is defined over K, the polynomials $h(x)$ and $g_i(x)$, $i = 1,2,3$, are elements of $K[x]$.

Theorem 3.1.1 *Let $G \subseteq E[p](\bar{K})$ defined over K have order p. Suppose G is contained in the kernel of reduction. Let $E^{(p)}$ be defined by*

$$y^2 = x\big(x - a^{(p)}\big)\big(x - b^{(p)}\big),$$

where

$$a^{(p)} = a^p \cdot \left(\frac{h(b)}{h(a)}\right)^2 \quad \text{and} \quad b^{(p)} = b^p \cdot \left(\frac{h(a)}{h(b)}\right)^2.$$

Then $E^{(p)}$ is an elliptic curve, and there exists an isogeny

$$F : E \to E^{(p)}$$

given by

$$(x, y) \mapsto \left(\frac{x g_1(x)^2}{h(x)^2}, \frac{\prod_{i=1}^3 g_i(x)}{h(x)^3} y\right)$$

having kernel G. We have $a^{(p)}, b^{(p)} \in R$ and $h(x), g_i(x) \in R[x]$, $i = 1, 2, 3$. The curve $E^{(p)}$ reduces to $\bar{E}^{(p)}$ and the isogeny F lifts the relative Frobenius $\bar{F}$. Also we have

$$F^*\left(\frac{dx}{y}\right) = \operatorname{lead}(h) \cdot \frac{dx}{y},$$

where lead(h) *denotes the leading coefficient of $h(x)$.*

A proof of Theorem 3.1.1 can be found in Section 3.5.1. Formulas of the same kind, but for separable isogenies, can be found in [Vel71]. A subgroup G as in the theorem does not always exist. In this chapter we focus on the following special case.

Remark 3.1.2 *Let E have ordinary reduction. Then there exists a subgroup $G \leq E[p](\bar{K})$ defined over K, which is uniquely determined by the conditions that it is of order p and lies in the kernel of reduction.*

The above remark is proven at the end of Section 3.5.1. Taking together Theorem 3.1.1 and Remark 3.1.2 we get an elementary proof for the existence of a lift of relative Frobenius in the case of ordinary reduction. For a more general existence theorem see Proposition 2.1.1.

Also in the case that E has supersingular reduction a subgroup G as in Theorem 3.1.1 can exist. We do not discuss this here.

3.2 An algorithm for lifting Frobenius in the ordinary case

Let now $R = W_p(\mathbb{F}_q)$, where $\mathbb{F}_q$ denotes the finite field with q elements. Let E be as in Section 3.1. We assume that E has ordinary reduction. By Remark 3.1.2 we can apply Theorem 3.1.1 in order to get an explicit Frobenius lift. Let $E^{(p)}$, $a^{(p)}$ and $b^{(p)}$ be as in Theorem 3.1.1.

Theorem 3.2.1 *There exists a deterministic algorithm having as input the coefficients a and b of E with precision m and as output the coefficients $a^{(p)}$ and $b^{(p)}$ of $E^{(p)}$ with precision m. This algorithm has complexity*

$$\tilde{O}\big(p^2 dm\big)$$

where $d = \log_p(q)$.

We say that an element $x \in R$ is given with *precision m* if it is given modulo p^m. One can carry out arithmetic operations with precision m by considering the given quantities as elements of the quotient ring $R/(p^m)$. For the implementation of the arithmetic in $R/(p^m)$ see [FGH00] §2.

Recall the definition of the $\tilde{O}$*-notion*. Let X be a set and let $f, g : X \to \mathbb{R}^+$ be functions. We define

$$f \in \tilde{O}(g) \coloneqq \big(\exists c \geq 0\big)\big(\forall x \in X\big)\ \ f(x) \leq \max\big(2, \log_2 g(x)\big)^c \cdot g(x).$$

Instead of writing $f \in \tilde{O}(g)$, we also say that f is of order $\tilde{O}(g)$. In our case X is the set of all possible inputs of the Algorithm 3.2.2 and f is the function describing the running time depending on the input. In general we say that an algorithm has complexity $\tilde{O}(g)$, if the function describing the number of bit operations, needed to compute the output in terms of the input, is of order $\tilde{O}(g)$.

In the following we will outline the algorithm, whose existence is claimed in Theorem 3.2.1. By $\psi_p(x)$ we denote the p-th division polynomial corresponding to the points of order p on E. For a definition of ψ_p and its properties see Section 3.4.

Algorithm 3.2.2 *Input: $a, b \in R/(p^m)$; Output: $a^{(p)}, b^{(p)} \in R/(p^m)$*

1. *Compute $\psi_p(x) \bmod p^m$. See Section 3.5.2 for the algorithm that we use to compute $\psi_p(x)$.*

2. *Find a decomposition*

$$\psi_p(x) \equiv U(x) \cdot V(x) \bmod p^m$$

   where

$$U(x) \equiv \psi_p(x) \bmod p \quad \textit{and} \quad V(x) \equiv 1 \bmod p$$

   using Hensel's Lemma.

3. *Compute*

$$a^{(p)} = a^p \cdot \left(\frac{V(b)}{V(a)}\right)^2 \bmod p^m \quad \textit{and} \quad b^{(p)} = b^p \cdot \left(\frac{V(a)}{V(b)}\right)^2 \bmod p^m.$$

The correctness of the above algorithm and the complexity bound of Theorem 3.2.1 is proven in Section 3.5.2.

3.3 The GAGM sequence and point counting

Let $\bar{E}$ be an ordinary elliptic curve over a finite field $\mathbb{F}_q$ of characteristic $p > 2$ given by the Weierstrass equation

$$y^2 = x(x - \bar{a})(x - \bar{b})$$

where $\bar{a}, \bar{b} \in \mathbb{F}_q$. By our assumptions all points on $\bar{E}$ of order 2 are rational over $\mathbb{F}_q$.

Theorem 3.3.1 *There exists a deterministic algorithm having as input a finite field $\mathbb{F}_q$ and the coefficients $\bar{a}, \bar{b}$ of $\bar{E}$ and as output the number $\#\bar{E}(\mathbb{F}_q)$. This algorithm has complexity*

$$\tilde{O}(p^2 d^3)$$

where $d = \log_p(q)$.

In the following we will present the algorithm, whose existence is claimed in Theorem 3.3.1. The correctness of the algorithm and the complexity bound of Theorem 3.3.1 will be proven in Section 3.5.3. In the following exposition of our algorithm we use the notation introduced in the Sections 3.1 and 3.2.

Algorithm 3.3.2 *Input: $\bar{a}, \bar{b} \in \mathbb{F}_q$; Output: $\#\bar{E}(\mathbb{F}_q)$*

1. *Set*

$$d = \log_p(q) \quad \textit{and} \quad m = \lfloor d/2 \rfloor + 3.$$

2. *Choose $a, b \in R/(p^m)$ such that*

$$a \equiv \bar{a} \bmod p \quad \textit{and} \quad b \equiv \bar{b} \bmod p.$$

3. *Compute the sequence*

$$a, b, a_1, b_1, \ldots, a_{m-1}, b_{m-1},$$

where $a_i = a^{(p^i)}$ and $b_i = b^{(p^i)}$, by iterating $(m-1)$-times the Algorithm 3.2.2 with precision m.

4. *Compute a sequence*

$$a_m, b_m, c_m, \ldots, a_{m+d-1}, b_{m+d-1}, c_{m+d-1},$$

where a_i, b_i are as in Step 3 computed with precision m and c_i is computed with precision $m-1$ as follows. We use a modified version of Algorithm 3.2.2 having as additional output the number

$$c = \left(\frac{\operatorname{lead}(V)}{p \cdot V(0)}\right)^{-1} \bmod p^{m-1},$$

where $\operatorname{lead}(V)$ denotes the leading coefficient of the polynomial $V(x)$ computed in Step 2 of Algorithm 3.2.2. Compute iteratively

$$e = \left(\prod_{i=m}^{m+d-1} c_i\right) \bmod p^{m-1}.$$

5. *If $j(\bar{E}) \neq 0$ then find the unique $u \in R/(p^{m-1})$ satisfying*

$$u^4 \equiv \frac{a_{m-1}^2 - a_{m-1}b_{m-1} + b_{m-1}^2}{a_{m+d-1}^2 - a_{m+d-1}b_{m+d-1} + b_{m+d-1}^2} \bmod p^{m-1}$$

and $u \equiv 1 \bmod p$. This can be done using Newton iteration. Otherwise find the unique solution of the congruence

$$u^6 \equiv \frac{2a_{m-1}^3 - 3a_{m-1}^2 b_{m-1} - 3a_{m-1}b_{m-1}^2 + 2b_{m-1}^3}{2a_{m+d-1}^3 - 3a_{m+d-1}^2 b_{m+d-1} - 3a_{m+d-1}b_{m+d-1}^2 + 2b_{m+d-1}^3}$$

modulo p^{m-1} using that $u \equiv 1 \bmod p$. Set

$$v = u \cdot e \bmod p^{m-1}$$

and compute

$$t = \left\{ \begin{array}{cc} v + \frac{q}{v} & \textit{if} \quad d = 2 \\ v & \textit{if} \quad d > 2 \end{array} \right\} \bmod p^{m-1}.$$

Ensure that $|t| \leq 2\sqrt{q}$ by choosing a suitable representative of its class modulo p^{m-1} and return $q + 1 - t$.

We remark that in Step 3 one could compute the GAGM sequence until the $(m-1)$-th curve increasing the precision in each step by one. This is justified by Theorem 2.1.2 of Section 2.1. Doing so one could achieve a better performance in practice, but the complexity stays the same.

3.4 Division polynomials

Let K be a field of characteristic $\neq 2$. Suppose we are given an elliptic curve E over K by an equation

$$y^2 = x(x-a)(x-b) \tag{3.2}$$

where $a, b \in K^*$ and $a \neq b$. In this section we introduce the so-called division polynomials, which describe the torsion of E.

Definition 3.4.1 *Let*

$$\begin{aligned}
&\psi_0 = 0, \ \ \psi_1 = 1, \ \ \psi_2 = 2y \\
&\psi_3 = 3x^4 - 4(a+b)x^3 + 6abx^2 - (ab)^2 \\
&\psi_4 = 2y\big(2x^6 - 4(a+b)x^5 + 10abx^4 - 10(ab)^2x^2 \\
&\quad +4(ab)^2(a+b) - 2(ab)^3\big) \\
&\ldots \\
&\psi_{2l+1} = \psi_{l+2}\psi_l^3 - \psi_{l-1}\psi_{l+1}^3, \ \ l \geq 2, \\
&\psi_{2l} = \frac{\psi_l}{2y}(\psi_{l+2}\psi_{l-1}^2 - \psi_{l-2}\psi_{l+1}^2), \ \ l > 2.
\end{aligned}$$

The polynomial $\psi_m(x, y)$, $m \geq 0$, is called the m-th division polynomial *of E.*

Note that for even m the polynomial $\psi_m(x, y)$ is divisible by $2y$. This can be proven by induction and shows that our definition is correct. The polynomial $\psi_m(x, y)$ defines a function on E. The following Proposition is well-known.

