Geometric quadratic chabauty and other topics in number theory

Lido, G.M.

GEOMETRIC QUADRATIC CHABAUTY AND OTHER TOPICS IN NUMBER THEORY

Proefschrift

ter verkrijging van
de graad van doctor aan de Universiteit Leiden
op gezag van rector magnificus prof. dr. ir. H. Bijl,
volgens besluit van het college voor promoties
te verdedigen op dinsdag 12 oktober 2021
klokke 11.15 uur

door

Guido Maria Lido
geboren te Roma, Italia, in 1992

Promotor: Prof. dr. Bas Edixhoven (Universiteit Leiden)

Promotor: Prof. dr. René Schoof (Università di Roma "Tor Vergata")

Samenstelling van de promotiecommissie:

Voorzitter: Prof. dr. F.A. van der Duijn Schouten

Secretaris: Prof. dr. Peter Stevenhagen (Universiteit Leiden)

Prof. dr. Davide Lombardo (Università di Pisa)

Prof. dr. Marusia Rebolledo (Université B. Pascal Clermont-Ferrand 2)

Prof. dr. Michael Stoll (Universität Bayreuth)

This work was carried out at Università di Roma "Tor Vergata" and Universiteit Leiden. It was funded jointly by Università di Roma "Tor Vergata" and Universiteit Leiden.

The images in the front cover of this thesis, from the bottom to the top, are: an illustration of the geometric quadratic Chabauty method drawn by Sachi Hashimoto, available in [51], and representations of the modular curves $X_{\mathrm{ns}}(13)$ and $X_{\mathrm{ns}}^{+}(13)$, drawn using the equations in [36].

The illustration in the back cover has been drawn by Giulia Caudullo and represents the descent algorithm in Chapter 4.

Contents

Introduction

This thesis consists of three parts. The first part is devoted to the quadratic Chabauty method, the second part to automorphisms of modular curves of Cartan type and the third to the discrete logarithm problem over finite fields whose characteristic is small compared to the cardinality.

The first two chapters are the result of a joint work with Bas Edixhoven and describe a method that, in certain cases, determines the set of rational points on a curve $C/\mathbb{Q}$ of genus at least 2. The finiteness of the set $C(\mathbb{Q})$ is a special case of a theorem proved by Faltings in [43], but computing this set for each curve C is still an unsolved problem. In [24], Chabauty proposed a method to solve this problem when $C(\mathbb{Q})$ contains at least one point b and the rank r of the Mordell-Weil group of the jacobian of C is smaller than the genus g of the curve. Denoting J the jacobian of C and $j_b\colon C \to J$ the map sending a point x to $[x-b]$, Chabauty's method is based on the following diagram, which is commutative for every choice of a prime p

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{j_b} & J(\mathbb{Q}) \\ \downarrow & & \downarrow \\ C(\mathbb{Q}_p) & \xrightarrow{j_b} & J(\mathbb{Q}_p) \end{array} .$$

The commutativity of the diagram implies that $C(\mathbb{Q})$, considered as a subset of $J(\mathbb{Q}_p)$, is contained in the intersection of $C(\mathbb{Q}_p)$ and the closure $\overline{J(\mathbb{Q})}$ of $J(\mathbb{Q})$. Up to computing generators for $J(\mathbb{Q})$, both the sets $C(\mathbb{Q}_p)$ and $\overline{J(\mathbb{Q})}$ can be computed with arbitrarily large precision inside $J(\mathbb{Q}_p)$ and their intersection is finite when r is smaller than g. Chabauty's method is to compute such an intersection, so to determine a finite subset of $C(\mathbb{Q}_p)$ containing $C(\mathbb{Q})$. Such an intersection can be larger than $C(\mathbb{Q})$ but in practice the Mordell-Weil sieve is usually enough to get rid of the undesired points.

In [62] and [63], Minhyong Kim proposes a non-abelian generalization of the Chabauty method, using the Galois cohomology of the $\mathbb{Q}_p$-pro-unipotent fundamental group of C.

The most interesting application of Kim's method is the so-called "quadratic Chabauty method", which is explicit and works when the rank ρ of the group $\mathrm{Pic}(J)/\mathrm{Pic}^0(J)$ is larger than $r-g+1$. In [10] this method is applied to the so-called cursed curve ($r = g = 3$).

In chapter 1 we aim to make the quadratic Chabauty method *small* and *geometric* again: our generalization of Chabauty's method works by substituting J with a product of $\mathbb{G}_\mathrm{m}$-torsors over J and by extending the geometry over $\mathbb{Z}$.

Let $J^\vee$ be the dual abelian variety of J and let P be the Poincaré bundle on $J \times J^\vee$, the universal translational-invariant line bundle on J. After removing the zero-section of P we get a $\mathbb{G}_\mathrm{m}$-torsor $P^\times \to J \times J^\vee$, named *Poincaré torsor of* J, which is the main actor in our method. For any $\mathbb{Q}$-scheme S and any choice of points $x, x_1, x_2 \in J(S)$ and $y, y_1, y_2 \in J^\vee(S)$, the theorem of the cube implies the existence of canonical isomorphisms $(x_1, y)^*P \otimes (x_2, y)^*P = (x_1 + x_2, y)^*P$ and $(x, y_1)^*P \otimes (x, y_2)^*P = (x, y_1 + y_2)^*P$. This implies the existence of maps

$$+_1 \colon (x_1, y)^*P^\times \times_S (x_2, y)^*P^\times \longrightarrow (x_1 + x_2, y)^*P^\times ,$$
$$+_2 \colon (x, y_1)^*P^\times \times_S (x, y_2)^*P^\times \longrightarrow (x, y_1 + y_2)^*P^\times .$$

These partial operations $+_1, +_2$ give the Poincaré torsor a structure of *biextension*.

Moreover, the group of line bundles on J that arise as $(\mathrm{id}, g)^*P$ for some morphism $g \colon J \to J^\vee$ is a subgroup of $\mathrm{Pic}(J)$ of finite index: all the elements of $\mathrm{Pic}^0(J)$ can be obtained with g constant and, for any class $[\mathcal{L}] \in \mathrm{Pic}(J)/\mathrm{Pic}^0(J)$, the class $2[\mathcal{L}]$ can be obtained choosing $g \colon x \mapsto \mathrm{tr}_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$, where tr_x is the translation by x on J. This implies the existence of maps $g_1, \dots, g_{\rho-1} \colon J \to J^\vee$ such that the line bundles $\mathcal{L}_i := (\mathrm{id}, g_i)^*P$ are linearly independent in $\mathrm{Pic}(J)$ and, for every $i \in \{1, \dots, \rho-1\}$, the line bundle $j_b^*(\mathcal{L}_i)$ on C is the trivial. Let $\mathcal{L}_i^\times$ be the $\mathbb{G}_\mathrm{m}$-torsor on J obtained removing the zero-section from $\mathcal{L}_i$ and let T be the $\mathbb{G}_\mathrm{m}^{\rho-1}$-torsor on J obtained as the product of all the $\mathcal{L}_i^\times$. Then j_b^*T is a trivial $\mathbb{G}_\mathrm{m}^{\rho-1}$-torsor on C, implying that the map $j_b \colon C \to J$ can be lifted to a map

$$\widetilde{j_b} \colon C \longrightarrow T .$$

This construction can be extended over $\mathbb{Z}$. The abelian varieties J and $J^\vee$ admit Néron models over $\mathbb{Z}$ and the Poincaré torsor uniquely extends, as a biextension, to a $\mathbb{G}_\mathrm{m}$-torsor over the product of the Néron model of J and the scheme $J^{\vee 0}$, defined as the fibrewise connected component of 0 in the Néron model of $J^\vee$. Up to composing g_i with a certain multiplication map on $J^\vee$, we can suppose that the image of the Néron model of J under g_i is contained in $J^{\vee 0}$. This gives the extension of $\mathcal{L}_i$ and T as torsors over the Néron model of J. The curve $C/\mathbb{Q}$ can be extended to a regular proper curve $C/\mathbb{Z}$, but to apply our method we need to restrict to certain open sub-schemes. Inside the smooth part of

C let U be an open sub-scheme obtained by removing, for each prime q of bad reduction, all but one irreducible component of the fibre at $\mathbb{F}_q$. The map j_b extends to the smooth part of C and the line bundles $j_b^*\mathcal{L}_i$ are trivial on U. Hence there exists a lift $\widetilde{j_b}\colon U \to T$ of j_b making the following diagram commutative for every prime p

$$\begin{array}{ccc} U(\mathbb{Z}) & \xrightarrow{\widetilde{j_b}} & T(\mathbb{Z}) \\ \downarrow & & \downarrow \\ U(\mathbb{Z}_p) & \xrightarrow{\widetilde{j_b}} & T(\mathbb{Z}_p) \end{array} .$$

For simplicity we suppose $p > 2$. Since $T(\mathbb{Z})$ is a $\mathbb{G}_{\mathrm{m}}(\mathbb{Z})^{\rho-1}$-torsor over $J(\mathbb{Z})$ and since $\mathbb{G}_{\mathrm{m}}(\mathbb{Z})^{\rho-1}$ is a finite group, we expect the closure $\overline{T(\mathbb{Z})}$ of $T(\mathbb{Z})$ inside $T(\mathbb{Z}_p)$ to be a p-adic variety of dimension at most r. This is a consequence of Theorem 1.4.10: the set of points in $\overline{T(\mathbb{Z})}$ with a given reduction modulo p, when not empty, is the image of an analytic map $\kappa\colon \mathbb{Z}_p^r \to T(\mathbb{Z}_p)$, constructed using the biextension structure on $P^\times$. Since $U(\mathbb{Z}_p)$ is 1-dimensional and $T(\mathbb{Z}_p)$ has dimension $g+\rho-1$, we expect the set $\overline{T(\mathbb{Z})} \cap U(\mathbb{Z}_p)$ to be finite when ρ is larger than $r-g+1$. This is proven in Section 1.9.2.

The geometric quadratic Chabauty method is to compute $\overline{T(\mathbb{Z})} \cap U(\mathbb{Z}_p)$, so to determine a finite subset of $U(\mathbb{Z}_p)$ containing $U(\mathbb{Z})$. Since $C(\mathbb{Q})$ is the union of the sets $U(\mathbb{Z})$ for all possible U's and since there are finitely many U's, the method can be used to prove that a certain list of points in $C(\mathbb{Q})$ is complete. In Theorem 1.4.12 we explain how, sometimes, computations in $T(\mathbb{Z}/p^2\mathbb{Z})$ imply a bound on the cardinality of $\overline{T(\mathbb{Z})} \cap U(\mathbb{Z}_p)$. In Sections 1.6 and 1.7 we explain how to make the method explicit. In Section 1.8 we apply our method to a specific example, with $g = r = \rho = 2$. Chapter 2 is devoted to an alternative proof of Theorem 1.4.10, using formal biextensions.

A motivation to study modular curves associated to Cartan and Cartan-plus subgroups of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, as we do in chapter 3, comes from Serre's uniformity conjecture. This conjecture states that, for p prime big enough, the natural Galois representation $G_{\mathbb{Q}} \to \mathrm{GL}(E[p])$ is surjective for any elliptic curve $E/\mathbb{Q}$. The conjecture would be solved if we knew, for each prime p and each maximal subgroup $H < \mathrm{GL}_2(\mathbb{F}_p)$ such that $\det(H) = \mathbb{F}_p^\times$, the rational points on the modular curve associated with H. All the H's for which we do not know the answer are Cartan-plus subgroups, which are maximal for $p > 3$. This also gives motivation to study the so-called cursed curve, which is a modular curve associated to a Cartan-plus subgroup of $\mathrm{GL}_2(\mathbb{F}_{13})$.

Given a positive integer n, a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ is a subgroup arising as $A^\times \subset \mathrm{GL}(A) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ for some étale $\mathbb{Z}/n\mathbb{Z}$-algebra A of rank 2. We call Cartan-plus subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ a subgroup generated by $A^\times$ and the group of ring automorphisms of A, for some étale $\mathbb{Z}/n\mathbb{Z}$-algebra A of rank 2. For example, if n is prime there are two Cartan subgroups and two Cartan-plus subgroups up to conjugacy: the split

Cartan, respectively Cartan-plus, if $A \cong \mathbb{F}_n \times \mathbb{F}_n$ and the non-split Cartan, respectively Cartan-plus, if $A \cong \mathbb{F}_{n^2}$. We notice that the term *Cartan-plus* is not common in the literature: the most studied cases are the ones where $n > 3$ is prime and in these cases Cartan-plus subgroups are just normalizers of Cartan subgroups. We also deal with composite level and studying Cartan-plus subgroups allows us to state certain results with more uniformity than we could have done if we had studied normalizers of Cartan subgroups.