Proposition 3.4.2 *Assume K to be algebraically closed. Then the function*

$$\psi_m : E \to \mathbb{P}^1_K, (x,y) \mapsto \psi_m(x,y)$$

has divisor

$$\sum_{P \in E[m](K)} \deg_{\mathrm{i}}[m](P) \quad - \quad m^2(0_E),$$

where 0_E denotes the point at infinity and $\deg_{\mathrm{i}}[m]$ *the degree of inseparability of the isogeny $[m] : E \to E$.*

In the following we assume that m is odd. By induction one proves that the variable y in $\psi_m(x,y)$ occurs only with even exponent. Substituting successively y^2 by $x(x-a)(x-b)$ we get a polynomial in the variable x. We denote the resulting polynomial by $\psi_m(x)$. Let $\bar{K}$ denote an algebraic closure of K. Choose $S \subseteq E[m](\bar{K})$ such that $S \cap -S = \emptyset$ and $E[m](\bar{K}) = S \cup -S \cup \{0_E\}$.

Corollary 3.4.3 *There exists a constant $c \in K$ such that*

$$\psi_m(x) = c \prod_{P \in S} (x - x(P))^{\deg_i[m]} \tag{3.3}$$

where $x(P)$ denotes the x-coordinate of P. If $\deg_i[m] = 1$*, then*

$$\deg(\psi_p) = \frac{m^2-1}{2} \quad and \quad c = m.$$

Proof. The first claim follows from Proposition 3.4.2, since the function on the right hand side of equation (3.3) has the same divisor as $\psi_m(x)$. Now assume that $\deg_i[m] = 1$. This implies that $\psi_m(x)$ has degree $(m^2-1)/2$. Using induction on m one shows that the coefficient of $x^{(m^2-1)/2}$ in $\psi_m(x)$ equals m. This implies the second claim. □

Now let $\mathbb{F}_q$ be a finite field of characteristic $p > 2$, $R = W_p(\mathbb{F}_q)$ the ring of Witt vectors with values in $\mathbb{F}_q$ and K its field of fractions. Assume that $a, b \in R^*$ and $a \not\equiv b \bmod p$, where a and b are the coefficients of the elliptic curve (3.2). By our assumption the model (3.2) is a Weierstrass minimal model and E has good reduction. Let v be an additive discrete valuation of K normalized such that $v(p) = 1$.

Proposition 3.4.4 *The curve E has ordinary reduction if and only if the Newton polygon of $\frac{1}{p}\psi_p(x)$ with respect to v is as in* Figure 3.1.

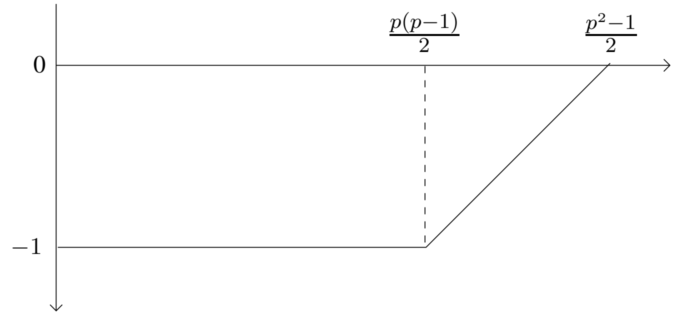

Figure 3.1: Newton polygon in case of ordinary reduction

Proof. We use the notation from above. Let $\psi_p(x) \in R[x]$ denote the p-th division polynomial on E and $\bar{\psi}_p(x) \in k[x]$ its reduction modulo p. Since $\operatorname{char}(K) = 0$, the degree of inseparability of $[m]$ on E equals 1. By Corollary 3.4.3 the polynomial $\psi_p(x)$ has degree $(p^2-1)/2$ and leading coefficient p. The unique extension of v to $\bar{K}$ will also be denoted by v. Note that $Q \in E(\bar{K})$ is in the kernel of reduction if and only if

$$v\big(x(Q)\big) < 0.$$

Since $p > 2$, the x-coordinates of points in $E[p](\bar{K})$, which are not in the kernel of reduction, have valuation 0.

Assume that E has ordinary reduction. This means that $\#\bar{E}(\bar{k}) = p$ and the degree of inseparability of the isogeny $[p]$ on $\bar{E}$ equals p (compare [Sil86] Ch.III, Corollary 6.4). By Corollary 3.4.3 we conclude that $\bar{\psi}_p(x)$ has degree $p(p-1)/2$. By the above discussion the Newton polygon of $\psi_p(x)$ has a segment of slope 0 and length $p(p-1)/2$. Also it has a segment of strictly positive slope, which has length $(p-1)/2$ and corresponds to the points of $E[p](\bar{K})$ lying in the kernel of reduction. Since by Corollary 3.4.3 the leading coefficient of $\psi_p(x)$ equals p and v is integer valued on K, we conclude that the constant term of $\psi_p(x)$ has valuation 0 and the segment of strictly positive slope of the Newton polygon of $\psi_p(x)$ is a straight line.

Assume that E has supersingular reduction. Then $\#\bar{E}(\bar{k}) = 1$. By Corollary 3.4.3 the polynomial $\bar{\psi}_p(x)$ equals a constant. This implies that the Newton polygon of $\psi_p(x)$ has strictly positive slope. This finishes the proof of the proposition. □

For more details about division polynomials we refer to [Lan78] Ch.II and [Cas66].

3.5 The proofs

In this Section we prove the statements of Section 3.1, Section 3.2 and Section 3.3.

3.5.1 Proof of Theorem 3.1.1 and Remark 3.1.2

In the following we prove Theorem 3.1.1. We use the notation of Section 3.1. Abstract theory guarantees the existence of a quotient $E^{(p)}$ of E by G. We have to construct suitable coordinate functions $\tilde{x}$ and $\tilde{y}$ on $E^{(p)}$ using the coordinates x and y on E. Consider the functions $\tilde{x}, \tilde{y} : E \to \mathbb{P}^1_K$ given by

$$\tilde{x}(x,y) = \frac{x g_1(x)^2}{h(x)^2}$$

and

$$\tilde{y}(x,y) = \frac{\prod_{i=1}^{3} g_i(x)}{h(x)^3} y.$$

The function $\tilde{x}$ has divisor

$$2 \cdot \sum_{Q \in G} \big(Q + P_1\big) - 2 \cdot \sum_{Q \in G} \big(Q\big) \tag{3.4}$$

and the function $\tilde{y}$ has divisor

$$\sum_{i=1}^{3} \sum_{Q \in G} \big(Q + P_i\big) - 3 \cdot \sum_{Q \in G} \big(Q\big). \tag{3.5}$$

We claim that the functions $\tilde{x}$ and $\tilde{y}$ are G-invariant, i.e. invariant under composing with translations given by points of G. There exist G-invariant functions on E having the divisors (3.4) and (3.5). The latter is due to the fact that by abstract theory the quotient $E^{(p)}$ exists and we can pull back suitable coordinate functions. They differ multiplicatively from $\tilde{x}$ resp. $\tilde{y}$ by a constant. This implies the claim.

We claim that the functions $\tilde{x}$ and $\tilde{y}$ defined above satisfy the equation

$$(\tilde{y})^2 = \tilde{x}\big(\tilde{x} - a^{(p)}\big)\big(\tilde{x} - b^{(p)}\big). \tag{3.6}$$

One computes

$$a g_1(a)^2 = a \prod_{Q \in S} \big(a - x(Q + P_1)\big)^2 = a \prod_{Q \in S} a^2 \left(1 - \frac{b}{x(Q)}\right)^2 = a^p h(b)^2$$

and hence by definition

$$\tilde{x}(P_2) = a^{(p)}.$$

Similarly one gets

$$\tilde{x}(P_3) = b^{(p)}.$$

It follows that the divisors of $(\tilde{y})^2$ and

$$\tilde{x}\big(\tilde{x} - a^{(p)}\big)\big(\tilde{x} - b^{(p)}\big)$$

are equal. Hence these two functions differ multiplicatively by a constant. We determine the constant by looking at expansions in $z = -\frac{x}{y}$. One has

$$x(z) = \frac{1}{z^2} + \dots \quad \text{and} \quad y(z) = -\frac{1}{z^3} + \dots$$

We set $l = \mathrm{lead}(h)$. Then

$$h(x(z)) = \frac{l}{z^{p-1}} + \dots$$

Since the $g_i(x)$, $i = 1, 2, 3$, are monic we get

$$\tilde{x}\big(x(z), y(z)\big) = \frac{\frac{1}{z^{2p}} + \dots}{\frac{l^2}{z^{2p-2}} + \dots} \quad \text{and} \quad \tilde{y}\big(x(z), y(z)\big) = \frac{-\frac{1}{z^{3p}} + \dots}{\frac{l^3}{z^{3p-3}} + \dots}$$

Hence the above mentioned constant equals 1 and equality (3.6) holds. This proves our claim.

Next we prove that the curve $E^{(p)}$ given by equation (3.6) and the morphism $F : E \to E^{(p)}$ given by

$$(x, y) \mapsto \big(\tilde{x}(x, y), \tilde{y}(x, y)\big)$$

are defined over R. Let $Q \in S$. Using the addition formulas (see [Sil86] Ch. III, §2) we compute

$$x(Q + P_1) = \frac{ab}{x(Q)}, \tag{3.7}$$

$$x(Q + P_2) = \frac{a(x(Q) - b)}{x(Q) - a}, \tag{3.8}$$

$$x(Q + P_3) = \frac{b(x(Q) - a)}{x(Q) - b}. \tag{3.9}$$

Note that a point $Q \in E(\bar{K})$ is in the kernel of reduction if and only if

$$v\big(x(Q)\big) < 0.$$

It follows by (3.7)-(3.9) that

$$v\big(x(Q+P_i)\big) \geq 0$$

for $Q \in S$ and $i = 1,2,3$. As a consequence we get $h(x), g_i(x) \in R[x]$, $i = 1,2,3$.

We claim that the isogeny F reduces to relative Frobenius. Note that

$$\tilde{x}(x,y) \equiv x^p \bmod p \quad \text{and} \quad \tilde{y}(x,y) \equiv y^p \bmod p \tag{3.10}$$

imply

$$a^{(p)} \equiv a^p \bmod p \quad \text{and} \quad b^{(p)} \equiv b^p \bmod p.$$

By (3.7) and $v\big(x(Q)\big) < 0$ we have $v(Q+P_1) > 0$ for $Q \in S$. It follows that

$$g_1(x)^2 \equiv x^{p-1} \bmod p.$$

Since for $Q \in S$ we have $v\big(x(Q)\big) < 0$ it follows by the definition of $h(x)$ that

$$h(x) \equiv 1 \bmod p.$$

We claim that

$$\prod_{i=1}^{3} \big(x - x(Q+P_i)\big) \equiv y^2 \bmod p. \tag{3.11}$$

Let $Q \in S$. By (3.7)-(3.9) and $v\big(x(Q)\big) < 0$ we have

$$\begin{aligned} x(Q+P_1) &\equiv 0 \bmod p, \\ x(Q+P_2) &= \frac{ax(Q)-ab}{x(Q)-a} = \frac{a - \frac{ab}{x(Q)}}{1 - \frac{a}{x(Q)}} \equiv a \bmod p \end{aligned}$$

and analogously

$$x(Q+P_3) \equiv b \bmod p.$$

This proves the congruence (3.11) and hence the congruences (3.10) hold. Thus our claim is proven. Beside that the above discussion shows that $a^{(p)}$ and $b^{(p)}$ are well-defined and $E^{(p)}$ is an elliptic curve.

Finally we claim that

$$F^*\left(\frac{dx}{y}\right) = \operatorname{lead}(h) \cdot \frac{dx}{y}.$$

We set

$$f(x) = \frac{h(x)g_1(x) + 2x\big(h(x)g_1'(x) - h'(x)g_1(x)\big)}{g_2(x)g_3(x)}.$$

One computes that

$$F^*\left(\frac{dx}{y}\right) = f(x) \cdot \frac{dx}{y}.$$

Since $\frac{dx}{y}$ defines a global regular differential the function $f(x)$ must be defined on all of E. This implies that $f(x)$ is constant. We have

$$f(0) = \frac{h(0)g_1(0)}{g_2(0)g_3(0)} = \frac{g_1(0)}{g_2(0)g_3(0)}.$$

Recall that $h(x)$ is normalized with respect to its constant term. The formulas (3.7)-(3.9) imply that

$$x(Q + P_1)x(Q) = x(Q + P_2)x(Q + P_3).$$

The claim now follows from the definition of $h(x)$ and $g_i(x)$, $i = 1, 2, 3$. This finishes the proof of Theorem 3.1.1.

Next we want to prove Remark 3.1.2. Assume that E has ordinary reduction. By Lemma 3.4.4 it follows that there are precisely p points of order p on E lying in the kernel of reduction. Let $0_E \neq P \in E[p](\bar{K})$ be in the kernel of reduction. Then the multiples of P are as well, since the reduction map is a homomorphism of groups. This proves the remark.

3.5.2 Proof of Theorem 3.2.1

We use the notation of Section 3.2. First we will prove the correctness of Algorithm 3.2.2 and after that we will analyze its complexity.

The p-th division polynomial $\psi_p(x)$ is computed in Step 1 with precision m. For a definition of $\psi_p(x)$ and its properties see Section 3.4. Since E has ordinary reduction, it follows by Lemma 3.4.4 that the polynomial $\psi_p(x)$ reduces modulo p to a polynomial of degree $p(p-1)/2$. By Hensel's Lemma one can find a decomposition

$$\psi_p(x) = U(x) \cdot V(x)$$

where $U(x), V(x) \in R/(p^m)[x]$ such that

$$\deg(U) = \frac{p(p-1)}{2}, \quad \deg(V) = \frac{p-1}{2}$$

and $V(x) \equiv 1 \bmod p$. The latter composition is computed in Step 2. The factor $V(x)$ corresponds to a subgroup $G \leq E[p](\bar{K})$ of order p contained in the kernel of reduction (compare Remark 3.1.2 and Lemma 3.4.4). One can apply Theorem 3.1.1 to G in order to compute the coefficients $a^{(p)}$ and $b^{(p)}$ of the curve $E^{(p)}$. This is done in Step 3. The polynomial $V(x)$ differs multiplicatively from $h(x)$ by a unit. Hence we have

$$\frac{V(b)}{V(a)} \equiv \frac{h(b)}{h(a)} \bmod p^m.$$

This proves the correctness of the Algorithm 3.2.2.

Next we provide some well-known results about the complexity of the arithmetic operations in the Witt vectors of a finite field. Elements of $R/(p^m)$ allocate

$$O\big(md\log_2(p)\big)$$

bits if one stores them as integers, where m and d are as in Theorem 3.2.1. For details see [FGH00] §2. Using fast integer multiplication techniques we conclude that a multiplication in $R/(p^m)$ has complexity

$$\tilde{O}\big(md\log_2(p)\big) \tag{3.12}$$

Inversion of $a \in R/(p^m)$ can be done using a simple Newton iteration with the polynomial $ax-1 \in R/(p^m)[x]$. The complexity of the Newton iteration is analyzed in [FGH00] §2.5. The resulting complexity for an inversion is equal to that of the multiplication. Representing elements of $R/(p^m)[x]$ as integers and using a fast arithmetic for integers the complexity of the multiplication of two polynomials of degree n becomes

$$\tilde{O}\big(nmd\log_2(p)\big).$$

In order to prove the complexity bound of Theorem 3.2.1 we will analyze step-by-step the relevant parts of Algorithm 3.2.2.

Step 1: For the computation of the division polynomial ψ_p we use the formulas of Section 3.4. Note that for every $m \geq 5$ the polynomial ψ_m can be computed in terms of polynomials forming a subset of the set

$$\{\psi_{n+2}, \dots, \psi_{n-2}\}, \tag{3.13}$$

where $n = \lfloor m/2 \rfloor$. This shows that a recursive algorithm for computing ψ_p has depth $\lfloor \log_2(p) \rfloor$. The necessary multiplications of polynomials to compute ψ_m in terms of the polynomials (3.13) can be performed in

$$\tilde{O}\big(n^2 md\log_2(p)\big)$$

bit operations, since ψ_n has degree $(n^2-1)/2$. Let $s_1 = \lfloor p/2 \rfloor + 2$ and $t_1 = \lfloor p/2 \rfloor - 2$. For $i \geq 1$ we have to compute the polynomials

$$\psi_{s_i}, \ldots, \psi_{t_i}$$

where

$$s_i = \lfloor \frac{s_{i-1}}{2} \rfloor + 2 \quad \text{and} \quad t_i = \lfloor \frac{t_{i-1}}{2} \rfloor - 2$$

for $i > 1$. By induction on i one can prove that

$$s_i \leq \lfloor \frac{p}{2^i} \rfloor + (i-1) + 2 \quad \text{and} \quad t_i \geq \lfloor \frac{p}{2^i} \rfloor - (i-1) - 2.$$

It follows that the number of polynomials to be computed on each recursion level grows linearly in the index i. Since $i \leq \lfloor \log_2(p) \rfloor$ we conclude that the p-th division polynomial ψ_p can be computed in

$$\tilde{O}\big(p^2md\big)$$

bit operations.

Step 2: Using the standard Hensel algorithm (see [Coh93] Section 3.5.3) we get for Step (2) the complexity

$$\tilde{O}(p^2md). \tag{3.14}$$

Note that Hensel's algorithm converges quadratically. We assume that one uses in each iteration the minimal precision required in order to get the correct result.

Step 3: Evaluating a polynomial in $R/(p^m)[x]$ of degree $(p-1)/2$ at a value in $R/(p^m)$ has complexity

$$\tilde{O}(pmd).$$

To achieve this complexity one uses a squaring table and a 2-adic representation of exponents. We do not describe this method in detail because it is standard.

Summing up the above complexities we get the complexity bound as stated in Theorem 3.2.1.

3.5.3 Proof of Theorem 3.3.1

In this section we prove Theorem 3.3.1. First we prove the correctness of Algorithm 3.3.2. Following up is a study of its complexity. The key ingredient in the proof of correctness is the Convergence Theorem for the GAGM sequence (see Corollary 2.1.4).

We use the notation of Section 3.3. Let d and m be as in Step 1. Note that by Corollary 2.1.5 the curve $E^{(p^{m-1})}$ computed in Step 3 is the canonical lift over $R/(p^m)$ of its reduction. The latter is also true for the curve $E^{(p^{m+d-1})}$, which is computed in Step 4. The reductions of $E^{(p^{m-1})}$ and $E^{(p^{m+d-1})}$ coincide. As a consequence there exists a unique isomorphism

$$\varphi : E^{(p^{m+d-1})} \xrightarrow{\sim} E^{(p^{m-1})}$$

defined over $R/(p^m)$ such that the composed map

$$\Phi = \varphi \circ F^d \in \mathrm{End}_{R/(p^m)}\big(E^{(p^{m-1})}\big)$$

reduces to the absolute Frobenius of the reduction $\bar{E}^{(p^{m-1})}$. The map

$$\mathrm{End}_{R/(p^m)}\big(E^{(p^{m-1})}\big) \to \mathrm{End}_{\mathbb{F}_q}\big(\bar{E}^{(p^{m-1})}\big) \tag{3.15}$$

induced by reduction is bijective by Lemma 2.4.11. Let $V = \hat{\Phi}$ be the dual isogeny of Φ. The isogeny V lifts the Verschiebung on $\bar{E}^{(p^{m-1})}$. By the injectivity of (3.15) the equality

$$V^2 - [t] \circ V + [q] = 0 \tag{3.16}$$

holds in

$$\mathrm{End}_{R/(p^m)}\big(E^{(p^{m-1})}\big),$$

where t denotes the trace of the absolute q-Frobenius on $\bar{E}^{(p^{m-1})}$. As a consequence of equation (3.16) we get

$$\big(V^2 - [t] \circ V + [q]\big)^* \left(\frac{dx}{y}\right) = 0. \tag{3.17}$$

We define $v \in R/(p^m)$ by

$$V^* \left(\frac{dx}{y}\right) = v \cdot \frac{dx}{y}.$$

Note that the Verschiebung is a separable isogeny acting as a non-zero scalar on the differentials of $\bar{E}^{(p^{m-1})}$ over $\mathbb{F}_q$. This shows that v is invertible modulo

p^{m-1}. We remark that the scalar describing the action of F on differentials is divisible by p. This is the reason why we work with the isogeny V instead of the isogeny Φ. We conclude from (3.17) that

$$t \equiv v + \frac{q}{v} \bmod p^{m-1}. \tag{3.18}$$

The number of $\mathbb{F}_q$-rational points on $\bar{E}$ equals that of $\bar{E}^{(p^{m-1})}$ since they are isogenous over $\mathbb{F}_q$. This shows that the above number t is in fact the trace of the absolute Frobenius on $\bar{E}$.

In the following we want to describe the relevant steps of Algorithm 3.3.2 in more detail. In particular we give their complexity.