When a modular curve X is geometrically connected, the set $Y(\mathbb{C})$, made of its complex non-cuspidal points, is the quotient of $\mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ by the action of a subgroup $\Gamma < \mathrm{PSL}_2(\mathbb{Z})$. Every matrix $m \in \mathrm{PSL}_2(\mathbb{R})$ defines a complex automorphism of $\mathbb{H}$, that descends to an automorphism of $Y(\mathbb{C})$ if and only if the matrix m lies in the normalizer of Γ. When this happens, the automorphism extends to the whole $X(\mathbb{C})$. We call *modular* automorphism of $X_{\mathbb{C}}$ any such automorphism. We call *Cartan curve* a modular curve associated to a Cartan or to a Cartan-plus subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Using this terminology we state the main result of chapter 3.

Theorem. *Let n be either an integer larger than 10^{400} or a prime power such that $n > 11$ and $n \notin \{3^3, 2^4, 2^5, 2^6\}$. Then, over $\mathbb{C}$, all the automorphisms of a Cartan curve of level n are modular.*

For each Cartan or Cartan-plus subgroup $H < \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, the group of modular automorphisms of the modular curve associated to H is easy to compute: it is either isomorphic to $N'/H' \times \mathbb{Z}/2\mathbb{Z}$ or to N'/H', where $N' < \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ is the normalizer of $H' := H \cap \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$. This is stated more precisely in Proposition 3.6.13. Remark 3.6.16 gives N'/H' for each possible H.

In the proof of the main result of chapter 3, one of the steps is the following generalization of a result of Chen.

Theorem. *Let n be a positive integer. Then the jacobian of a Cartan curve of level n is a quotient of the jacobian of the modular curve $X_0(n^2)$.*

Using the last theorem and a result of Shimura characterizing the CM sub-abelian varieties of $J_0(n^2)$, we prove that, for all but finitely many n, a large part of the jacobian of a Cartan curve does not contain any CM sub-abelian variety. This, using a result of Ribet, implies that all the automorphisms of a Cartan curve of level n are defined over a compositum of quadratic fields for all but finitely many n.

The main result of chapter 3 then follows from Abramovich's lower bound of the gonality of modular curves and the following criterion.

Lemma. *Let n be a positive integer and let X be the base change to $\mathbb{C}$ of a modular curve associated with a subgroup $H < \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Suppose that H contains the scalar*

matrices, that $\det(H)$ *is the whole* $(\mathbb{Z}/n\mathbb{Z})^\times$ *and that there are two primes* $\ell_1 < \ell_2$ *not dividing* n *such that* $5 \leq \ell_2 < \frac{1}{2}\mathrm{gon}(X) - 1$*, with* $\mathrm{gon}(X)$ *the gonality of* X*. Then every automorphism of* X *which is defined over a compositum of quadratic fields is modular.*

For an automorphism $u\colon X \to X$ to be modular it is necessary and sufficient that u preserves the set of cusps, so that u restricts to an automorphism of the non-cuspidal locus Y, and preserves the set of elliptic points, namely the branch points of the map $\mathbb{H} \to Y(\mathbb{C})$.

In Section 3.3 we see how to distinguish cusps, elliptic points and all the other points on X by looking at the action of Hecke operators T_{l_1}, T_{l_2}. More precisely, we look for multiple points in the divisors $T_{l_i}(x)$ for $x \in X(\mathbb{C})$: if x is a cusp, then $T_{l_i}(x)$ contains a point of multiplicity at least l_i; if $x = (E, \phi)$ is an elliptic point such that $j(E) = 0$, then $T_{l_i}(x)$ contains a point of multiplicity 3; if $x = (E, \phi)$ is an elliptic point such that $j(E) = 1728$, then $T_{l_i}(x)$ contains $\lfloor (l_i - 1)/2 \rfloor$ points of multiplicity 2.

These characterizations help proving the Lemma because of the following commutation rule in the group of divisors of X

$$uT_{l_i} = T_{l_i} u^{\sigma_i} ,$$

where $\sigma_i \in G_{\mathbb{Q}}$ is a l_i-th Frobenius and $u\colon X \to X$ is supposed to be defined over a compositum of quadratic fields. The Eichler-Shimura relations imply the above equality in $\mathrm{Pic}^0(X)$ and the hypothesis on the gonality implies that the equality extends to the group of divisors of X.

In the last chapter we describe an algorithm to solve the discrete logarithm problem. Given a group G with a generator $g \in G$, solving the discrete logarithm problem means, for each element $h \in G$, computing an integer z such that $g^z = h$. The security of certain public-key cryptographic protocols depends on the hardness of this problem, depending on the choice of G. We are concerned with the cases where G is the multiplicative group of a finite field of *small characteristic*, which, for us, means a field of characteristic p and cardinality p^n for some integer $n > p$. The main result of the last chapter states that the discrete logarithm problem on finite fields of small characteristic is quasi-polynomial, hence not too hard.

Theorem. *There exists a probabilistic algorithm, described in Section 4.4, that solves the discrete logarithm problem in* $K^\times$ *for all finite fields* K *of small characteristic (namely the fields* $\mathbb{F}_{p^n}$ *with* $n > p$*) in expected time*

$$(\log \#K)^{O(\log\log \#K)} .$$

Our algorithm uses some ideas of the algorithm in [19], whose running time is only heuristic, and adapts them to finite fields with a different type of presentation. Let $\mathbb{F}_q$ be

a finite field with $q > 2$ elements, let $E/\mathbb{F}_q$ be an elliptic curve and let P_1 be a point on E such that $\phi(P_1) - P_1 \in E(\mathbb{F}_q)$, where $\phi\colon E \to E$ is the q-th Frobenius. If $K = \mathbb{F}_q(P_1)$, then the coordinates of P_1 are generators of the extension $\mathbb{F}_q \subset K$ on which the q-th Frobenius acts "simply". If this happens and if, moreover $[K : \mathbb{F}_q] > 2$, the elliptic curve E and the point P_1 give an *elliptic presentation* of K. Given the abundance of elliptic curves over $\mathbb{F}_q$, for q big enough, it is easy to prove that every finite field of small characteristic can be embedded in a slightly larger field admitting an elliptic presentation such that q is small compared to $\#K$. A more precise statement is given in Proposition 4.1.5.

Given a finite field K with an elliptic presentation, we represent elements in $K^\times$ as $f(P_1)$ with f varying among the rational functions in $\mathbb{F}_q(E)$ that are regular and non-vanishing on P_1. Hence, we extend the discrete logarithm to these rational functions and, in a weak sense, to divisors on E. Notice that each divisor defined over $\mathbb{F}_q$ is a linear combination of irreducible divisors, namely those divisors that are the sum, with multiplicity 1, of all the $G_{\mathbb{F}_q}$-conjugates of a point in $E(\overline{\mathbb{F}_q})$.

Our algorithm is an index calculus using divisors: the idea is looking for linear relations among the discrete logarithm of h and the "discrete logarithms" of irreducible divisors of small degree; when many relations are found, we compute the discrete logarithm of h by solving a linear system.

We find relations using a descent procedure, which, given an irreducible divisor D of degree $4d \geq 320$, computes irreducible divisors D_i of degree dividing $2d$ such that the "discrete logarithm" of D is a linear combination of the "discrete logarithms" of the D_i's. Most of the last chapter is devoted to the description and the proof of the correctness of this descent procedure. It mainly uses the following equalities

$$f(P_1)^q = f^\phi(\phi(P_1)) = f^\phi(P_1 + P_0) = f^\phi \circ \tau_{P_0}(P_1)\,,$$

where $f \in \overline{\mathbb{F}_q}(E)$ is a function regular and non vanishing in P_1, the point $P_0 \in E(\mathbb{F}_q)$ is equal to $\phi(P_1) - P_1$, the map $f \to f^\phi$ is the automorphism on $\overline{\mathbb{F}_q}(E)$ that acts as the q-th Frobenius on $\overline{\mathbb{F}_q}$ and sends x and y to themselves. In Section 4.5 we see that, in order to compute the divisors D_i, it is sufficient to find a rational function f and a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ satisfying certain conditions. After parametrizing the possible f's, this problem boils down to finding points in $\mathcal{C}(k)$, where $k \subset \overline{\mathbb{F}_q}$ is the extension of $\mathbb{F}_q$ of degree d and $\mathcal{C}$ is a variety of dimension at most 2 whose definition depends on D. We prove that $\mathcal{C}(k)$ is large using Weil's estimates. To prove that the geometrically irreducible components of $\mathcal{C}$ are defined over k, we use a little bit of Galois theory, condensed in Proposition 4.6.1, and some tedious computations, mostly contained in Proposition 4.6.3 and in the Claims 4.8.2.3, 4.8.2.6, 4.8.3.2.

Chapter 1

Geometric quadratic Chabauty

This chapter is the result of a joint work with Bas Edixhoven. It will appear in Journal de l'Institut de Mathematiques de Jussieu

Since Faltings proved Mordell's conjecture (1983) we know that the sets of rational points on curves of genus at least 2 are finite. Determining these sets, in individual cases, is still an unsolved problem. Chabauty's method (1941) is to intersect, for a prime number p, in the p-adic Lie group of p-adic points of the jacobian, the closure of the Mordell-Weil group with the p-adic points of the curve. If the Mordell-Weil rank is less than the genus, and if one has generators for the Mordell-Weil group, and if one can implement Chabauty's method and the Mordell-Weil sieve, then, as far as we know, this method has been applied successfully to determine all rational points in many cases.

Minhyong Kim's non-abelian Chabauty programme aims to remove the condition on the rank. The simplest case, called quadratic Chabauty, was developed by Balakrishnan, Besser, Dogra, Müller, Tuitman and Vonk, and applied in a tour de force to the so-called cursed curve (rank and genus both 3).

This article aims to make the quadratic Chabauty method *small* and *geometric* again, by describing it in terms of only 'simple algebraic geometry' (line bundles over the jacobian and models over the integers).

1.1 Introduction

Faltings proved in 1983, see [43], that for every number field K and every curve C over K of genus at least 2, the set of K-rational points $C(K)$ is finite. However, determining $C(K)$, in individual cases, is still an unsolved problem. For simplicity, we restrict ourselves in this article to the case $K = \mathbb{Q}$.

Chabauty's method (1941) for determining $C(\mathbb{Q})$ is to intersect, for a prime number p, in the p-adic Lie group of p-adic points of the jacobian, the closure of the Mordell-Weil group with the p-adic points of the curve. If the Mordell-Weil rank r satisfies $r < g$, and if one has generators for the Mordell-Weil group, and if one can implement Chabauty's method and (if $r = g - 1$) the Mordell-Weil sieve, then, as far as we know, this method has never failed.

For a general introduction to Chabauty's method and Coleman's effective version of it, we highly recommend [78], and, for an implementation of it that is 'geometric' in the sense of this article, to [44], in which equations for the curve embedded in the Jacobian are pulled back via local parametrisations of the closure of the Mordell-Weil group.

Minhyong Kim's non-abelian Chabauty programme aims to remove the condition that $r < g$. The 'non-abelian' refers to fundamental groups; the fundamental group of the jacobian of a curve is the abelianised fundamental group of the curve. The most striking result in this direction is the so-called quadratic Chabauty method, applied in [10], a technical tour de force, to the so-called cursed curve ($r = g = 3$). For more details we recommend the introduction of [10].