Step 1: In order to turn the congruence (3.18) into an equality, which holds in $\mathbb{Z}$, we have to choose the right precision. Also one carefully has to choose a representative of its congruence class (compare Step 5). Hasse's Theorem (see [Sil86] Ch. V, Theorem 1.1) states that

$$|t| \leq 2\sqrt{q}.$$

One estimates

$$t \leq 2\sqrt{q} < p\sqrt{q} \leq p^{m-1}$$

for $m \geq \lfloor d/2 \rfloor + 3$. It will be explained in Step 4 why we actually compute with precision m instead of precision $(m-1)$.

Step 3: One has to iterate $(m-1)$-times Algorithm 3.2.2 with precision m. The resulting complexity of Step 3 is $\tilde{O}(p^2 d^3)$ by Theorem 3.2.1.

Step 4: The modified version of Algorithm 3.2.2 has complexity $\tilde{O}(p^2 d^2)$. The number c is the scalar describing the action of the dual of F on differentials. Using the notation of Theorem 3.1.1 and Algorithm 3.2.2 we have

$$\text{lead}(h) = \frac{\text{lead}(V)}{V(0)}.$$

In order to be able to divide by p without losing precision, one has to compute the GAGM sequence with precision m. As in Step 3 the overall complexity of Step 4 is $\tilde{O}(p^2 d^3)$.

Step 5: In order to get the scalar v (see above) describing the action of

V on differentials, one has to compute the action of φ on differentials. The isomorphism φ is of the form

$$(x,y) \mapsto \left(u^2x + s, u^3y\right)$$

for $u \in R/(p^{m-1})^*$ and $s \in R/(p^{m-1})$. In addition we know that φ reduces to the identity and hence $u \equiv 1 \bmod p$. Pulling back by φ equals multiplication by $1/u$ on differentials. Let e be as in Step 4 and v as above. The relation between e, u and v is given by

$$v = u \cdot e,$$

because

$$[q] = V \circ \Phi$$

with Φ as above.

In the following we will explain how to compute the scalar u. If $j(\bar{E}) \neq 0$ then

$$j(\bar{E}^{(p^{m+d-1})}) \neq 0.$$

As a consequence

$$j(E^{(p^{m+d-1})}) \in R^* \quad \text{and hence} \quad c_4(E^{(p^{m+d-1})}) \in R^*.$$

There is a relation of modular forms

$$u^4 \cdot c_4\left(E^{(p^{m+d-1})}\right) \equiv c_4\left(E^{(p^{m-1})}\right) \bmod p^{m-1}. \tag{3.19}$$

Expressing congruence (3.19) in terms of coefficients of the defining equations yields the congruence

$$u^4 \equiv \frac{a_{m-1}^2 - a_{m-1}b_{m-1} + b_{m-1}^2}{a_{m+d-1}^2 - a_{m+d-1}b_{m+d-1} + b_{m+d-1}^2} \bmod p^m. \tag{3.20}$$

One can find the correct value for u by reducing the congruence (3.20) modulo p and using Newton iteration with initial condition $u \equiv 1 \bmod p$.

Note that if $p = 3$ then $j(\bar{E}) \neq 0$ since $\bar{E}$ is ordinary. Let now $p > 3$ and $j(\bar{E}) = 0$. By the latter assumption we have

$$j(\bar{E}^{(p^{m+d-1})}) = 0.$$

It follows that

$$c_4(\bar{E}^{(p^{m+d-1})}) = 0 \quad \text{and} \quad c_6(\bar{E}^{(p^{m+d-1})}) \neq 0.$$

This implies that

$$c_6(E^{(p^{m+d-1})}) \in R^*.$$

We can use the relation of modular forms

$$u^6 \cdot c_6\left(E^{(p^{m+d-1})}\right) \equiv c_6\left(E^{(p^{m-1})}\right) \bmod p^{m-1}$$

in order to find u. Computing both sides in terms of coefficients yields

$$u^6 \equiv \frac{2a_{m-1}^3 - 3a_{m-1}^2 b_{m-1} - 3a_{m-1}b_{m-1}^2 + 2b_{m-1}^3}{2a_{m+d-1}^3 - 3a_{m+d-1}^2 b_{m+d-1} - 3a_{m+d-1}b_{m+d-1}^2 + 2b_{m+d-1}^3}$$

modulo p^{m-1}. Using this congruence and the condition $u \equiv 1 \bmod p$ one can compute u modulo p^{m-1} using Newton iteration.

Finally note that if $d > 2$ then $m - 1 \leq d$ and hence the congruence (3.18) becomes

$$t \equiv v \bmod p^{m-1}.$$

Perspectives

The algorithms presented in Section 3.2 and Section 3.3 may be improved with respect to their complexity. This improvement might be relevant in practice.

The complexity bound given in Theorem 3.2.1 may be improved to a bound that is linear in p (for notation see Section 3.2). In order to do so, one has to avoid computing with the p-th division polynomial, which has degree of order p^2. Perhaps it is possible to use the formal group law of the elliptic curve E instead. We remark that the formal group incorporates the local part of the p-torsion, or equivalently, the kernel of reduction.

Also it is worthwhile trying to improve the complexity bound of Theorem 3.3.1 with respect to d. One expects that there is an algorithm whose complexity is essentially quadratic in d. In order to improve the complexity bound with respect to d, one may consider a fusion of Algorithm 3.2.2 with the iterative computation of the GAGM sequence in Step 3 of Algorithm 3.3.2. Also one has to replace Step 4 in the latter algorithm by a norm computation similar to the one described in [Ver03] Ch.3, Sections 3.6.2, 3.7.2 and 3.10.3.

The author has not implemented any of the algorithms presented in this article. It is desirable to see their behavior in practice in order to compare them to the algorithms of K. Kedlaya [Ked01], D. Kohel [Koh03] and T. Satoh [Sat02] which belong to the same class of methods for point counting, the so-called p-adic methods.

The author believes that Algorithm 3.3.2 is in fact practical. Spending some effort on optimization one should be able to make it into a fast alternative to existing methods, i.e. Satoh's and Kedlaya's method, for primes ≤ 100.

Bibliography

[Cas66] John William Scott Cassels. Diophantine equations with special reference to elliptic curves. *Journal of the London Mathematical Society*, 41:193–291, 1966.

[Coh93] Henry Cohen. *A course in computational algebraic number theory.* Number 138 in Graduate Texts in Mathematics. Springer-Verlag, 1993.

[FGH00] Mireille Fouquet, Pierrick Gaudry, and Robert Harley. An extension of Satoh's algorithm and its implementation. *Journal of the Ramanujan Mathematical Society*, 15(4):281–318, 2000.

[Ked01] Kiran Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *Journal of the Ramanujan Mathematical Society*, 16(4):323–338, 2001.

[Koh03] David Kohel. The AGM-$X_0(N)$ Heegner point lifting algorithm and elliptic curve point counting. In *Proceedings of ASIACRYPT'03*, number 2894 in Lecture Notes in Computer Science, pages 124–136. Springer-Verlag, 2003.

[Lan78] Serge Lang. *Elliptic curves: Diophantine analysis.* Number 231 in Grundlehren der mathematischen Wissenschaften. Springer-Verlag, 1978.

[Sat02] Takakazu Satoh. On p-adic point-counting algorithms for elliptic curves over finite fields. In Claus Fieker and David Kohel, editors, *Proceedings Algorithmic Number Theory Symposium ANTS-V*, number 2369 in Lecture Notes in Computer Science, pages 43–66, 2002.

[Sil86] Joseph H. Silverman. *The arithmetic of elliptic curves.* Number 106 in Graduate Texts in Mathematics. Springer-Verlag, 1986.

[Vel71] Jacques Velu. Isogénies entre courbes elliptiques. *Comptes Rendus de l'Académie des Sciences Paris, Série A*, 273:238–241, 1971.

[Ver03] Frederik Vercauteren. *Computing zeta functions of curves over finite fields.* PhD thesis, Katholieke Universiteit Leuven, Belgium, 2003.

Chapter 4

A theta structure induced by a lift of relative Frobenius

The main result of the present chapter is given by Theorem 4.1.1 which states the existence of a certain theta structure induced by the relative Frobenius. We remark that a theta structure for an abelian scheme with a given relatively ample line bundle induces a projective embedding of the abelian scheme. Thus Theorem 4.1.1 is an important step towards explicit coordinates for the GAGM sequence in higher dimensions (compare Section 1.3).

Structure of Chapter 4:	
Section 4.1:	We state our main theorem about the existence of a certain theta structure induced by a lift of the relative Frobenius.
Section 4.2:	Some general remarks are made about the notation that we will use in this chapter.
Section 4.3:	We provide some facts about theta groups and theta structures that we will need later on.
Section 4.4:	We state two theorems about the descent of line bundles along lifts of the relative Frobenius and the Verschiebung which are used in the proof of Theorem 4.1.1.
Section 4.5:	We give proofs of the statements made in the preceding sections.
Acknowledgments	
Bibliography	

4.1 The main result

Let R be a complete noetherian local ring with perfect residue class field k of characteristic $p > 0$ and A an abelian scheme over R of relative dimension g having ordinary reduction. Let $\mathcal{L}$ be an ample line bundle of degree 1 on A.

The following is a short exposition of some facts that will be discussed in detail in Section 4.4. There exists an isogeny of abelian schemes $F : A \rightarrow A^{(p)}$, which is uniquely determined up to isomorphism by the condition that it lifts the relative p-Frobenius on the special fiber. Also there exists an ample line bundle $\mathcal{L}^{(p)}$ of degree 1 on $A^{(p)}$ such that $F^*\mathcal{L}^{(p)} \cong \mathcal{L}^{\otimes p}$. It is uniquely determined up to isomorphism by the condition that $\left(\mathcal{L}^{(p)}\right)_k \cong \mathrm{pr}^*\mathcal{L}_k$, where $\mathrm{pr} : A_k^{(p)} \rightarrow A_k$ is an isomorphism making the diagram

$$\begin{tikzcd}
A_k^{(p)} \arrow[r, "\mathrm{pr}"] \arrow[d] & A_k \arrow[d] \\
\mathrm{Spec}(k) \arrow[r, "f_p"] & \mathrm{Spec}(k)
\end{tikzcd}$$

cartesian. Here f_p denotes the morphism induced by the absolute p-Frobenius of the field k and the vertical arrows are the structure morphisms. Assume that we have an isomorphism

$$(\mathbb{Z}/p\mathbb{Z})_k^g \xrightarrow{\sim} A_k[p]^{\mathrm{et}} \tag{4.1}$$

where $A_k[p]^{\mathrm{et}}$ denotes the maximal étale quotient of $A_k[p]$ (compare Section 2.9). The following is the main result of the present chapter.

Theorem 4.1.1 *Suppose $p > 2$. Then there exists a natural theta structure of type $(\mathbb{Z}/p\mathbb{Z})_R^g$ for the pair*

$$\left(A^{(p)}, \left(\mathcal{L}^{(p)}\right)^{\otimes p}\right)$$

depending on the isomorphism (4.1).

For a definition of a theta structure we refer to Section 4.3.3.

Corollary 4.1.2 *Let k be a finite field of characteristic $p > 2$. Assume that A is the canonical lift of A_k. Then there exists a natural theta structure of type $(\mathbb{Z}/p\mathbb{Z})_R^g$ for the pair*

$$\left(A, \mathcal{L}^{\otimes p}\right)$$

depending on the isomorphism (4.1).

Theorem 4.1.1 and Corollary 4.1.2 will be proven in Section 4.5.3.

4.2 Notation

Let R be a ring, X an R-scheme and S an R-algebra. By X_S we denote the base extended scheme $X \times_R \operatorname{Spec}(S)$. Let $\mathcal{M}$ be a sheaf on X. Then we denote by $\mathcal{M}_S$ the sheaf that one gets by pulling back via the projection $X_S \to X$. Let $I : X \to Y$ be a morphism of R-schemes. Then I_S denotes the morphism that is induced by I via base extension with S. We use the same symbol for a scheme and the fppf-sheaf represented by it. By a *group* we mean a group object in the category of fppf-sheaves. If a representing object has the property of being finite (resp. flat, étale, connected, etc.) then we simply say that it is a finite (resp. flat, étale, connected, etc.) group. Similarly we will say that a morphism of groups is finite (resp. faithfully flat, smooth, etc.) if the groups are representable and the induced morphism of schemes has the corresponding property.

A group resp. a morphism of groups is called finite locally free if it is finite flat and of finite presentation. The Cartier dual of a finite locally free commutative group G will be denoted by G^D. The multiplication by an integer $n \in \mathbb{Z}$ on G will be denoted by $[n]_G$ or simply $[n]$. A finite locally free and surjective morphism between groups is called an *isogeny.* By an *elliptic curve* we mean an abelian scheme of relative dimension 1. We use the notion of a *torsor* in the sense of [DG70] Ch. III, §4, Def. 1.3. We only consider torsors for the fppf-topology.

4.3 Theta groups

In the following section we recall some well-known facts about theta groups. We refer to [Mum66], [Mum70] Ch. IV, §23 and [MB85] Ch. V for more details. Let R be a ring and G a group over R.

Definition 4.3.1 *Assume that there exists a central exact sequence of groups*

$$0 \to \mathbb{G}_{m,R} \to G \xrightarrow{\pi} H \to 0,$$

where H is a commutative finite locally free group whose rank is the square of an integer. Then the group G is called a theta group *over H.*

By the term *central exact sequence* we mean that $\mathbb{G}_{m,R}$ is mapped into the center of G. Now let G be a theta group over H. By definition G is a $\mathbb{G}_{m,R}$-torsor over H. It follows by descent that the group G is representable by an affine faithfully flat group scheme of finite presentation over H (compare

[DG70] Ch. III, §4, Prop. 1.9). Let S be an R-algebra. One defines the *commutator pairing*

$$e : H \times_R H \to \mathbb{G}_{m,R}$$

by lifting x resp. y in $H(S)$ to $\tilde{x}$ resp. $\tilde{y}$ in $G(S')$, where $S \to S'$ is an fppf-extension, and by setting

$$e(x,y) = \tilde{x}\tilde{y}\tilde{x}^{-1}\tilde{y}^{-1}.$$

Because H is abelian, we have $e(x,y) \in \mathbb{G}_{m,R}(S')$. Since $e(x,y)$ does not depend on the choice of $\tilde{x}$ and $\tilde{y}$, it follows by descent that $e(x,y) \in \mathbb{G}_{m,R}(S)$.

4.3.1 The theta group of an ample line bundle

Next we give a first example of a theta group. Let A be an abelian scheme over a ring R and $\mathcal{L}$ a line bundle on A. One defines a morphism

$$\varphi_{\mathcal{L}} : A \to \check{A} = \mathrm{Pic}^0_{A/R}$$

by setting

$$x \mapsto \langle T_x^* \mathcal{L} \otimes \mathcal{L}^{-1} \rangle.$$

The group $\mathrm{Pic}^0_{A/R}$ is representable by an abelian scheme. This follows from the fact that the categories of abelian algebraic spaces and abelian schemes coincide (see [FC90] Ch. I, Theorem 1.9) and $\mathrm{Pic}^0_{A/R}$ is representable by an abelian algebraic space (compare [BLR90] Ch. 8, Theorem 1). We denote the kernel of the morphism $\varphi_{\mathcal{L}}$ by $H(\mathcal{L})$. A line bundle $\mathcal{L}$ on A satisfies $H(\mathcal{L}) = A$ if and only if its class is in $\mathrm{Pic}^0_{A/R}(R)$. Also it is well-known that if $\mathcal{L}$ is relatively ample then $\varphi_{\mathcal{L}}$ is an isogeny. In the latter case we say that $\mathcal{L}$ has degree d if $\varphi_{\mathcal{L}}$ is fiber-wise of degree d. Let S be an R-algebra. We define

$$G(\mathcal{L})(S) = \left\{ \ (x, \varphi) \mid x \in H(\mathcal{L})(S), \ \ \varphi : \mathcal{L}_S \xrightarrow{\sim} T_x^* \mathcal{L}_S \ \right\}.$$

This functor is a group with respect to the group law

$$\big((y,\psi),(x,\varphi)\big) \mapsto (x+y, T_x^*(\psi) \circ \varphi).$$

There is a natural morphism $\pi : G(\mathcal{L}) \to H(\mathcal{L})$ given by $(x,\varphi) \mapsto x$. We get a central exact sequence of fppf-sheaves

$$0 \to \mathbb{G}_{m,R} \to G(\mathcal{L}) \xrightarrow{\pi} H(\mathcal{L}) \to 0. \tag{4.2}$$

Now let $\mathcal{L}$ be relatively ample of degree d. Then $H(\mathcal{L})$ is finite locally free of order d^2 and hence $G(\mathcal{L})$ is a theta group. The commutator pairing on $H(\mathcal{L})$ as defined above will be denoted by $e_{\mathcal{L}}$. One can show that the pairing $e_{\mathcal{L}}$ is perfect, which is equivalent to the fact that the center of $G(\mathcal{L})$ equals $\mathbb{G}_{m,R}$.

4.3.2 Descent of line bundles along isogenies

Let R be a ring. Let $I : A \to B$ be an isogeny of abelian schemes over R and K its kernel. Assume we are given a relatively ample line bundle $\mathcal{L}$ on A and $K \subseteq H(\mathcal{L})$. Define G' by the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{G}_{m,R} \arrow[r] & G(\mathcal{L}) \arrow[r] & H(\mathcal{L}) \arrow[r] & 0 \\
0 \arrow[r] & \mathbb{G}_{m,R} \arrow[r] \arrow[u, "\mathrm{id}"] & G' \arrow[r, "\pi"] \arrow[u] & K \arrow[r] \arrow[u, hook, "i"'] & 0,
\end{tikzcd} \tag{4.3}$$

where the second row is the pull back of the first via the inclusion $K \overset{i}{\hookrightarrow} H(\mathcal{L})$, i.e. the right hand square is Cartesian. Let S be an R-algebra and $\mathcal{M}$ a line bundle on B_S. Suppose we are given an isomorphism $\alpha : I_S^*\mathcal{M} \xrightarrow{\sim} \mathcal{L}_S$. We define a morphism $s_\alpha : K_S \to G'_S$ by mapping $x \in K(S')$, where S' is an S-algebra, to

$$\big(x, T_x^*(\alpha_{S'}) \circ \alpha_{S'}^{-1}\big).$$

This is well-defined because $T_x^*(I_{S'}^*\mathcal{M}_{S'}) = I_{S'}^*\mathcal{M}_{S'}$. It is clear that $\pi_S \circ s_\alpha = \mathrm{id}$, where π is as in diagram (4.3). We define

$$\underline{\mathrm{Sect}}_K(S) = \{\ s : K_S \to G'_S \ \mid\ \pi_S \circ s = \mathrm{id}\ \}$$

and denote by

$$\underline{\mathrm{Desc}}(\mathcal{L})(S)$$

the set of isomorphism classes of line bundles $\mathcal{M}$ on B_S such that $I_S^*\mathcal{M} \cong \mathcal{L}_S$. The following classical result about descent was proven by A. Grothendieck.

Proposition 4.3.2 *Mapping*

$$(\mathcal{M}, \alpha) \mapsto s_\alpha$$

gives an isomorphism of functors

$$\underline{\mathrm{Desc}}(\mathcal{L}) \to \underline{\mathrm{Sect}}_K.$$

Compare [Mum70] Ch. IV, §23, Theorem 2 or [BLR90] Ch. 6.1, Theorem 4.

4.3.3 Theta structures

In the following we define the standard theta group of a given type. Let K be an a commutative finite locally free group of square order over a base ring R. We set

$$H(K) = K \times_R K^D, \quad G(K) = \mathbb{G}_{m,R} \times_R H(K),$$

and define a group law for $G(K)$ by

$$(\alpha_1, x_1, l_1) * (\alpha_2, x_2, l_2) = (\alpha_1 \cdot \alpha_2 \cdot l_2(x_1), x_1 + x_2, l_1 \cdot l_2).$$

We have an exact sequence of groups

$$0 \to \mathbb{G}_{m,R} \to G(K) \to H(K) \to 0,$$

where the right hand map is the natural projection on $H(K)$. The center of G_K is given by $\mathbb{G}_{m,R}$. Hence $G(K)$ is a theta group. We denote the corresponding commutator pairing by $e(K)$. Using the definition of the multiplication in $G(K)$ one computes

$$e(K)\big((x_1, l_1), (x_2, l_2)\big) = \frac{l_2(x_1)}{l_1(x_2)}. \tag{4.4}$$

We remark that $e(K)$ is a perfect pairing. Now assume we are given an abelian scheme A over R and a relatively ample line bundle $\mathcal{L}$ on A.

Definition 4.3.3 *A* theta structure *of type K for the pair $(A, \mathcal{L})$ is an isomorphism $\theta : G(K) \xrightarrow{\sim} G(\mathcal{L})$ making the diagram*

$$\begin{tikzcd}
\mathbb{G}_{m,S} \arrow[r] & G(\mathcal{L}) \\
\mathbb{G}_{m,S} \arrow[r] \arrow[u, "\mathrm{id}"] & G(K) \arrow[u, "\theta"]
\end{tikzcd}$$

commutative. Here the horizontal arrows are the natural inclusions.

Next we want to give another characterization of a theta structure.

Definition 4.3.4 *A* Lagrangian decomposition *for $H(\mathcal{L})$ of type K is an isomorphism*

$$\delta : H(K) \xrightarrow{\sim} H(\mathcal{L}),$$

which is compatible with the commutator pairings $e_{\mathcal{L}}$ resp. $e(K)$ on $H(\mathcal{L})$ resp. $H(K)$.