This article aims to make the quadratic Chabauty method *small* and *geometric* again, by describing it in terms of only 'simple algebraic geometry' (line bundles over the jacobian, models over the integers, and biextension structures). The main result is Theorem 1.4.12. It gives a criterion for a given list of rational points to be complete, in terms of points with values in $\mathbb{Z}/p^2\mathbb{Z}$ only. Section 1.2 describes the geometric method in less than 3 pages, Sections 1.3–1.5 give the necessary theory, Sections 1.6–1.7 give descriptions that are suitable for computer calculations, and Section 1.8 treats an example with $r = g = 2$ and 14 rational points. As explained in the remarks following Theorem 1.4.12, we expect that this approach will make it possible to treat many more curves. Section 1.9.1 gives some remarks on the fundamental groups of the objects we use. They are subgroups of higher dimensional Heisenberg groups, where the commutator pairing is the intersection pairing of the first cohomology group of the curve. Section 1.9.2 reproves the finiteness of $C(\mathbb{Q})$, for C with $r < g + \rho - 1$, with ρ the rank of the $\mathbb{Z}$-module of symmetric endomorphisms of the jacobian of C. It also shows that a version of Theorem 1.4.12 that uses higher p-adic precision will always give a finite upper bound for $C(\mathbb{Q})$. Section 1.9.3 gives, through an appropriate choice of coordinates that split the Poincaré biextension, the relation between our geometric approach and the p-adic heights used in the cohomological approach.

Already for the case of classical Chabauty (working with J instead of T, and under the assumption that $r < g$), where everything is linear, the criterion of Theorem 1.4.12 can be useful; this has been worked out and implemented in [98]. We recommend this work as

a gentle introduction into the geometric approach taken in this article. A generalisation from $\mathbb{Q}$ to number fields is given in [29]. For a generalisation of the cohomological approach, see [6] (quadratic Chabauty) and [34] (non-abelian Chabauty).

Although this article is about geometry, it contains no pictures. Fortunately, many pictures can be found in [51], and some in [40].

1.2 Algebraic geometry

Let C be a scheme over $\mathbb{Z}$, proper, flat, regular, with $C_{\mathbb{Q}}$ of dimension one and geometrically connected. Let n be in $\mathbb{Z}_{\geq 1}$ such that the restriction of C to $\mathbb{Z}[1/n]$ is smooth. Let g be the genus of $C_{\mathbb{Q}}$. We assume that $g \geq 2$ and that we have a rational point $b \in C(\mathbb{Q})$; it extends uniquely to a $b \in C(\mathbb{Z})$. We let J be the Néron model over $\mathbb{Z}$ of the jacobian $\mathrm{Pic}^0_{C_{\mathbb{Q}}/\mathbb{Q}}$. We denote by $J^\vee$ the Néron model over $\mathbb{Z}$ of the dual $J^\vee_{\mathbb{Q}}$ of $J_{\mathbb{Q}}$, and $\lambda\colon J \to J^\vee$ the isomorphism extending the canonical principal polarisation of $J_{\mathbb{Q}}$. We let $P_{\mathbb{Q}}$ be the Poincaré *line bundle* on $J_{\mathbb{Q}} \times J^\vee_{\mathbb{Q}}$, trivialised on the union of $\{0\} \times J^\vee_{\mathbb{Q}}$ and $J_{\mathbb{Q}} \times \{0\}$. Then the Poincaré *torsor* is the $\mathbb{G}_{\mathrm{m}}$-torsor on $J_{\mathbb{Q}} \times J^\vee_{\mathbb{Q}}$ defined as

$$P^\times_{\mathbb{Q}} = \mathbf{Isom}_{J_{\mathbb{Q}} \times J^\vee_{\mathbb{Q}}}(\mathcal{O}_{J_{\mathbb{Q}} \times J^\vee_{\mathbb{Q}}}, P_{\mathbb{Q}})\,. \tag{1.2.1}$$

For every scheme S over $J_{\mathbb{Q}} \times J^\vee_{\mathbb{Q}}$, $P^\times_{\mathbb{Q}}(S)$ is the set of isomorphisms from $\mathcal{O}_S$ to $(P_{\mathbb{Q}})_S$, with a free and transitive action of $\mathcal{O}_S(S)^\times$. Locally on S for the Zariski topology, $(P^\times_{\mathbb{Q}})_S$ is trivial, and $P^\times_{\mathbb{Q}}$ is represented by a scheme over $J_{\mathbb{Q}} \times J^\vee_{\mathbb{Q}}$.

The theorem of the cube gives $P^\times_{\mathbb{Q}}$ the structure of a *biextension* of $J_{\mathbb{Q}}$ and $J^\vee_{\mathbb{Q}}$ by $\mathbb{G}_{\mathrm{m}}$, a notion for the details of which we recommend Section I.2.5 of [77], Grothendieck's Exposés VII and VIII [91], and references therein. This means the following. For S a $\mathbb{Q}$-scheme, x_1 and x_2 in $J_{\mathbb{Q}}(S)$, and y in $J^\vee_{\mathbb{Q}}(S)$, the theorem of the cube gives a canonical isomorphism of $\mathcal{O}_S$-modules

$$(x_1, y)^* P_{\mathbb{Q}} \otimes_{\mathcal{O}_S} (x_2, y)^* P_{\mathbb{Q}} = (x_1 + x_2, y)^* P_{\mathbb{Q}}\,. \tag{1.2.2}$$

This induces a morphism of schemes

$$(x_1, y)^* P^\times_{\mathbb{Q}} \times_S (x_2, y)^* P^\times_{\mathbb{Q}} \longrightarrow (x_1 + x_2, y)^* P^\times_{\mathbb{Q}}\,. \tag{1.2.3}$$

as follows. For any S-scheme T, and z_1 in $((x_1, y)^* P^\times_{\mathbb{Q}})(T)$ and z_2 in $((x_2, y)^* P^\times_{\mathbb{Q}})(T)$, we view z_1 and z_2 as nowhere vanishing sections of the invertible $\mathcal{O}_T$-modules $(x_1, y)^* P_{\mathbb{Q}}$ and $(x_2, y)^* P_{\mathbb{Q}}$. The tensor product of these two then gives an element of $((x_1+x_2, y)^* P^\times_{\mathbb{Q}})(T)$. This gives $P^\times_{\mathbb{Q}} \to J^\vee_{\mathbb{Q}}$ the structure of a commutative group scheme, which is an extension

of $J_{\mathbb{Q}}$ by $\mathbb{G}_{\mathrm{m}}$, over the base $J^{\vee}_{\mathbb{Q}}$. We denote this group law, and the one on $J_{\mathbb{Q}} \times J^{\vee}_{\mathbb{Q}}$, as

$$\begin{array}{ccc} (z_1, z_2) & \longmapsto & z_1 +_1 z_2 \\ \downarrow & & \downarrow \\ ((x_1, y), (x_2, y)) & \longmapsto & (x_1, y) +_1 (x_2, y) = (x_1 + x_2, y)\,. \end{array} \tag{1.2.4}$$

In the same way, $P^{\times}_{\mathbb{Q}} \to J_{\mathbb{Q}}$ has a group law $+_2$ that makes it an extension of $J^{\vee}_{\mathbb{Q}}$ by $\mathbb{G}_{\mathrm{m}}$ over the base $J_{\mathbb{Q}}$. In this way, $P^{\times}_{\mathbb{Q}}$ is both the universal extension of $J_{\mathbb{Q}}$ by $\mathbb{G}_{\mathrm{m}}$ and the universal extension of $J^{\vee}_{\mathbb{Q}}$ by $\mathbb{G}_{\mathrm{m}}$. The final ingredient of the notion of biextension is that the two partial group laws are compatible in the following sense. For any $\mathbb{Q}$-scheme S, for x_1 and x_2 in $J_{\mathbb{Q}}(S)$, y_1 and y_2 in $J^{\vee}_{\mathbb{Q}}(S)$, and, for all i and j in $\{1, 2\}$, $z_{i,j}$ in $((x_i, y_j)^* P^{\times}_{\mathbb{Q}})(S)$, we have

$$\begin{array}{ccc} (z_{1,1} +_1 z_{2,1}) +_2 (z_{1,2} +_1 z_{2,2}) & = & (z_{1,1} +_2 z_{1,2}) +_1 (z_{2,1} +_2 z_{2,2}) \\ \downarrow & & \downarrow \\ (x_1 + x_2, y_1) +_2 (x_1 + x_2, y_2) & = & (x_1, y_1 + y_2) +_1 (x_2, y_1 + y_2) \end{array} \tag{1.2.5}$$

with the equality in the upper line taking place in $((x_1 + x_2, y_1 + y_2)^* P^{\times}_{\mathbb{Q}})(S)$.

Now we extend the geometry above over $\mathbb{Z}$. We denote by J^0 the fibrewise connected component of 0 in J, which is an open subgroup scheme of J, and by Φ the quotient J/J^0, which is an étale (not necessarily separated) group scheme over $\mathbb{Z}$, with finite fibres, supported on $\mathbb{Z}/n\mathbb{Z}$. Similarly, we let $J^{\vee 0}$ be the fibrewise connected component of $J^{\vee}$. Theorem 7.1, in Exposé VIII of [91] gives that $P^{\times}_{\mathbb{Q}}$ extends uniquely to a $\mathbb{G}_{\mathrm{m}}$-biextension

$$P^{\times} \longrightarrow J \times J^{\vee 0} \tag{1.2.6}$$

(Grothendieck's pairing on component groups is the obstruction to the existence of such an extension). Note that in this case the existence and the uniqueness follow directly from the requirement of extending the rigidification on $J_{\mathbb{Q}} \times \{0\}$. For details see Section 1.6.7.

Our base point $b \in C(\mathbb{Z})$ gives an embedding $j_b \colon C_{\mathbb{Q}} \to J_{\mathbb{Q}}$, which sends, functorially in $\mathbb{Q}$-schemes S, an element $c \in C_{\mathbb{Q}}(S)$ to the class of the invertible $\mathcal{O}_{C_S}$-module $\mathcal{O}_{C_S}(c - b)$. Then j_b extends uniquely to a morphism

$$j_b \colon C^{\mathrm{sm}} \longrightarrow J \tag{1.2.7}$$

where C^{sm} is the open subscheme of C consisting of points at which C is smooth over $\mathbb{Z}$. Note that $C_{\mathbb{Q}}(\mathbb{Q}) = C(\mathbb{Z}) = C^{\mathrm{sm}}(\mathbb{Z})$.

Our next step is to lift j_b, at least on certain opens of C^{sm}, to a morphism to a $\mathbb{G}_{\mathrm{m}}^{\rho-1}$-torsor over J, where ρ is the rank of the free $\mathbb{Z}$-module $\mathrm{Hom}(J_{\mathbb{Q}}, J^{\vee}_{\mathbb{Q}})^+$, the $\mathbb{Z}$-module of

self-dual morphisms from $J_{\mathbb{Q}}$ to $J^{\vee}_{\mathbb{Q}}$. This torsor will be the product of pullbacks of $P^{\times}$ via morphisms

$$(\mathrm{id}, m\cdot \circ \mathrm{tr}_c \circ f)\colon J \to J \times J^{\vee 0}\,, \tag{1.2.8}$$

with $f\colon J \to J^{\vee}$ a morphism of group schemes, $c \in J^{\vee}(\mathbb{Z})$, tr_c the translation by c, m the least common multiple of the exponents of all $\Phi(\overline{\mathbb{F}}_p)$ with p ranging over all primes, and $m\cdot$ the multiplication by m map on $J^{\vee}$. For such a map $m\cdot\circ\mathrm{tr}_c\circ f$, $j_b\colon C_{\mathbb{Q}} \to J_{\mathbb{Q}}$ can be lifted to $(\mathrm{id}, m\cdot\circ\mathrm{tr}_c\circ f)^*P^{\times}_{\mathbb{Q}}$ if and only if $j_b^*(\mathrm{id}, m\cdot\circ\mathrm{tr}_c\circ f)^*P^{\times}_{\mathbb{Q}}$ is trivial. The degree of this $\mathbb{G}_{\mathrm{m}}$-torsor on $C_{\mathbb{Q}}$ is minus the trace of $\lambda^{-1}\circ m\cdot\circ(f+f^{\vee})$ acting on $\mathrm{H}_1(J(\mathbb{C}),\mathbb{Z})$. For example, for $f=\lambda$ the degree is $-4mg$. Note that $j_b\colon C_{\mathbb{Q}} \to J_{\mathbb{Q}}$ induces

$$j_b^* = -\lambda^{-1}\colon J^{\vee}_{\mathbb{Q}} \to J_{\mathbb{Q}}\,, \tag{1.2.9}$$

(see [76], Propositions 2.7.9 and 2.7.10). This implies that for f such that this degree is zero, there is a unique c such that $j_b^*(\mathrm{id},\mathrm{tr}_c\circ f)^*P^{\times}_{\mathbb{Q}}$ is trivial on $C_{\mathbb{Q}}$, and hence also its mth power $j_b^*(\mathrm{id}, m\cdot\circ\mathrm{tr}_c\circ f)^*P^{\times}_{\mathbb{Q}}$.