Let δ be a Lagrangian decomposition for $H(\mathcal{L})$ of type K. We can consider K and K^D as subgroups of $H(\mathcal{L})$ via δ. Assume we are given a pair (u, v) where u resp. v is a section of the pullback of the extension

$$0 \to \mathbb{G}_{m,R} \to G(\mathcal{L}) \xrightarrow{\pi} H(\mathcal{L}) \to 0 \tag{4.5}$$

via the inclusion $K \hookrightarrow H(\mathcal{L})$ resp. $K^D \hookrightarrow H(\mathcal{L})$. We define a morphism $\theta_{u,v} : G(K) \to G(\mathcal{L})$ by

$$\theta_{u,v}(\alpha, x, l) = \alpha \cdot v(l) \cdot u(x).$$

Proposition 4.3.5 *The map*

$$(\delta, u, v) \mapsto \theta_{u,v} \tag{4.6}$$

gives a bijection between the set of triples as above and the set of theta structures for $(A, \mathcal{L})$ of type K.

Proof. First we have to show that the map (4.6) is well-defined. We claim that $\theta_{u,v}$ is a theta structure of type K for $(A, \mathcal{L})$. We have

$$\begin{aligned}&\theta_{u,v}\big((\alpha_1, x_1, l_1) * (\alpha_2, x_2, l_2)\big)\\ &\qquad = \alpha_1 \cdot \alpha_2 \cdot l_2(x_1) \cdot v(l_1) \cdot v(l_2) \cdot u(x_1) \cdot u(x_2).\end{aligned}$$

By the definition of the pairing $e_{\mathcal{L}}$ we have

$$v(l_2) \cdot u(x_1) = e_{\mathcal{L}}\big(\delta(l_2), \delta(x_1)\big) \cdot u(x_1) \cdot v(l_2).$$

Since δ is a Lagrangian decomposition we have

$$e_{\mathcal{L}}\big(\delta(l_2), \delta(x_1)\big) = e(K)\big((0, l_2), (x_1, 1)\big) = \frac{1}{l_2(x_1)}.$$

The right hand equality follows by (4.4). This proves that $\theta_{u,v}$ is a morphism of groups. Clearly $\theta_{u,v}$ is $\mathbb{G}_{m,R}$-equivariant.

Next we prove that $\theta_{u,v}$ is an isomorphism by giving an inverse. Let g be a point of $G(\mathcal{L})$. Then $\pi(g) = \delta(x_g, l_g)$ for uniquely determined x_g in K and l_g in K^D. Here π is the projection map of the extension (4.5). Now g and $\theta_{u,v}(1, x_g, l_g)$ both lift $\delta(x_g, l_g)$. Hence those two differ by a unique scalar α_g, i.e.

$$g = \alpha_g \cdot \theta_{u,v}(1, x_g, l_g) = (\alpha_g, x_g, l_g).$$

Hence an inverse of $\theta_{u,v}$ is given by the morphism defined by

$$g \mapsto (\alpha_g, x_g, l_g).$$

In order to prove Proposition 4.3.5 it is sufficient to give an inverse of the map (4.6). Assume we are given a theta structure θ of type K for the pair $(A, \mathcal{L})$. The isomorphism θ induces an isomorphism $\delta(\theta) : H(K) \overset{\sim}{\to} H(\mathcal{L})$. By the definition of the commutator pairing it follows that the isomorphism $\delta(\theta)$ is a Lagrangian decomposition. There are two natural sections of the natural projection $G(\mathcal{L}) \to H(\mathcal{L})$ over K resp. K^D given by

$$u(\theta) : (x, 1) \mapsto \theta\big(1, x, 1\big) \quad \text{and} \quad v(\theta) : (0, l) \mapsto \theta\big(1, 0, l\big).$$

Here we consider K and K^D as subgroups of $H(\mathcal{L})$ via $\delta(\theta)$. An inverse of (4.6) is given by

$$\theta \mapsto \big(\delta(\theta), u(\theta), v(\theta)\big).$$

This finishes the proof of the proposition. □

4.4 Descent along lifts of relative Frobenius and Verschiebung

In the following we repeat some facts about the existence of Frobenius lifts and the descent of line bundles along lifts of Frobenius and Verschiebung. Theorem 4.4.1 and 4.4.2 are known to the experts but they are not yet available in the literature. We prove them in Section 4.5.1 and 4.5.2.

Let R be a complete noetherian local ring with perfect residue class field k of characteristic $p > 0$ and A an abelian scheme having ordinary reduction. By Proposition 2.1.1 there exists an abelian scheme $A^{(p)}$ over R and a commutative diagram of isogenies

$$\begin{tikzcd} A \arrow[r, "F"] \arrow[d, "{[p]}"'] & A^{(p)} \arrow[dl, "V"] \\ A & \end{tikzcd} \qquad (4.7)$$

such that F_k equals relative Frobenius. The latter condition determines F uniquely. The kernel of F is given by $A[p]^{\mathrm{loc}}$. The condition that F_k equals relative Frobenius means that there exists a commutative diagram

$$\begin{tikzcd}
A_k \arrow[dr, "F_k"] \arrow[drr, bend left, "f_p"] \arrow[ddr, bend right] & & \\
& A_k^{(p)} \arrow[r, "\mathrm{pr}"] \arrow[d] & A_k \arrow[d] \\
& \mathrm{Spec}(k) \arrow[r, "f_p"] & \mathrm{Spec}(k)
\end{tikzcd}$$

where f_p denotes the absolute p-Frobenius, the vertical maps are the structure maps and the square is Cartesian. Let $\mathcal{L}$ be a line bundle on A. We have a natural isomorphism

$$F_k^*(\mathrm{pr}^*\mathcal{L}_k) = f_p^*\mathcal{L}_k \xrightarrow{\sim} \mathcal{L}_k^{\otimes p} \tag{4.8}$$

given by $l \otimes 1 \mapsto l^{\otimes p}$.

Theorem 4.4.1 *Let $\mathcal{L}$ be ample. There exists a line bundle $\mathcal{L}^{(p)}$ on $A^{(p)}$ determined uniquely up to isomorphism by the following two conditions:*

1. $\left(\mathcal{L}^{(p)}\right)_k \cong \mathrm{pr}^*\mathcal{L}_k$,
2. $F^*\mathcal{L}^{(p)} \cong \mathcal{L}^{\otimes p}$.

Moreover, the line bundle $\mathcal{L}^{(p)}$ is ample and has the same degree as $\mathcal{L}$.

A proof of Theorem 4.4.1 is presented in Section 4.5.1. We set $\mathcal{L}_\alpha = \mathcal{L}^{\otimes\alpha}$ for $\alpha = 1, 2$.

Theorem 4.4.2 *If $\mathcal{L}$ is ample and symmetric then there exists an isomorphism*

$$V^*\mathcal{L}_\alpha \xrightarrow{\sim} \left((\mathcal{L}_\alpha)^{(p)}\right)^{\otimes p} \tag{4.9}$$

for

$$\alpha = \begin{cases} 2 & \text{if } p = 2, \\ 1 & \text{if } p > 2. \end{cases}$$

For $p = 2$ and $\alpha = 1$ the isomorphism (4.9) does not always exist. We illustrate this by a counterexample for the case of elliptic curves in Section 4.5.2. A proof of Theorem 4.4.2 will be given in Section 4.5.2.

4.5 The proofs

In this section we prove the statements of Section 4.1 and 4.4.

4.5.1 Proof of Theorem 4.4.1

In the following we prove Theorem 4.4.1. We use the notation of Section 4.4. Let A be an abelian scheme over R having ordinary reduction and $\mathcal{L}$ an ample line bundle on A. Let $K = A[p]^{\mathrm{loc}}$ and let G' be defined by the Cartesian diagram

$$\begin{tikzcd}
G(\mathcal{L}^{\otimes p}) \arrow[r] & H(\mathcal{L}^{\otimes p}) \\
G' \arrow[r] \arrow[u] & K. \arrow[u]
\end{tikzcd}$$

Remark 4.5.1 *The group G' is commutative.*

Proof. The commutativity of G' is equivalent to the condition that the commutator pairing $e : A[p] \times A[p] \to \mathbb{G}_m$ is trivial on K. Let T be an R-algebra and $x \in K(T)$. Then the map $e(x, \cdot) : K_T \to \mathbb{G}_{m,T}$ is a T-valued point of $K^D \cong \check{A}[p]^{\mathrm{et}}$ where $\check{A}$ denotes the dual abelian scheme. The map $K \to \check{A}[p]^{\mathrm{et}}$ given by $x \mapsto e(x, \cdot)$ is equal to zero since the image of K is connected and hence equals the image of the unit section in $\check{A}[p]^{\mathrm{et}}$ which forms a connected component. □

The main ingredient in the proof of Theorem 4.4.1 is the following result.

Lemma 4.5.2 *The functor $\underline{\mathrm{Sect}}_K$ is a K^D-torsor over R.*

For the definition of $\underline{\mathrm{Sect}}_K$ see Section 4.3.2.

Proof. Clearly the functor $\underline{\mathrm{Hom}}(K, \mathbb{G}_m)$ acts transitively and faithfully on $\underline{\mathrm{Sect}}_K$. Consider the extension

$$0 \to \mathbb{G}_{m,R} \to G' \to K \to 0. \tag{4.10}$$

We will show that this extension has a section over an fppf-extension of R. The exact sequence (4.10) induces an exact sequence

$$0 \to \mu_p \to G'[p] \to K \to 0. \tag{4.11}$$

This follows from the Snake Lemma and the exactness of the Kummer sequence. By Remark 4.5.1 the group $G'[p]$ is commutative. Hence we can apply Cartier duality. Dualizing the exact sequence (4.11) we get an exact sequence

$$0 \to K^D \to G'[p]^D \xrightarrow{\pi} \mathbb{Z}/p\mathbb{Z} \to 0. \tag{4.12}$$

The group $G'[p]^D$ is a K^D-torsor over $\mathbb{Z}/p\mathbb{Z}$ via π. By descent (see [DG70] Ch. III, §4, Prop. 1.9) we conclude that $G'[p]^D$ is finite locally free and hence has a point of order p over an fppf-extension $R \to R'$. As a consequence (4.10)–(4.12) have a splitting over R'. □

Corollary 4.5.3 *The functor* $\underline{\mathrm{Sect}}_K$ *is representable by a finite étale scheme.*

Proof. The representability by a finite locally free R-scheme follows from Lemma 4.5.2 and [DG70] Ch. III, §4, Prop. 1.9. Since A has ordinary reduction, we have $\underline{\mathrm{Hom}}_R(K, \mathbb{G}_m) \cong \check{A}[p]^{\mathrm{et}}$ where $\check{A}$ denotes the dual of A (compare Lemma 2.4.5). It follows by descent that $\underline{\mathrm{Sect}}_K$ is étale. □

Now we can complete the proof of Theorem 4.4.1. We have already seen that there exists a k-rational point x of $\underline{\mathrm{Sect}}_K$ given by the isomorphism (4.8). By Corollary 4.5.3 and the theory of finite étale schemes over Henselian local rings there is a unique R-rational point of $\underline{\mathrm{Sect}}_K$ reducing to the k-rational point x. The first part of the claim of Theorem 4.4.1 now follows from Proposition 4.3.2.