The map

$$\mathrm{Hom}(J_{\mathbb{Q}}, J^{\vee}_{\mathbb{Q}}) \longrightarrow \mathrm{Pic}(J_{\mathbb{Q}}) \longrightarrow \mathrm{NS}_{J_{\mathbb{Q}}/\mathbb{Q}}(\mathbb{Q}) = \mathrm{Hom}(J_{\mathbb{Q}}, J^{\vee}_{\mathbb{Q}})^{+} \tag{1.2.10}$$

sending f to the class of $(\mathrm{id}, f)^*P_{\mathbb{Q}}$ sends f to $f+f^{\vee}$, hence its kernel is $\mathrm{Hom}(J_{\mathbb{Q}}, J^{\vee}_{\mathbb{Q}})^{-}$, the group of antisymmetric morphisms. But actually, for f antisymmetric, its image in $\mathrm{Pic}(J_{\mathbb{Q}})$ is already zero (see for example [16] and the references therein). Hence the image of $\mathrm{Hom}(J_{\mathbb{Q}}, J^{\vee}_{\mathbb{Q}})$ in $\mathrm{Pic}(J_{\mathbb{Q}})$ is free of rank ρ, and its subgroup of classes with degree zero on $C_{\mathbb{Q}}$ is free of rank $\rho-1$. Let $f_1,\dots,f_{\rho-1}$ be elements of $\mathrm{Hom}(J_{\mathbb{Q}}, J^{\vee}_{\mathbb{Q}})$ whose images in $\mathrm{Pic}(J_{\mathbb{Q}})$ form a basis of this subgroup, and let $c_1,\dots,c_{\rho-1}$ be the corresponding elements of $J^{\vee}(\mathbb{Z})$.

By construction, for each i, the morphism $j_b\colon C_{\mathbb{Q}} \to J_{\mathbb{Q}}$ lifts to $(\mathrm{id}, m\cdot\circ\mathrm{tr}_{c_i}\circ f_i)^*P^{\times}_{\mathbb{Q}}$, unique up to $\mathbb{Q}^{\times}$. Now we spread this out over $\mathbb{Z}$, to open subschemes U of C^{sm} obtained by removing, for each q dividing n, all but one irreducible components of $C^{\mathrm{sm}}_{\mathbb{F}_q}$, with the remaining irreducible component geometrically irreducible. For such a U, the morphism $\mathrm{Pic}(U) \to \mathrm{Pic}(C_{\mathbb{Q}})$ is an isomorphism, and $\mathcal{O}_C(U) = \mathbb{Z}$, thus, for each i, there is a lift

$$\begin{array}{ccc} & & (\mathrm{id}, m\cdot\circ\mathrm{tr}_{c_i}\circ f_i)^*P^{\times} \\ & \overset{\widetilde{j_b}}{\nearrow} & \big\downarrow \\ U & \xrightarrow[j_b]{} & J \end{array} \tag{1.2.11}$$

unique up to $\mathbb{Z}^{\times} = \{1,-1\}$.

At this point we can explain the strategy of our approach to the quadratic Chabauty method. Let T be the $\mathbb{G}_{\mathrm{m}}^{\rho-1}$-torsor on J obtained by taking the product of all the $\mathbb{G}_{\mathrm{m}}$-torsors $T_i := (\mathrm{id}, m\cdot \circ \mathrm{tr}_{c_i} \circ f_i)^* P^\times$:

$$\begin{array}{ccccc} & & T & \longrightarrow & P^{\times,\rho-1} \\ & \overset{\widetilde{j_b}}{\nearrow} & \downarrow & & \downarrow \\ U & \xrightarrow{j_b} & J & \xrightarrow{(\mathrm{id},m\cdot\circ\mathrm{tr}_{c_i}\circ f_i)_i} & J\times (J^{\vee 0})^{\rho-1}. \end{array} \tag{1.2.12}$$

Then each $c \in C_{\mathbb{Q}}(\mathbb{Q}) = C^{\mathrm{sm}}(\mathbb{Z})$ lies in one of the finitely many $U(\mathbb{Z})$'s. For each U, we have a lift $\widetilde{j_b}\colon U \to T$, and, for each prime number p, $\widetilde{j_b}(U(\mathbb{Z}))$ is contained in the intersection, in $T(\mathbb{Z}_p)$, of $\widetilde{j_b}(U(\mathbb{Z}_p))$ and the closure $\overline{T(\mathbb{Z})}$ of $T(\mathbb{Z})$ in $T(\mathbb{Z}_p)$ with the p-adic topology. Of course, one expects this closure to be of dimension at most $r := \mathrm{rank}(J(\mathbb{Q}))$, and therefore one expects this method to be successful if $r < g + \rho - 1$, the dimension of $T(\mathbb{Z}_p)$. The next two sections make this strategy precise, giving first the necessary p-adic formal and analytic geometry, and then the description of $\overline{T(\mathbb{Z})}$ as a finite disjoint union of images of $\mathbb{Z}_p^r$ under maps constructed from the biextension structure.

1.3 From algebraic geometry to formal geometry

Let p be a prime number. Given X a smooth scheme of relative dimension d over $\mathbb{Z}_p$ and $x \in X(\mathbb{F}_p)$ let us describe the set $X(\mathbb{Z}_p)_x$ of elements of $X(\mathbb{Z}_p)$ whose image in $X(\mathbb{F}_p)$ is x. The smoothness implies that the maximal ideal of $\mathcal{O}_{X,x}$ is generated by p together with d other elements $t_1, \ldots, t_d$. In this case we call $p, t_1, \ldots, t_d$ *parameters at* x; if moreover $y \in X(\mathbb{Z}_p)_x$ is a lift of x such that $t_1(y) = \ldots = t_d(y) = 0$ then we say that the t_i's are *parameters at* y. The t_i can be evaluated on all the points in $X(\mathbb{Z}_p)_x$, inducing a bijection $t := (t_1, \ldots, t_d)\colon X(\mathbb{Z}_p)_x \to (p\mathbb{Z}_p)^d$. We get a bijection

$$\tilde{t} := (\tilde{t}_1, \ldots, \tilde{t}_d) = \left(\frac{t_1}{p}, \ldots, \frac{t_d}{p}\right) : X(\mathbb{Z}_p)_x \xrightarrow{\sim} \mathbb{Z}_p^d. \tag{1.3.1}$$

This bijection can be geometrically interpreted as follows. Let $\pi\colon \widetilde{X}_x \to X$ denote the blow up of X in x. By shrinking X, X is affine and the t_i are regular on X, $t\colon X \to \mathbb{A}^d_{\mathbb{Z}_p}$ is etale, and $t^{-1}\{0_{\mathbb{F}_p}\} = \{x\}$. Then $\pi\colon \widetilde{X}_x \to X$ is the pull back of the blow up of $\mathbb{A}^d_{\mathbb{Z}_p}$ at the origin over $\mathbb{F}_p$. The affine open part $\widetilde{X}^p_x$ of $\widetilde{X}_x$ where p generates the image of the ideal m_x of x is the pullback of the corresponding open part of the blow up of $\mathbb{A}^d_{\mathbb{Z}_p}$, which is the multiplication by p morphism $\mathbb{A}^d_{\mathbb{Z}_p} \to \mathbb{A}^d_{\mathbb{Z}_p}$ that corresponds to $\mathbb{Z}_p[t_1, \ldots, t_d] \to \mathbb{Z}_p[\tilde{t}_1, \ldots, \tilde{t}_d]$ with $t_i \mapsto p\tilde{t}_i$. It follows that the p-adic completion $\mathcal{O}(\widetilde{X}^p_x)^{\wedge_p}$ of $\mathcal{O}(\widetilde{X}^p_x)$ is the p-adic completion $\mathbb{Z}_p\langle\tilde{t}_1, \ldots, \tilde{t}_d\rangle$ of $\mathbb{Z}_p[\tilde{t}_1, \ldots, \tilde{t}_d]$. Explicitly,

we have

$$\mathbb{Z}_p\langle \tilde{t}_1, \dots, \tilde{t}_d\rangle = \left\{ \sum_{I\in\mathbb{N}^d} a_I \tilde{t}^I \in \mathbb{Z}_p[[\tilde{t}_1, \dots, \tilde{t}_d]] : \forall n \geq 0,\ \forall^{\text{almost}} I,\ v_p(a_I) \geq n \right\}. \tag{1.3.2}$$

With these definitions, we have

$$\begin{aligned} X(\mathbb{Z}_p)_x = \widetilde{X}^p_x(\mathbb{Z}_p) &= \mathrm{Hom}(\mathbb{Z}_p\langle \tilde{t}_1, \dots, \tilde{t}_d\rangle, \mathbb{Z}_p) = \mathbb{A}^d(\mathbb{Z}_p)\,, \\ (\widetilde{X}^p_x)_{\mathbb{F}_p} &= \mathrm{Spec}(\mathbb{F}_p[\tilde{t}_1, \dots, \tilde{t}_d]). \end{aligned} \tag{1.3.3}$$

The affine space $(\widetilde{X}^p_x)_{\mathbb{F}_p}$ is canonically a torsor under the tangent space of $X_{\mathbb{F}_p}$ at x.

This construction is functorial. Let Y be a smooth $\mathbb{Z}_p$-scheme, $f\colon X \to Y$ a morphism over $\mathbb{Z}_p$, and $y := f(x) \in Y(\mathbb{F}_p)$. Then the ideal in $\mathcal{O}_{\widetilde{X}^p_x}$ generated by the image of $m_{f(x)}$ is generated by p. That gives us a morphism $\widetilde{X}^p_x \to \widetilde{Y}^p_{f(x)}$, and then a morphism from $\mathcal{O}(\widetilde{Y}^p_{f(x)})^{\wedge_p}$ to $\mathcal{O}(\widetilde{X}^p_x)^{\wedge_p}$. Reduction mod p then gives a morphism $(\widetilde{X}^p_x)_{\mathbb{F}_p} \to (\widetilde{Y}^p_{f(x)})_{\mathbb{F}_p}$, the tangent map of f at x, up to a translation.

If this tangent map is injective, and d_x and d_y denote the dimensions of $X_{\mathbb{F}_p}$ at x and of $Y_{\mathbb{F}_p}$ at y, then there are $t_1, \dots, t_{d_y}$ in $\mathcal{O}_{Y,y}$ such that $p, t_1, \dots, t_{d_y}$ are parameters at y, and such that $t_{d_x+1}, \dots, t_{d_y}$ generate the kernel of $\mathcal{O}_{Y,y} \to \mathcal{O}_{X,x}$. Then the images in $\mathcal{O}_{X,x}$ of $p, t_1, \dots, t_{d_x}$ are parameters at x, and $\mathcal{O}(\widetilde{Y}^p_{f(x)})^{\wedge_p} \to \mathcal{O}(\widetilde{X}^p_x)^{\wedge_p}$ is $\mathbb{Z}_p\langle \tilde{t}_1, \dots, \tilde{t}_{d_y}\rangle \to \mathbb{Z}_p\langle \tilde{t}_1, \dots, \tilde{t}_{d_x}\rangle$, with kernel generated by $\tilde{t}_{d_x+1}, \dots, \tilde{t}_{d_y}$.

1.4 Integral points, closure and finiteness

Let us now return to our original problem. The notation $U, J, T, j_b, \widetilde{j_b}, r, \rho$ is as at the end of Section 1.2. Let $c = (c_1, \dots, c_{\rho-1}) \in J^{\vee,\rho-1}(\mathbb{Z})$, let $f = (f_1, \dots, f_{\rho-1})\colon J \to J^{\vee,\rho-1}$. We assume moreover that p does not divide n (n as in the start of Section 1.2) and that $p > 2$ (for $p = 2$ everything that follows can probably be adapted by working with residue polydiscs modulo 4).