The second part of the claim states that the line bundle $\mathcal{L}^{(p)}$ is ample and of the same degree as $\mathcal{L}$. It suffices to verify the claim on the special fiber since the degree does not jump in a flat connected family. We remark that an abelian scheme over a connected base is connected. It is obvious from the construction that $\mathcal{L}_k^{(p)}$ is ample and has the same degree as $\mathcal{L}_k$. This finishes the proof of Theorem 4.4.1.

4.5.2 Proof of Theorem 4.4.2

First we prove Theorem 4.4.2 in the case $R = k$. Let A be an abelian variety over k and $\mathcal{L}$ a symmetric line bundle on A. We set $\mathcal{L}_\alpha = \mathcal{L}^{\otimes \alpha}$ for $\alpha = 1, 2$.

Proposition 4.5.4 *We have*

$$V^*\mathcal{L}_\alpha \cong \left((\mathcal{L}_\alpha)^{(p)} \right)^{\otimes p}$$

for

$$\alpha = \begin{cases} 2 & \text{if } p = 2, \\ 1 & \text{if } p > 2. \end{cases}$$

Note that we have not assumed that A is ordinary!

Proof. The line bundle

$$\mathcal{L}' = V^*\mathcal{L} \otimes \left(\mathcal{L}^{(p)}\right)^{\otimes -p}$$

is in $\mathrm{Pic}^0_{A^{(p)}/k}$. In order to prove the proposition we have to show that $\mathcal{L}'$ is trivial. By the symmetry of $\mathcal{L}$ we conclude that

$$F^*(V^*\mathcal{L}) \cong [p]^*\mathcal{L} \cong \mathcal{L}^{\otimes p^2}. \tag{4.13}$$

Together with Theorem 4.4.1 this implies that $F^*\mathcal{L}'$ is trivial on A. This means that $\mathcal{L}'$ is in the kernel of the dual

$$\check{F} = \mathrm{Pic}^0_{A/R}(F)$$

of F. The group $\mathrm{Ker}(\check{F})$ is the Cartier dual of $\mathrm{Ker}(F)$ and hence is annihilated by the isogeny $[p]$. As a consequence $\mathcal{L}'$ has order dividing p. Since we have assumed $\mathcal{L}$ to be symmetric, it follows by the definition of $\mathcal{L}^{(p)}$ that

$$[-1]^*\mathcal{L}^{(p)} \cong \mathcal{L}^{(p)}. \tag{4.14}$$

This implies that $\mathcal{L}'$ is symmetric, which is equivalent to

$$\langle \mathcal{L}' \rangle \in \mathrm{Pic}^0_{A/R}[2](k)$$

where $\langle\cdot\rangle$ denotes the class in $\mathrm{Pic}^0_{A/R}$. By the above discussion the element $\langle \mathcal{L}' \rangle$ has order dividing the greatest common divisor of p and 2. If $p > 2$, we conclude that $\mathcal{L}'$ is trivial. If $p = 2$, then

$$\left(\mathcal{L}'\right)^{\otimes 2} = V^*\mathcal{L}_2 \otimes \left(\mathcal{L}_2^{(2)}\right)^{\otimes -2}$$

is trivial. This proves the proposition. □

Counterexample $p = 2$, $\alpha = 1$: We assume k to be algebraically closed. Let E be an ordinary elliptic curve over k and $Q \in E^{(2)}[2](k)$ a generator of the kernel of Verschiebung $V : E^{(2)} \to E$. We have

$$V^*(0_E) = (0_{E^{(2)}}) + (Q) \not\sim 2 \cdot (0_{E^{(2)}}),$$

where 0_E resp. $0_{E^{(2)}}$ denote the zero sections of E resp. $E^{(2)}$ and $\sim$ stands for linear equivalence of Weil divisors.

Now we switch to the notation of Section 4.4. The ring R is assumed to be complete noetherian local with perfect residue class field k of characteristic $p > 0$. Assume we are given an abelian scheme A over R having ordinary reduction and an ample symmetric line bundle $\mathcal{L}$ on A. Let

$$\alpha = \begin{cases} 2 \text{ if } p = 2, \\ 1 \text{ if } p > 2, \end{cases}$$

and $\mathcal{L}_\alpha = \mathcal{L}^{\otimes \alpha}$. We set

$$\mathcal{L}' = V^* \mathcal{L}_\alpha \otimes \left(\mathcal{L}_\alpha^{(p)} \right)^{\otimes -p}.$$

Let G denote the kernel of the dual $\check{F} = \mathrm{Pic}^0_{A/R}(F)$ of F. Reasoning as in the proof of Theorem 4.5.4 one shows that $\mathcal{L}'$ gives an R-rational point x of G. Since A has ordinary reduction the kernel of F is toroidal. We have $G^D = \mathrm{Ker}(F)$ and hence G is étale. By Proposition 4.5.4 the point x reduces to zero. By the étaleness of G we conclude that x itself is equal to zero. This proves Theorem 4.4.2.

4.5.3 Proof of Theorem 4.1.1 and Corollary 4.1.2

We use the notation of Section 4.1. Let A be an abelian scheme of relative dimension g over R having ordinary reduction and $\mathcal{L}$ an ample line bundle of degree 1 on A.

First we prove Theorem 4.1.1. Let $K = (\mathbb{Z}/p\mathbb{Z})^g_R$. As a first step we will construct a Lagrangian decomposition

$$K \times_R K^D \xrightarrow{\sim} H\left(\left(\mathcal{L}^{(p)} \right)^{\otimes p} \right) = A^{(p)}[p]$$

depending on the isomorphism (4.1). In a second step we will show that this Lagrangian decomposition is part of a natural theta structure of type K for the pair

$$\left(A^{(p)}, \left(\mathcal{L}^{(p)} \right)^{\otimes p} \right).$$

Assume we are given an isomorphism

$$(\mathbb{Z}/p\mathbb{Z})^g_k \xrightarrow{\sim} A_k[p]^{\mathrm{et}}. \tag{4.15}$$

The reduction functor gives an equivalence of the categories of finite étale groups over R and of finite étale groups over k. Hence the isomorphism (4.15) determines in a unique way an isomorphism

$$K \xrightarrow{\sim} A[p]^{\mathrm{et}}. \tag{4.16}$$

The isogeny $F : A \to A^{(p)}$ induces a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & A[p]^{\mathrm{loc}} \arrow[r] \arrow[d, "F[p]^{\mathrm{loc}}"] & A[p] \arrow[r] \arrow[d, "F[p]"] & A[p]^{\mathrm{et}} \arrow[r] \arrow[d, "F[p]^{\mathrm{et}}"] & 0 \\
0 \arrow[r] & A^{(p)}[p]^{\mathrm{loc}} \arrow[r] & A^{(p)}[p] \arrow[r] & A^{(p)}[p]^{\mathrm{et}} \arrow[r] & 0
\end{tikzcd}$$

where $F[p]^{\mathrm{et}}$ is an isomorphism (compare Lemma 2.5.2). Composing the isomorphism (4.16) with $F[p]^{\mathrm{et}}$ we get an isomorphism

$$m : K \xrightarrow{\sim} A^{(p)}[p]^{\mathrm{et}}. \tag{4.17}$$

The isomorphism $F[p]^{\mathrm{et}}$ induces a unique section

$$r : A^{(p)}[p]^{\mathrm{et}} \to A^{(p)}[p]$$

of the natural projection $A^{(p)}[p] \to A^{(p)}[p]^{\mathrm{et}}$. We define $t = r \circ m$. For ease of notation we set

$$H = A^{(p)}[p], \quad C = A^{(p)}[p]^{\mathrm{loc}} \quad \text{and} \quad E = A^{(p)}[p]^{\mathrm{et}}.$$

Let $e(\cdot,\cdot)$ denote the commutator pairing on

$$H = H\left(\left(\mathcal{L}^{(p)}\right)^{\otimes p}\right).$$

Since e is a perfect pairing, it induces an isomorphism

$$\varphi : H \xrightarrow{\sim} H^D, \ x \mapsto e(x, \cdot).$$

Since C is connected, the isomorphism φ maps C to the connected component of H^D. As a matter of fact the connected component of H^D is given by E^D (compare Lemma 2.4.5), and the isomorphism φ induces isomorphisms

$$\alpha : C \xrightarrow{\sim} E^D \quad \text{resp.} \quad \beta : E \xrightarrow{\sim} C^D$$

on the local resp. étale part of H. We define

$$k = -(\alpha^{-1} \circ m^{-D}) : K^D \xrightarrow{\sim} C,$$

and set $s = i \circ k$.

Lemma 4.5.5 *The morphism $\delta = s \oplus t$ is a Lagrangian decomposition of type K for H.*

Proof. Consider the commutative diagram

$$\begin{tikzcd}
K^D \arrow[r, "k"] \arrow[d] \arrow[dr, "s"] & C \arrow[r, "\alpha"] \arrow[d, "i"] & E^D \arrow[r, "m^D"] \arrow[d, "p^D"] & K^D \arrow[d] \\
K \times K^D \arrow[r, "\delta"] \arrow[d] & H \arrow[r, "\varphi"] \arrow[d, "p"] & H^D \arrow[r, "\delta^D"] \arrow[d, "i^D"] & K \times K^D \arrow[d] \\
K \arrow[r, "m"] \arrow[ur, "t"] & E \arrow[r, "\beta"] & C^D \arrow[r, "k^D"] & K.
\end{tikzcd}$$

By definition we have

$$m^D \circ \alpha \circ k = -\mathrm{id}.$$

Since the pairing e is alternating, we have $\varphi^D = -\varphi$. This implies that $\beta^D = -\alpha$. Hence

$$k^D \circ \beta \circ m = \big(m^D \circ (-\alpha) \circ k\big)^D = \mathrm{id}.$$

The commutator pairing $e(K)$ on $K \times K^D$ gives an isomorphism

$$\tau : K \times K^D \to K \times K^D, \;\; z \mapsto e(K)\big(z, \cdot\big).$$

One computes

$$\tau\big((x, l)\big) = (x, l^{-1}).$$

As a consequence

$$\tau = \delta^D \circ \varphi \circ \delta,$$

which proves that δ is compatible with the natural commutator pairings on H and $K \times K^D$. □

Now the image of K under δ is by construction the kernel of the lift of Verschiebung $V : A^{(p)} \to A$. For the definition of V see Section 4.4. If we combine Theorem 4.4.1 and Theorem 4.4.2 with Proposition 4.3.2, then we get sections

$$u : K \to G\left(\left(\mathcal{L}^{(p)}\right)^{\otimes p}\right) \quad \text{and} \quad v : K^D \to G\left(\left(\mathcal{L}^{(p)}\right)^{\otimes p}\right)$$

of the natural projection

$$G\left(\left(\mathcal{L}^{(p)}\right)^{\otimes p}\right) \to H.$$

Here K and K^D are considered as subgroups of H via the level structure δ constructed above. By Proposition 4.3.5 the triple (δ, u, v) gives a theta structure of type K for the pair

$$\left(A, \left(\mathcal{L}^{(p)}\right)^{\otimes p}\right).$$

This finishes the proof of Theorem 4.1.1.