Let u be in $U(\mathbb{F}_p)$, and $t := \widetilde{j_b}(u)$. We want a description of the closure $\overline{T(\mathbb{Z})_t}$ of $T(\mathbb{Z})_t$ in $T(\mathbb{Z}_p)_t$. Using the biextension structure of $P^\times$, we will produce, for each element of $J(\mathbb{Z})_{j_b(u)}$, an element of $T(\mathbb{Z})$ over it. Not all of these points are in $T(\mathbb{Z})_t$, but we will then produce a subset of $T(\mathbb{Z})_t$ whose closure is $\overline{T(\mathbb{Z})_t}$.

If $T(\mathbb{Z})_t$ is empty then $\overline{T(\mathbb{Z})_t}$ is empty, too. So we assume that we have an element $\widetilde{t}$ in $T(\mathbb{Z})_t$ and we denote $x_{\widetilde{t}} \in J(\mathbb{Z})$ the projection of $\widetilde{t}$. We denote by $P^{\times,\rho-1}$ the product over $J \times (J^{\vee 0})^{\rho-1}$ of the $\rho-1$ $\mathbb{G}_{\mathrm{m}}$-torsors obtained by pullback of $P^\times$ via the projections to $J \times J^{\vee 0}$; it is a biextension of J and $(J^{\vee 0})^{\rho-1}$ by $\mathbb{G}_{\mathrm{m}}^{\rho-1}$, and $T = (\mathrm{id}, m\cdot\circ \mathrm{tr}_c \circ f)^* P^{\times,\rho-1}$. We choose a basis $x_1, \dots, x_r$ of the free $\mathbb{Z}$-module $J(\mathbb{Z})_0$, the kernel of $J(\mathbb{Z}) \to J(\mathbb{F}_p)$.

For each $i, j \in \{1, \dots, r\}$ we choose $P_{i,j}$, $R_{i,\widetilde{t}}$, and $S_{\widetilde{t},j}$ in $P^{\times,\rho-1}(\mathbb{Z})$ whose images in $(J \times (J^{\vee 0})^{\rho-1})(\mathbb{Z})$ are $(x_i, f(mx_j))$, $(x_i, (m\cdot \circ \mathrm{tr}_c \circ f)(x_{\widetilde{t}}))$ and $(x_{\widetilde{t}}, f(mx_j))$:

(1.4.1)

$$\begin{array}{cccc} P_{i,j} & R_{i,\widetilde{t}} & S_{\widetilde{t},j} & P^{\times,\rho-1} \\ \big\downarrow & \big\downarrow & \big\downarrow & \big\downarrow \\ (x_i, f(mx_j)) & (x_i, (m\cdot \circ \mathrm{tr}_c \circ f)(x_{\widetilde{t}})) & (x_{\widetilde{t}}, f(mx_j)) & J \times (J^{\vee 0})^{\rho-1}\,. \end{array}$$

For each such choice there are $2^{\rho-1}$ possibilities.

For each $\nu \in \mathbb{Z}^r$ we use the biextension structure on $P^{\times,\rho-1} \to J \times (J^{\vee 0})^{\rho-1}$ to define the following points in $P^{\times,\rho-1}(\mathbb{Z})$, with specified images in $(J \times (J^{\vee 0})^{\rho-1})(\mathbb{Z})$:

(1.4.2)

$$\begin{array}{cc} A_{\widetilde{t}}(\nu) = \sum_{j=1}^{r}{}_2\, \nu_j \cdot_2 S_{\widetilde{t},j} & B_{\widetilde{t}}(\nu) = \sum_{i=1}^{r}{}_1\, \nu_i \cdot_1 R_{i,\widetilde{t}} \\ \big\downarrow & \big\downarrow \\ \left(x_{\widetilde{t}}, \sum_{i=1}^{r} \nu_i f(mx_i)\right) & \left(\sum_{i=1}^{r} \nu_i x_i\,, (m\cdot \circ \mathrm{tr}_c \circ f)(x_{\widetilde{t}})\right) \end{array}$$

(1.4.3)

$$\begin{array}{c} C(\nu) = \sum_{i=1}^{r}{}_1\, \nu_i \cdot_1 \left(\sum_{j=1}^{r}{}_2\, \nu_j \cdot_2 P_{i,j}\right) \\ \big\downarrow \\ \left(\sum_{i=1}^{r} \nu_i x_i\,, \sum_{i=1}^{r} \nu_i f(mx_i)\right) \end{array}$$

where $\sum_1$ and $\cdot_1$ denote iterations of the first partial group law $+_1$ as in (1.2.4), and analogously for the second group law. We define, for all $\nu \in \mathbb{Z}^r$,

$$D_{\widetilde{t}}(\nu) := \big(C(\nu) +_2 B_{\widetilde{t}}(\nu)\big) +_1 \big(A_{\widetilde{t}}(\nu) +_2 \widetilde{t}\big) \in P^{\times,\rho-1}(\mathbb{Z})\,, \tag{1.4.4}$$

which is mapped to

$$\left(x_{\widetilde{t}} + \sum_{i=1}^{r} \nu_i x_i, (m\cdot \circ \mathrm{tr}_c \circ f)\left(x_{\widetilde{t}} + \sum_{i=1}^{r} \nu_i x_i\right)\right) \in \big(J \times (J^{\vee 0})^{\rho-1}\big)(\mathbb{Z})\,. \tag{1.4.5}$$

Hence $D_{\widetilde{t}}(\nu)$ is in $T(\mathbb{Z})$, and its image in $J(\mathbb{F}_p)$ is $j_b(u)$. We do not know its image in $T(\mathbb{F}_p)$.

We claim that for ν in $(p-1)\mathbb{Z}^r$, $D_{\widetilde{t}}(\nu)$ is in $T(\mathbb{Z})_t$. Let ν' be in $\mathbb{Z}^r$ and let $\nu = (p-1)\nu'$. Then, in the trivial $\mathbb{F}_p^{\times,\rho-1}$-torsor $P^{\times,\rho-1}(j_b(u),0)$, on which $+_2$ is the group law, we have:

$$A_{\widetilde{t}}(\nu) = (p-1)\cdot_2 A_{\widetilde{t}}(\nu') = 1 \quad \text{in } \mathbb{F}_p^{\times,\rho-1}. \tag{1.4.6}$$

Similarly, in $P^{\times,\rho-1}(0,(m\cdot\circ\,\mathrm{tr}_c\circ f)(j_b(u))) = \mathbb{F}_p^{\times,\rho-1}$, we have $B_{\widetilde{t}}(\nu) = 1$, and, similarly, in $P^{\times,\rho-1}(0,0) = \mathbb{F}_p^{\times,\rho-1}$, we have $C(\nu) = 1$. So, with apologies for the mix of additive and multiplicative notations, in $P^{\times,\rho-1}(\mathbb{F}_p)$ we have

$$D_{\widetilde{t}}(\nu) = (1 +_2 1) +_1 (1 +_2 t) = t\,, \tag{1.4.7}$$

mapping to the following element in $(J \times J^{\vee 0,\rho-1})(\mathbb{F}_p)$:

(1.4.8)
$$\begin{aligned}&((0,0) +_2 ((0,(m\cdot\circ\,\mathrm{tr}_c\circ f)(j_b(u))))) +_1 ((j_b(u),0) +_2 (j_b(u),(m\cdot\circ\,\mathrm{tr}_c\circ f)(j_b(u))))\\ &= (j_b(u),(m\cdot\circ\,\mathrm{tr}_c\circ f)(j_b(u)))\,.\end{aligned}$$

We have proved our claim that $D_{\widetilde{t}}(\nu) \in T(\mathbb{Z})_t$.

So we now have the map

$$\kappa_{\mathbb{Z}}\colon \mathbb{Z}^r \to T(\mathbb{Z})_t, \quad \nu \mapsto D_{\widetilde{t}}((p-1)\nu)\,. \tag{1.4.9}$$

The following theorem will be proved in Section 1.5.

Theorem 1.4.10. *Let $w_1,\dots,w_g$ be in $\mathcal{O}_{J,j_b(u)}$ such that together with p they form a system of parameters of $\mathcal{O}_{J,j_b(u)}$, and let $v_1,\dots,v_{\rho-1}$ be in $\mathcal{O}_{T,t}$ such that $p, w_1,\dots,w_g$, $v_1,\dots,v_{\rho-1}$ are parameters of $\mathcal{O}_{T,t}$. As in Section 1.3 these parameters, divided by p, give a bijection*

$$T(\mathbb{Z}_p)_t \longrightarrow \mathbb{Z}_p^{g+\rho-1}\,. \tag{1.4.10.1}$$

The composition of the map $\kappa_{\mathbb{Z}}$ with the map (1.4.10.1) is given by uniquely determined $\kappa_1,\dots,\kappa_{g+\rho-1}$ in $\mathcal{O}(\mathbb{A}^r_{\mathbb{Z}_p})^{\wedge_p} = \mathbb{Z}_p\langle z_1,\dots,z_r\rangle$. The images in $\mathbb{F}_p[z_1,\dots,z_r]$ of $\kappa_1,\dots,\kappa_g$ are of degree at most 1, and the images of $\kappa_{g+1},\dots,\kappa_{g+\rho-1}$ are of degree at most 2. The map $\kappa_{\mathbb{Z}}$ extends uniquely to the continuous map

$$\kappa = (\kappa_1,\dots,\kappa_{g+\rho-1})\colon \mathbb{A}^r(\mathbb{Z}_p) = \mathbb{Z}_p^r \longrightarrow T(\mathbb{Z}_p)_t\,. \tag{1.4.10.2}$$

and the image of κ is $\overline{T(\mathbb{Z})_t}$.

Now the moment has come to confront $U(\mathbb{Z}_p)_u$ with $\overline{T(\mathbb{Z})_t}$. We have $\widetilde{j_b}\colon U \to T$, whose tangent map (mod p) at u is injective (here we use that $C_{\mathbb{F}_p}$ is smooth over $\mathbb{F}_p$).

Then, as at the end of Section 1.3, $\widetilde{j_b}\colon \widetilde{U}_u^p \to \widetilde{T}_t^p$ is, after reduction mod p, an affine linear embedding of codimension $g+\rho-2$, $\widetilde{j_b}^*\colon \mathcal{O}(\widetilde{T}_t^p)^{\wedge_p} \to \mathcal{O}(\widetilde{U}_u^p)^{\wedge_p}$ is surjective and its kernel is generated by elements $F_1, \dots, F_{g+\rho-2}$, whose images in $\mathbb{F}_p \otimes \mathcal{O}(\widetilde{T}_t^p)$ are of degree at most 1, and such that $F_1, \dots, F_{g-1}$ are in $\mathcal{O}(\widetilde{J}^p_{j_b(u)})^{\wedge_p}$. The pullbacks $\kappa^* f_i$ are in $\mathbb{Z}_p\langle z_1, \dots, z_r\rangle$; let I be the ideal in $\mathbb{Z}_p\langle z_1, \dots, z_r\rangle$ generated by them, and let

$$A := \mathbb{Z}_p\langle z_1, \dots, z_r\rangle / I\,. \tag{1.4.11}$$

Then the elements of $\mathbb{Z}_p^r$ whose image is in $U(\mathbb{Z}_p)_u$ are zeros of I, hence morphisms of rings from A to $\mathbb{Z}_p$, and hence from the reduced quotient A_{red} to $\mathbb{Z}_p$.

Theorem 1.4.12. *For $i \in \{1, \dots, g+\rho-2\}$, let $\kappa^*\overline{F_i}$ be the image of $\kappa^* f_i$ in $\mathbb{F}_p[z_1, \dots, z_r]$, and let $\overline{I}$ be the ideal of $\mathbb{F}_p[z_1, \dots, z_r]$ generated by them. Then $\kappa^*\overline{F_1}, \dots, \kappa^*\overline{F_{g-1}}$ are of degree at most 1, and $\kappa^*\overline{F_g}, \dots, \kappa^*\overline{F_{g+\rho-2}}$ are of degree at most 2. Assume that $\overline{A} := A/pA = \mathbb{F}_p[z_1, \dots, z_r]/\overline{I}$ is finite. Then $\overline{A}$ is the product of its localisations $\overline{A}_m$ at its finitely many maximal ideals m. The sum of the $\dim_{\mathbb{F}_p} \overline{A}_m$ over the m such that $\overline{A}/m = \mathbb{F}_p$ is an upper bound for the number of elements of $\mathbb{Z}_p^r$ whose image under κ is in $U(\mathbb{Z}_p)_u$, and also an upper bound for the number of elements of $U(\mathbb{Z})$ with image u in $U(\mathbb{F}_p)$.*

Proof. As every $\overline{F_i}$ is of degree at most 1 in $w_1, \dots, w_g, v_1, \dots, v_{\rho-1}$, every $\kappa^*\overline{F_i}$ is an $\mathbb{F}_p$-linear combination of $\kappa_1, \dots, \kappa_{g+\rho-1}$, hence of degree at most 2. For $i < g$, $\overline{F_i}$ is a linear combination of $w_1, \dots, w_g$, and therefore $\kappa^*\overline{F_i}$ is of degree at most 1.

We claim that A is p-adically complete. More generally, let R be a noetherian ring that is J-adically complete for an ideal J, and let I be an ideal in R. The map from R/I to its J-adic completion $(R/I)^\wedge$ is injective ([3, Thm.10.17]). As J-adic completion is exact on finitely generated R-modules ([3, Prop.10.12]), it sends the surjection $R \to R/I$ to a surjection $R = R^\wedge \to (R/I)^\wedge$ (see [3, Prop.10.5] for the equality $R = R^\wedge$). It follows that $R/I \to (R/I)^\wedge$ is surjective.

Now we assume that $\overline{A}$ is finite. As A is p-adically complete, A is the limit of the system of its quotients by powers of p. These quotients are finite: for every $m \in \mathbb{Z}_{\geq 1}$, $A/p^{m+1}A$ is, as abelian group, an extension of A/pA by a quotient of $A/p^m A$. As $\mathbb{Z}_p$-module, A is generated by any lift of an $\mathbb{F}_p$-basis of $\overline{A}$. Hence A is finitely generated as $\mathbb{Z}_p$-module.

The set of elements of $\mathbb{Z}_p^r$ whose image under κ is in $U(\mathbb{Z}_p)$ is in bijection with the set of $\mathbb{Z}_p$-algebra morphisms $\mathrm{Hom}(A, \mathbb{Z}_p)$. As A is the product of its localisations A_m at its maximal ideals, $\mathrm{Hom}(A, \mathbb{Z}_p)$ is the disjoint union of the $\mathrm{Hom}(A_m, \mathbb{Z}_p)$. For each m, $\mathrm{Hom}(A_m, \mathbb{Z}_p)$ has at most $\mathrm{rank}_{\mathbb{Z}_p}(A_m)$ elements, and is empty if $\mathbb{F}_p \to A/m$ is not an isomorphism. This establishes the upper bound for the number of elements of $\mathbb{Z}_p^r$ whose

image under κ is in $U(\mathbb{Z}_p)$. By Theorem 1.4.10, the elements of $U(\mathbb{Z})$ with image u in $U(\mathbb{F}_p)$ are in $\overline{T(\mathbb{Z})_t}$, and therefore of the form $\kappa(x)$ with $x \in \mathbb{Z}_p^r$ such that $\kappa(x)$ is in $U(\mathbb{Z}_p)_u$. This establishes the upper bound for the number of elements of $U(\mathbb{Z})$ with image u in $U(\mathbb{F}_p)$. □

We include some remarks to explain how Theorem 1.4.12 can be used, and what we hope that it can do.

Remark 1.4.13. The polynomials $\kappa^*\overline{F_i}$ in Theorem 1.4.12 can be computed from the reduction $\mathbb{F}_p^r \to T(\mathbb{Z}/p^2\mathbb{Z})$ of $\kappa_{\mathbb{Z}}$ and (to get the $\overline{F_i}$) from $\widetilde{j_b}\colon U(\mathbb{Z}/p^2\mathbb{Z})_u \to T(\mathbb{Z}/p^2\mathbb{Z})_t$. For this, one does not need to treat T and J as schemes, one just computes with $\mathbb{Z}/p^2\mathbb{Z}$-valued points. Now assume that $r \leq g + \rho - 2$. If, for some prime p, the criterion in Theorem 1.4.12 fails (that is, $\overline{A}$ is not finite), then one can try the next prime. We hope (but also expect) that one quickly finds a prime p such that $\overline{A}$ is finite for every U and for every u in $U(\mathbb{F}_p)$ such that $\widetilde{j_b}(u)$ is in the image of $T(\mathbb{Z}) \to T(\mathbb{F}_p)$. By the way, note that our notation in Theorem 1.4.12 does not show the dependence on U and u of $\widetilde{j_b}$, $\kappa_{\mathbb{Z}}$, κ and the $\overline{F_i}$. Instead of varying p, one could also increase the p-adic precision, and then the result of Section 1.9.2 proves that one gets an upper bound for the number of elements of $U(\mathbb{Z})$.

Remark 1.4.14. If $r < g + \rho - 2$ then we think that it is likely (when varying p), for dimension reasons, unless something special happens as in [7] or Remark 8.9 of [8], that, for all $u \in U(\mathbb{F}_p)$, the upper bound in Theorem 1.4.12 for the number of elements of $U(\mathbb{Z})$ with image u in $U(\mathbb{F}_p)$ is sharp. For a precise conjecture in the context of Chabauty's method, see the "Strong Chabauty" Conjecture in [99].

Remark 1.4.15. Suppose that $r = g + \rho - 2$. Then we expect, for dimension reasons, that it is likely (when varying p) that, for some $u \in U(\mathbb{F}_p)$, the upper bound in Theorem 1.4.12 for the number of elements of $U(\mathbb{Z})$ with image u in $U(\mathbb{F}_p)$ is not sharp. Then, as in the classical Chabauty method, one must combine the information gotten from several primes, analogous to 'Mordell-Weil sieving'; see [79]. In our situation, this amounts to the following. Suppose that we are given a subset B of $U(\mathbb{Z})$ that we want to prove to be equal to $U(\mathbb{Z})$. Let B' be the complement in $U(\mathbb{Z})$ of B. For every prime $p > 2$ not dividing n, Theorem 1.4.12 gives, interpreting $\overline{A}$ as in the end of the proof of Theorem 1.4.12, a subset O_p of $J(\mathbb{Z})$, that is a union of cosets for the subgroup $p \cdot \ker(J(\mathbb{Z}) \to J(\mathbb{F}_p))$, that contains $j_b(B')$. Then one hopes that, taking a large enough finite set S of primes, the intersection of the O_p for p in S is empty.

1.5 Parametrisation of integral points, and power series

In this section we give a proof of Theorem 1.4.10. The main tools here are the formal logarithm and formal exponential of a commutative smooth group scheme over a $\mathbb{Q}$-algebra ([54], Theorem 1): they give us identities like $n{\cdot}g = \exp(n{\cdot}\log g)$ that allow us to extend the multiplication to elements n of $\mathbb{Z}_p$.

The evaluation map from $\mathbb{Z}_p\langle z_1,\dots,z_n\rangle$ to the set of maps $\mathbb{Z}_p^n \to \mathbb{Z}_p$ is injective (induction on n, non-zero elements of $\mathbb{Z}_p\langle z\rangle$ have only finitely many zeros in $\mathbb{Z}_p$).

We say that a map $f\colon \mathbb{Z}_p^n \to \mathbb{Z}_p^m$ is *given by integral convergent power series* if its coordinate functions are in $\mathbb{Z}_p\langle z_1,\dots,z_n\rangle = \mathcal{O}(\mathbb{A}^n_{\mathbb{Z}_p})^{\wedge_p}$. This property is stable under composition: composition of polynomials over $\mathbb{Z}/p^k\mathbb{Z}$ gives polynomials.

1.5.1 Logarithm and exponential

Let p be a prime number, and let G be a commutative group scheme, smooth of relative dimension d over a scheme S smooth over $\mathbb{Z}_p$, with unit section e in $G(S)$. For any s in $S(\mathbb{F}_p)$, $G(\mathbb{Z}_p)_{e(s)}$ is a group fibred over $S(\mathbb{Z}_p)_s$. The fibres have a natural $\mathbb{Z}_p$-module structure: $G(\mathbb{Z}_p)_{e(s)}$ is the limit of the $G(\mathbb{Z}/p^n\mathbb{Z})_{e(s)}$ ($n \geq 1$), $S(\mathbb{Z}_p)_s$ is the limit of the $S(\mathbb{Z}/p^n\mathbb{Z})_s$, and for each $n \geq 1$, the fibres of $G(\mathbb{Z}/p^n\mathbb{Z})_{e(s)} \to S(\mathbb{Z}/p^n\mathbb{Z})_s$ are commutative groups annihilated by p^{n-1}. Let $T_{G/S}$ be the relative (geometric) tangent bundle of G over S. Then its pullback $T_{G/S}(e)$ by e is a vector bundle on S of rank d.

Lemma 1.5.1.1. *In this situation, and with n the relative dimension of S over $\mathbb{Z}_p$, the formal logarithm and exponential of G base changed to $\mathbb{Q}\otimes\mathcal{O}_{S,s}$ converge to maps*

$$\log\colon \widetilde{G}^p_{e(s)}(\mathbb{Z}_p) = G(\mathbb{Z}_p)_{e(s)} \to (T_{G/S}(e))(\mathbb{Z}_p)_{0(s)}$$
$$\exp\colon \widetilde{T}_{G/S}(e)^p_{0(s)}(\mathbb{Z}_p) = (T_{G/S}(e))(\mathbb{Z}_p)_{0(s)} \to G(\mathbb{Z}_p)_{e(s)}\,,$$

that are each other's inverse and, after a choice of parameters for $G \to S$ at $e(s)$ as in (1.3.1), are given by $n{+}d$ elements of $\mathcal{O}(\widetilde{G}^p_{e(s)})^{\wedge_p}$ and $n{+}d$ elements of $\mathcal{O}(\widetilde{T}_{G/S}(e)^p_{0(s)})^{\wedge_p}$.

For a in $\mathbb{Z}_p$ and g in $G(\mathbb{Z}_p)_{e(s)}$ we have $a{\cdot}g = \exp(a{\cdot}\log g)$, and, after a choice of parameters for $G \to S$ at $e(s)$, this map $\mathbb{Z}_p \times G(\mathbb{Z}_p)_{e(s)} \to G(\mathbb{Z}_p)_{e(s)}$ is given by $n{+}d$ elements of $\mathcal{O}(\mathbb{A}^1_{\mathbb{Z}_p} \times_{\mathbb{Z}_p} \widetilde{G}^p_{e(s)})^{\wedge_p}$. The induced morphism $\mathbb{A}^1_{\mathbb{F}_p} \times (\widetilde{G}^p_{e(s)})_{\mathbb{F}_p} \to (\widetilde{G}^p_{e(s)})_{\mathbb{F}_p}$, where $(\widetilde{G}^p_{e(s)})_{\mathbb{F}_p}$ is viewed as the product of $T_{S_{\mathbb{F}_p}}(s)$ and $T_{G/S}(e(s))$, is a morphism over $T_{S_{\mathbb{F}_p}}(s)$, bilinear in $\mathbb{A}^1_{\mathbb{F}_p}$ and $T_{G/S}(e(s))$.