It remains to prove Corollary 4.1.2. Let $\#k = q = p^d$. Assume now that A is the canonical lift of A_k. As a consequence there exists a unique isomorphism

$$A^{(q)} \xrightarrow{\sim} A$$

such that composing with F^d is an endomorphism of A lifting the absolute q-Frobenius. Applying Theorem 4.1.1 with $A = A^{(p^{d-1})}$ and $\mathcal{L} = \mathcal{L}^{(p^{d-1})}$ we get a natural theta structure of type $(\mathbb{Z}/p\mathbb{Z})^g_R$ for the pair

$$\left(A, \mathcal{L}^{\otimes p}\right).$$

This completes the proof of Corollary 4.1.2.

Bibliography

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron models.* Number 21 in Ergebnisse der Mathemathik, 3. Folge. Springer-Verlag, 1990.

[DG70] Michel Demazure and Pierre Gabriel. *Groupes Algébriques, Tome I.* North-Holland Publishing Company, Amsterdam, 1970.

[FC90] Gerd Faltings and Ching-Li Chai. *Degeneration of abelian varieties.* Number 22 in Ergebnisse der Mathematik, 3. Folge. Springer-Verlag, 1990.

[MB85] Laurent Moret-Bailly. *Pinceaux de variétés abéliennes*, volume 129 of *Astérisque.* Société Mathématiques de France, 1985.

[Mum66] David Mumford. On the equations defining abelian varieties I. *Inventiones Mathematicae*, 1:287–354, 1966.

[Mum70] David Mumford. *Abelian varieties.* Oxford University Press, London, 1970.

Index

Acknowledgments

I'm indebted to B. de Smit, B. Edixhoven, H.W. Lenstra, B. Moonen, J. Murre, F. Oort, P. Stevenhagen, E. Thomas, J. Top, M. van der Put and all other members of the algebra and geometry groups in Leiden and Groningen for their cooperativeness and for the warm hospitality that they offered to me. I'm grateful to G. Böckle, I. Bouw, G. Frey, D. Kohel, D. Lubicz, J.-F. Mestre, M. Raynaud, C. Ritzenthaler, T. Satoh, L. Thaelman and F. Vercauteren for making comments on my work.

I thank Aaron, Arie, Bas, Bill, Christiaan, Diego, Erwin, Gabor, Geert, Gert-Jan, Gonnie, Henk, Irene, Jeanine, Jasper, Jeroen, John, Joost, Jun, Lara, Maint, Marc, Martijn, Reinier, Remke, Renato, Riccardo, Richard, Robert, Roland, Theo, Theresa and Willem Jan for their support and company.

I dedicate this thesis to my parents who encouraged me whenever it was necessary during the past four years.

Samenvatting

Het onderdeel van de wiskunde waartoe dit proefschrift behoort, houdt zich bezig met het berekenen van zeta-functies van variëteiten over eindige lichamen. Zo'n variëteit is een meetkundig object gedefinieerd door vergelijkingen

$$f_i(x_1, \ldots, x_n) = 0, \quad i = 1, \ldots, r,$$

waarbij de f_i polynomen met coëfficiënten in een eindig lichaam $\mathbb{F}_q$ zijn. Het berekenen van de zeta-functie komt ruwweg neer op het bepalen van het aantal oplossingen van dit systeem vergelijkingen in $\mathbb{F}_q^n$. In de omgangstaal heet dit "punten tellen".

Vele methoden die cryptografen tegenwoordig gebruiken voor het versleutelen van gegevens, zoals de Diffie-Hellman- en ElGamal-cryptosystemen, zijn gebaseerd op berekeningen in een eindige abelse groep. De populaire crypto-software PGP (Pretty Good Privacy) gebruikt bijvoorbeeld het ElGamal-cryptosysteem met de multiplicatieve groep $\mathbb{F}_q^*$ van een eindig lichaam. Als andere mogelijkheid kan men in de groep van rationale punten $A(\mathbb{F}_q)$ op een abelse variëteit A over $\mathbb{F}_q$ rekenen. Een abelse variëteit is een projectieve variëteit waarvan de punten een abelse groep vormen. Abelse variëteiten van dimensie 1 zijn niets anders dan elliptische krommen.

De veiligheid van het ElGamal-cryptosysteem berust op de moeilijkheid van het *discrete logaritme-probleem* in de gebruikte groep, d.w.z. het zoeken van een geheel getal m zodanig dat $a = b^m$ voor gegeven groepselementen a en b waarvan bekend is dat zo'n m bestaat. De moeilijkheid van het discrete logaritme-probleem in een groep als $A(\mathbb{F}_q)$ wordt in de eerste plaats bepaald door de orde van de groep. Om te controleren of een gegeven abelse variëteit A cryptografisch bruikbaar is, moet men dus op een effectieve manier de rationale punten op A over $\mathbb{F}_q$ kunnen tellen.

Men onderscheidt l-adische en p-adische methoden voor het tellen van punten op een variëteit V gedefinieerd over een eindig lichaam $\mathbb{F}_q$ van karakteristiek p. Een l-adische methode berekent het gevraagde aantal modulo machten van verschillende kleine priemgetallen $l \neq p$, een p-adische modulo machten van p. In tegenstelling tot l-adische methoden, zijn p-adische methoden alleen van toepassing als de karakteristiek p klein is.

De eerste algoritme voor het tellen van punten op een elliptische kromme werd ontdekt door R. Schoof in de jaren '80. Schoof's algoritme is l-adisch. Zijn algoritme werd verder ontwikkeld door N.D. Elkies en A.O.L. Atkin. Eind jaren '90 werden p-adische methoden geïntroduceerd door T. Satoh, K. Kedlaya, A. Lauder en J.-F. Mestre. Een heel peloton onderzoekers werkt aan het optimaliseren en generaliseren van hun methoden. Satoh's algoritme is beperkt tot elliptische krommen. De algoritmen van Kedlaya en Lauder kunnen worden gebruikt voor een bredere klasse van variëteiten. De efficiëntste algoritme voor het tellen van punten op een hoger-dimensionale abelse variëteit werd gevonden door Mestre. Zijn zogenaamde AGM-methode werkt voor abelse variëteiten over een eindig lichaam van karakteristiek 2.

Mestre's methode gebruikt een klassieke constructie, het rekenkundig-meetkundige gemiddelde, in het Engels "arithmetic geometric mean" (AGM). Het AGM werd ontdekt en bestudeerd door C.F. Gauss en J.-L. Lagrange aan het eind van de 18de eeuw. Gauss slaagde erin de waarden van elliptische integralen uit te drukken in het AGM. De AGM-rij is een rij getallen, recursief gedefinieerd door

$$a_{n+1} = \frac{a_n + b_n}{2}, \quad b_{n+1} = \sqrt{a_n b_n}, \quad n \geq 0$$

voor gegeven a_0 en b_0. De AGM-rij kan worden gedefinieerd voor positieve reële getallen, maar ook voor complexe en p-adische getallen. In het p-adische geval moeten de beginwaarden zodanig worden gekozen dat men de wortel kan trekken. Om dit herhaald te kunnen doen moet men steeds de "juiste" wortel kiezen. Voor reële getallen convergeert de AGM-rij naar het AGM, de gemeenschappelijke limiet van a_n en b_n. Dit is ook waar in het complexe en p-adische geval als steeds de "juiste" wortel wordt gekozen. Een uitzondering vormt het 2-adische geval. Voor $p = 2$ kan de AGM-rij zowel convergeren als divergeren.

Elliptische krommen bieden de mogelijkheid de AGM-rij meetkundig te interpreteren. Stel a_n en b_n zijn gegeven door de AGM-formules, en laat de elliptische kromme E_n gegeven zijn door de vergelijking

$$y^2 = x(x - a_n^2)(x - b_n^2).$$

Er is een rationale afbeelding $E_n \to E_{n+1}$ gegeven door

$$(x, y) \mapsto \left(\frac{(x + a_n b_n)^2}{4x}, \frac{y(a_n b_n - x)(a_n b_n + x)}{8x^2} \right).$$

Deze afbeelding is een 2-isogenie, d.w.z. het is een surjectief morfisme van groepen met als kern de ondergroep van orde 2 voortgebracht door het punt $(0,0)$. Mestre heeft de rij krommen E_n bestudeerd over het lichaam van de 2-adische getallen $\mathbb{Q}_2$. Zoals Mestre opmerkt convergeert de rij van j-invarianten

$$j_n = 2^8 \frac{(a_n^4 - a_n^2 b_n^2 + b_n^4)^3}{a_n^4 b_n^4 (a_n^2 - b_n^2)^2}$$

behorend bij de rij E_n als E_0 goede gewone reductie heeft, d.w.z. de reductie van E_0 is een elliptische kromme met een rationaal punt van orde 2. De rij E_n heeft een hoger-dimensionaal analogon, een rij van 2-isogene abelse variëteiten over $\mathbb{Q}_2$ die ten grondslag ligt aan Mestre's algoritme voor het tellen van punten op een gewone hyperelliptische kromme over een eindig lichaam van karakteristiek 2.

Het onderzoeksprogramma dat voor een belangrijk deel in dit proefschrift is uitgevoerd, voorziet de methode van Mestre van een nieuwe conceptuele basis, die de mogelijkheid opent de methode uit te breiden naar willekeurige karakteristiek p. We definiëren de GAGM-rij (gegeneraliseerde AGM-rij) als een zekere rij van p-isogene abelse variëteiten over $\mathbb{Q}_p$ die in het 1-dimensionale geval voor $p = 2$ overeen komt met de rij E_n. In Hoofdstuk 2 bewijzen we dat de GAGM-rij p-adisch convergeert. In Hoofdstuk 3 wordt een algoritme geïntroduceerd die gebaseerd is op de GAGM-rij en de orde berekent van de groep van rationale punten op een elliptische kromme over een eindig lichaam van karakteristiek $p > 2$. In Hoofdstuk 4 wordt het bestaan van canonieke projectieve coördinaten voor de GAGM-rij aangetoond. Deze coördinaten worden geconstrueerd door de GAGM-rij in te bedden in de moduli-ruimte van abelse schema's met theta-struktuur. Het doel van ons onderzoeksprogramma is de AGM-rij te berekenen in termen van deze coördinaten.