Proof. Let $t_1,\dots,t_n$ be in $\mathcal{O}_{S,s}$ such that $p, t_1,\dots,t_n$ are parameters at s. Then we have

a bijection

$$\tilde{t}\colon S(\mathbb{Z}_p)_s \to \mathbb{Z}_p^n, \quad a \mapsto p^{-1}\cdot(t_1(a),\dots,t_n(a))\,. \tag{1.5.1.2}$$

Similarly, let $x_1,\dots,x_d$ be generators for the ideal $I_{e(s)}$ of e in $\mathcal{O}_{G,e(s)}$. Then p, the t_i and the x_j together are parameters for $\mathcal{O}_{G,e(s)}$, and give the bijection

$$(t,x)^{\sim}\colon G(\mathbb{Z}_p)_{e(s)} \to \mathbb{Z}_p^{n+d}\,, \quad b \mapsto p^{-1}\cdot(t_1(b),\dots,x_d(b))\,. \tag{1.5.1.3}$$

The $\mathrm{d}x_i$ form an $\mathcal{O}_{S,s}$-basis of $\Omega^1_{G/S}(e)_s$, and so give translation invariant differentials ω_i on $G_{\mathcal{O}_{S,s}}$. As G is commutative, for all i, $\mathrm{d}\omega_i = 0$ ([54], Proposition 1.3). We also have the dual $\mathcal{O}_{S,s}$-basis ∂_i of $T_{G/S}(e)$ and the bijection

(1.5.1.4)
$$(t,x)^{\sim}\colon (T_{G/S}(e))(\mathbb{Z}_p)_{0(s)} \to \mathbb{Z}_p^{n+d}\,, \quad (a,\sum_i v_i\partial_i) \mapsto p^{-1}\cdot(t_1(a),\dots,t_n(a),v_1,\dots,v_d)\,.$$

Then log is given by elements $\log_i$ in $(\mathbb{Q}\otimes\mathcal{O}_{S,s})[[x_1,\dots,x_d]]$ whose constant term is 0, uniquely determined (Proposition 1.1 in [54]) by the equality

$$\mathrm{d}\log_i = \omega_i\,, \quad \text{in } \oplus_j \mathcal{O}_{S,s}[[x_1,\dots,x_d]]\cdot\mathrm{d}x_j\,. \tag{1.5.1.5}$$

Hence the formula from calculus, $\log_i(x) - \log_i(0) = \int_0^1 (t\mapsto tx)^*\omega_i$, gives us that, with

$$\log_i = \sum_{J\neq 0} \log_{i,J}\, x^J \quad \text{and} \quad \log_{i,J} \in (\mathbb{Q}\otimes\mathcal{O}_{S,s})\,, \tag{1.5.1.6}$$

we have, for all i and J, with $|J|$ denoting the total degree of x^J,

$$|J|\cdot\log_{i,J} \in \mathcal{O}_{S,s}\,. \tag{1.5.1.7}$$

The claim about convergence and definition of $\log\colon G(\mathbb{Z}_p)_{e(s)} \to (T_{G/S}(e))(\mathbb{Z}_p)_{0(s)}$, is now equivalent to having an analytic bijection $\mathbb{Z}_p^{n+d} \to \mathbb{Z}_p^{n+d}$ given by

$$\begin{array}{ccc} G(\mathbb{Z}_p)_{e(s)} & \xrightarrow{\quad ? \quad} & (T_{G/S}(e))(\mathbb{Z}_p)_{0(s)} \\ \downarrow{\scriptstyle (t,x)^{\sim}} & & \downarrow{\scriptstyle (t,x)^{\sim}} \\ \mathbb{Z}_p^{n+d} & \xrightarrow{\quad ? \quad} & \mathbb{Z}_p^{n+d} \end{array} \tag{1.5.1.8}$$

$$(a,b) \xmapsto{\quad ? \quad} \left(a, p^{-1}\cdot\left(\textstyle\sum_{J\neq 0}\log_{i,J}(\tilde{t}^{-1}(a))(pb)^J\right)_i\right)\,.$$

We have, for each i,

$$p^{-1}\cdot\sum_{J\neq 0}\log_{i,J}(\tilde{t}^{-1}(a))(pb)^J = \sum_{J\neq 0}\frac{p^{|J|-1}}{|J|}(|J|\log_{i,J})(\tilde{t}^{-1}(a))b^J\,. \tag{1.5.1.9}$$

For each i, this expression is an element of $\mathbb{Z}_p\langle \tilde{t}_1, \dots, \tilde{t}_n, \tilde{x}_1, \dots, \tilde{x}_d\rangle = \mathcal{O}(\widetilde{G}^p_{e(s)})^{\wedge_p}$, even when $p = 2$, because for each J, $|J| \log_{i,J}$ is in $\mathcal{O}_{S,s}$, which is contained in $\mathbb{Z}_p\langle \tilde{t}_1, \dots, \tilde{t}_n\rangle$, and the function $\mathbb{Z}_{\geq 1} \to \mathbb{Q}_p$, $r \mapsto p^{r-1}/r$ has values in $\mathbb{Z}_p$ and converges to 0. The existence and analyticity of log is now proved (even for $p = 2$). As $p > 2$, the image of (1.5.1.9) in $\mathbb{F}_p \otimes \mathcal{O}(\widetilde{G}^p_{e(s)})^{\wedge_p}$ is $\tilde{x}_i$, and on the first n coordinates, log is the identity, so, by applying Hensel modulo powers of p, log is invertible, and the inverse is also given by $n + d$ elements of $\mathcal{O}(\widetilde{T}_{G/S}(e)^p_{0(s)})^{\wedge_p}$.

The function $\mathbb{Z}_p \times G(\mathbb{Z}_p)_{e(s)} \to G(\mathbb{Z}_p)_{e(s)}$, $(a, g) \mapsto \exp(a \cdot \log g)$ is a composition of maps given by integral convergent power series, hence it is also of that form. □

1.5.2 Parametrisation by power series

The notation and assumptions are as in the beginning of Section 1.4, in particular, $p > 2$ and T is as defined in (1.2.12). We have a t in $T(\mathbb{F}_p)$, with image $j_b(u)$ in $J(\mathbb{F}_p)$, and a $\tilde{t}$ in $T(\mathbb{Z})$ lifting t. For every Q in $T(\mathbb{Z})$ mapping to $j_b(u)$ in $J(\mathbb{F}_p)$ there are unique $\varepsilon \in \mathbb{Z}^{\times,\rho-1}$ and $\nu \in \mathbb{Z}^r$ such that $Q = \varepsilon \cdot D_{\tilde{t}}(\nu)$: the image of Q in $J(\mathbb{Z})$ is in $J(\mathbb{Z})_{j_b(u)}$, hence differs from the image $x_{\tilde{t}}$ in $J(\mathbb{Z})$ of $\tilde{t}$ by an element of $J(\mathbb{Z})_0$ (with here $0 \in J(\mathbb{F}_p)$), $\sum_i \nu_i x_i$ for a unique $\nu \in \mathbb{Z}^r$, hence $D_{\tilde{t}}(\nu)$ and Q are in $T(\mathbb{Z})$ and have the same image in $J(\mathbb{Z})$, and that gives the unique ε. So we have a bijection

(1.5.2.1)
$$\mathbb{Z}^{\times,\rho-1} \times \mathbb{Z}^r \longrightarrow T(\mathbb{Z})_{j_b(u)} = \{Q \in T(\mathbb{Z}) : Q \mapsto j_b(u) \in J(\mathbb{F}_p)\}\,, \quad (\varepsilon, \nu) \mapsto \varepsilon \cdot D_{\tilde{t}}(\nu)\,.$$

But a problem that we are facing is that the map $\mathbb{Z}^r \to T(\mathbb{F}_p)_{j_b(u)}$ sending ν to the image of $D_{\tilde{t}}(\nu)$ depends on the (unknown) images of the $P_{i,j}$, $R_{i,\tilde{t}}$ and $S_{\tilde{t},j}$ from (1.4.1) in $P^{\times,\rho-1}(\mathbb{F}_p)$, and so we do not know for which ν and ε the point $\varepsilon \cdot D_{\tilde{t}}(\nu)$ is in $T(\mathbb{Z})_t$. Luckily we have the $\mathbb{Z}_p^{\times,\rho-1}$-action on $T(\mathbb{Z}_p)$. Using that $\mathbb{Z}_p^\times = \mathbb{F}_p^\times \times (1 + p\mathbb{Z}_p)$ we have $\mathbb{F}_p^{\times,\rho-1}$ acting on $T(\mathbb{Z}_p)_{j_b(u)}$, compatibly with the torsor structure on $T(\mathbb{F}_p)_{j_b(u)}$. So, for every ν in $\mathbb{Z}^r$ there is a unique $\xi(\nu)$ in $\mathbb{F}_p^{\times,\rho-1}$ such that $\xi(\nu) \cdot D_{\tilde{t}}(\nu)$ is in $T(\mathbb{Z}_p)_t$. We define

$$D'(\nu) := \xi(\nu) \cdot D_{\tilde{t}}(\nu)\,. \tag{1.5.2.2}$$

Then for all ν in $\mathbb{Z}^r$,

$$\kappa_{\mathbb{Z}}(\nu) = D_{\tilde{t}}((p-1) \cdot \nu) = D'((p-1) \cdot \nu)\,, \tag{1.5.2.3}$$

because $D_{\tilde{t}}((p-1) \cdot \nu)$ maps to t in $T(\mathbb{F}_p)$. Moreover for every Q in $T(\mathbb{Z})_t$ there is a unique $\nu \in \mathbb{Z}^r$ and a unique $\varepsilon \in \mathbb{Z}^{\times,\rho-1}$ such that $Q = \varepsilon \cdot D_{\tilde{t}}(\nu) = \xi(\nu) \cdot D_{\tilde{t}}(\nu) = D'(\nu)$. Hence

$$T(\mathbb{Z})_t \subset D'(\mathbb{Z}^r)\,. \tag{1.5.2.4}$$

The following lemma proves the existence and uniqueness of the κ_i of Theorem 1.4.10, and the claims on the degrees of the $\overline{\kappa}_i$.

Lemma 1.5.2.5. *After any choice of parameters of $\mathcal{O}_{T,t}$ as in Theorem 1.4.10, D' is given by elements $\kappa'_1, \dots, \kappa'_{g+\rho-1}$ of $\mathcal{O}(\mathbb{A}^r_{\mathbb{Z}_p})^{\wedge_p}$, and then $\kappa_{\mathbb{Z}}$ is given by $\kappa_1, \dots, \kappa_{g+\rho-1}$ with, for all $i \in \{1, \dots, g+\rho-1\}$ and all $a \in \mathbb{Z}_p^r$,*

$$\kappa_i(a) = \kappa'_i((p-1)a)\,.$$

For all i in $\{1, \dots, g+\rho-1\}$ we let $\overline{\kappa}'_i$ be the reduction mod p of κ'_j. Then $\overline{\kappa}'_1, \dots, \overline{\kappa}'_g$ are of degree at most 1, and the remaining $\overline{\kappa}'_j$ are of degree at most 2.

Proof. In order to get a formula for $D'(\nu)$, we introduce variants of the $P_{i,j}$, $R_{i,\widetilde{t}}$, and $S_{\widetilde{t},j}$ as follows. The images in $(J \times (J^{\vee 0})^{\rho-1})(\mathbb{F}_p)$ of these points are of the form $(0,*)$, $(0,*)$, and $(*,0)$, respectively. Hence the fibers over them of $P^{\times,\rho-1}$ are rigidified, that is, equal to $\mathbb{F}_p^{\times,\rho-1}$. We define their variants $P'_{i,j}$, $R'_{i,\widetilde{t}}$, and $S'_{\widetilde{t},j}$ in $P^{\times,\rho-1}(\mathbb{Z}_p)$ to be the unique elements in their orbits under $\mathbb{F}_p^{\times,\rho-1}$ whose images in $P^{\times,\rho-1}(\mathbb{F}_p)$ are equal to the element 1 in $\mathbb{F}_p^{\times,\rho-1}$. Replacing, in (1.4.2) and (1.4.3), these $P_{i,j}$, $R_{i,\widetilde{t}}$, and $S_{\widetilde{t},j}$ by $P'_{i,j}$, $R'_{i,\widetilde{t}}$, and $S'_{\widetilde{t},j}$ gives variants A', B' and C', and using these in (1.4.4) gives a variant $D'_{\widetilde{t}}(\nu)$ of 1.5.2.2.

Then, for all ν in $\mathbb{Z}^r$, $D'_{\widetilde{t}}(\nu)$ and $D'(\nu)$ (as in (1.5.2.2)) are equal, because both are in $P^{\times,\rho-1}(\mathbb{Z}_p)_t$, and in the same $\mathbb{F}_p^{\times,\rho-1}$-orbit. Hence we have, for all ν in $\mathbb{Z}^r$:

$$\begin{aligned}
A'(\nu) &= \sum_{j=1}^{r}{}_2\, \nu_j \cdot_2 S'_{\widetilde{t},j}\,, \quad B'(\nu) = \sum_{i=1}^{r}{}_1\, \nu_i \cdot_1 R'_{i,\widetilde{t}}, \\
C'(\nu) &= \sum_{i=1}^{r}{}_1\, \nu_i \cdot_1 \left(\sum_{j=1}^{r}{}_2\, \nu_j \cdot_2 P'_{i,j} \right), \\
D'(\nu) &= (C'(\nu) +_2 B'(\nu)) +_1 \left(A'(\nu) +_2 \widetilde{t}\right).
\end{aligned} \tag{1.5.2.6}$$

This shows how the map $\nu \mapsto D'(\nu)$ is built up from the two partial group laws $+_1$ and $+_2$ on $P^{\times,\rho-1}$, and the iterations $\cdot_1$ and $\cdot_2$. Lemma 1.5.1.1 gives that the iterations are given by integral convergent power series. The functoriality in Section 1.3 gives that the maps induced by $+_1$ and $+_2$ on residue polydisks are given by integral convergent power series. Stability under composition then gives that $\nu \mapsto D'(\nu)$ is given by elements $\kappa'_1, \dots, \kappa'_{g+\rho-1}$ of $\mathbb{Z}_p\langle z_1, \dots, z_r\rangle$.

We call the κ'_i the coordinate functions of the extension $D' \colon \mathbb{Z}_p^r \to T(\mathbb{Z}_p)_t = \mathbb{Z}_p^{g+\rho-1}$, and their images $\overline{\kappa}'_1, \dots, \overline{\kappa}'_{g+\rho-1}$ in $\mathbb{F}_p[z_1, \dots, z_r]$ the mod p coordinate functions, viewed as a morphism $\overline{D}'_{\mathbb{F}_p} \colon \mathbb{A}^r_{\mathbb{F}_p} \to \mathbb{A}^{g+\rho-1}_{\mathbb{F}_p}$.

The mod p coordinate functions of $A'\colon \mathbb{Z}_p^r \to P^{\times,\rho-1}(\mathbb{Z}_p) = \mathbb{Z}_p^{\rho g+\rho-1}$ (after choosing the necessary parameters) are all of degree at most 1. The same holds for B'. We define

$$C_2'\colon \mathbb{Z}^r \times \mathbb{Z}^r \longrightarrow P^{\times,\rho-1}(\mathbb{Z}_p), \quad C_2'(\nu,\mu) = \sum_{i=1}^{r}{}_1\, \nu_i \cdot_1 \left(\sum_{j=1}^{r}{}_2\, \mu_j \cdot_2 P'_{i,j} \right). \tag{1.5.2.7}$$

Then the mod p coordinate functions of C_2', elements of $\mathbb{F}_p[x_1,\dots,x_r,y_1,\dots,y_r]$, are linear in the x_i, and in the y_j. Hence of degree at most 2, and the same follows for the mod p coordinate functions of C'. However, as the first ρg parameters for $P^{\times,\rho-1}$ come from $J \times J^{\vee\rho-1}$, and the 1st and 2nd partial group laws there act on different factors, the first ρg mod p coordinate functions of C' are in fact linear. As D' is obtained by summing, using the partial group laws, the results of A', B' and C', we conclude that $\overline{\kappa}_1', \dots, \overline{\kappa}_g'$ are of degree at most 1, and the remaining $\overline{\kappa}_j$ are of degree at most 2. The same holds then for all $\overline{\kappa}_j$. □

1.5.3 The p-adic closure

We know from (1.5.2.3) that $\kappa_{\mathbb{Z}}(\mathbb{Z}^r) = D'((p-1)\mathbb{Z}^r)$. From (1.4.9) we know that $\kappa_{\mathbb{Z}}(\mathbb{Z}^r) \subset T(\mathbb{Z})_t$. From (1.5.2.4) we know that $T(\mathbb{Z})_t \subset D'(\mathbb{Z}^r)$. So together we have:

$$D'((p-1)\mathbb{Z}^r) = \kappa_{\mathbb{Z}}(\mathbb{Z}^r) \subset T(\mathbb{Z})_t \subset D'(\mathbb{Z}^r)\,. \tag{1.5.3.1}$$

We have extended D' to a continuous map $\mathbb{Z}_p^r \to T(\mathbb{Z}_p)_t$. As $\mathbb{Z}_p^r$ is compact, $D'(\mathbb{Z}_p^r)$ is closed in $T(\mathbb{Z}_p)_t$. As $\mathbb{Z}^r$ and $(p-1)\mathbb{Z}^r$ are dense in $\mathbb{Z}_p^r$, the closures of their images under D' are both equal to $D'(\mathbb{Z}_p^r)$, and equal to $\kappa(\mathbb{Z}_p^r)$. This finishes the proof of Theorem 1.4.10.

1.6 Explicit description of the Poincaré torsor

The aim of this section is to give explicit descriptions of the Poincaré torsor $P^{\times}$ on $J \times J^{\vee,0}$ and its partial group laws, to be used for doing computations when applying Theorem 1.4.12. The main results are as follows. Proposition 1.6.3.2 describes the fibre of P over a point of $J \times J^{\vee,0}$, say with values in $\mathbb{Z}/p^2\mathbb{Z}$ with p not dividing n or in $\mathbb{Z}[1/n]$, when the corresponding points of J and $J^{\vee,0}$ are given by a line bundle on C (over $\mathbb{Z}/p^2\mathbb{Z}$ or $\mathbb{Z}[1/n]$, and rigidified at b) and an effective relative Cartier divisor on C (over $\mathbb{Z}/p^2\mathbb{Z}$ or $\mathbb{Z}[1/n]$). It also translates the partial group laws of $P^{\times}$ in terms of such data. Lemma 1.6.4.8 shows how to deal with linear equivalence of divisors. Lemma 1.6.5.4 makes the symmetry of $P^{\times}$ explicit. Lemma 1.6.6.8 gives parametrisations

of residue polydisks of $P^\times(\mathbb{Z}/p^2\mathbb{Z})$, and Lemma 1.6.6.13 gives partial group laws on these residue polydisks. Proposition 1.6.8.7 describes the unique extension over $J \times J^{\vee,0}$ of the Poincaré torsor on $(J \times J^{\vee,0})_{\mathbb{Z}[1/n]}$, in terms of line bundles and divisors on C. Finally, Proposition 1.6.9.3 describes the fibres of P over $\mathbb{Z}$-points of $J \times J^{\vee,0}$.

In this article, we have chosen to use line bundles and divisors on curves for describing the jacobian and the Poincaré torsor. Another option is to use line bundles on curves and the determinant of coherent cohomology, as in Section 2 of [76]. We note that in Section 2, only the restriction of P to $J^0 \times J^{\vee,0}$ is treated, and moreover, under the assumption that C is nodal (that is, all fibres $C_{\mathbb{F}_p}$ are reduced and have only the mildest possible singularities). Another choice we have made is to develop the basic theory of norms of $\mathbb{G}_\mathrm{m}$-torsors under finite locally free morphisms in this article (Sections 1.6.1–1.6.2) and not to refer, for example, to EGA or SGA, because we think this is easier for the reader, and because this way we could adapt the definition directly to our use of it.

1.6.1 Norms

Let S be a scheme, $f\colon S' \to S$ be finite and locally free, say of rank n. Then $\mathcal{O}_{S'} = f_*\mathcal{O}_{S'}$ (we view $\mathcal{O}_{S'}$ as a sheaf on S) is an $\mathcal{O}_S$-algebra, locally free as $\mathcal{O}_S$-module of rank n, and $\mathcal{O}_{S'}^\times$ is a subsheaf of groups of the sheaf $\mathrm{GL}_{\mathcal{O}_S}(\mathcal{O}_{S'})$ of $\mathcal{O}_S$-linear automorphisms of $\mathcal{O}_{S'}$. Then the norm morphism is the composition

$$\mathcal{O}_{S'}^\times \hookrightarrow \mathrm{GL}_{\mathcal{O}_S}(\mathcal{O}_{S'}) \xrightarrow{\det} \mathcal{O}_S^\times, \qquad \text{with } \mathcal{O}_{S'}^\times \xrightarrow{\mathrm{Norm}_{S'/S}} \mathcal{O}_S^\times \tag{1.6.1.1}$$

For T an $\mathcal{O}_{S'}^\times$-torsor (triviality locally on S and S' are equivalent, from the equivalence with invertible $\mathcal{O}_{S'}$-modules), we let $\mathrm{Norm}_{S'/S}(T)$ be the $\mathcal{O}_S^\times$-torsor

$$\mathrm{Norm}_{S'/S}(T) := \mathcal{O}_S^\times \otimes_{\mathcal{O}_{S'}^\times} T = \left(\mathcal{O}_S^\times \times T\right)/\mathcal{O}_{S'}^\times, \tag{1.6.1.2}$$

with, for every open U of S, and every element $u \in \mathcal{O}_{S'}^\times(U)$, the action of u given by $(v,t) \mapsto (v\cdot\mathrm{Norm}_{S'/S}(u), u^{-1}\cdot t)$. This definition is functorial in T: a morphism $\phi\colon T_1 \to T_2$ induces a morphism $\mathrm{Norm}_{S'/S}(\phi)$. It is also functorial for cartesian diagrams $(S_2' \to S_2) \to (S_1' \to S_1)$.

For $U \subset S$ open, T an $\mathcal{O}_{S'}^\times$-torsor, and $t \in T(U)$, we have the isomorphism of $\mathcal{O}_{S'}^\times|_U$-torsors $\mathcal{O}_{S'}^\times|_U \to T|_U$ sending 1 to t. Functoriality gives $\mathrm{Norm}_{S'/S}(t)$ in $(\mathrm{Norm}_{S'/S}(T))(U)$, also denoted $1 \otimes t$.

The norm functor (1.6.1.2) is multiplicative:

$$\mathrm{Norm}_{S'/S}(T_1 \otimes_{\mathcal{O}_{S'}} T_2) = \mathrm{Norm}_{S'/S}(T_1) \otimes_{\mathcal{O}_S} \mathrm{Norm}_{S'/S}(T_2), \tag{1.6.1.3}$$

such that, if $U \subset S$ is open and t_1 and t_2 are in $T_1(U)$ and $T_2(U)$, then

$$\mathrm{Norm}_{S'/S}(t_1 \otimes t_2) \mapsto \mathrm{Norm}_{S'/S}(t_1) \otimes \mathrm{Norm}_{S'/S}(t_2)\,. \tag{1.6.1.4}$$

Let $\mathcal{L}$ be an invertible $\mathcal{O}_{S'}$-module; locally on S, it is free of rank 1 as $\mathcal{O}_{S'}$-module. This gives us the $\mathcal{O}_{S'}^{\times}$-torsor (on S) $\mathrm{Isom}_{\mathcal{O}_{S'}}(\mathcal{O}_{S'}, \mathcal{L})$. We can get the invertible $\mathcal{O}_{S'}$-module $\mathcal{L}$ back as $\mathcal{L} = \mathcal{O}_{S'} \otimes_{\mathcal{O}_{S'}^{\times}} \mathrm{Isom}_{\mathcal{O}_{S'}}(\mathcal{O}_{S'}, \mathcal{L})$. The norm of $\mathcal{L}$ via $f\colon S' \to S$ is then defined as

$$\mathrm{Norm}_{S'/S}(\mathcal{L}) := \mathcal{O}_S \otimes_{\mathcal{O}_S^{\times}} \mathrm{Norm}_{S'/S}(\mathrm{Isom}_{\mathcal{O}_{S'}}(\mathcal{O}_{S'}, \mathcal{L}))\,. \tag{1.6.1.5}$$

This construction is functorial for isomorphisms of invertible $\mathcal{O}_{S'}$-modules.

1.6.2 Norms along finite relative Cartier divisors

This part is inspired by [59], section 1.1. Let S be a scheme, let $f\colon X \to S$ be an S-scheme of finite presentation. A finite effective relative Cartier divisor on $f\colon X \to S$ is a closed subscheme D of X that is finite and locally free over S, and whose ideal sheaf I_D is locally generated by a non-zero divisor (equivalently, I_D is locally free of rank 1 as $\mathcal{O}_X$-module). For such a D and an invertible $\mathcal{O}_X$-module $\mathcal{L}$, the norm of $\mathcal{L}$ along D is defined, using (1.6.1.5), as

$$\mathrm{Norm}_{D/S}(\mathcal{L}) := \mathrm{Norm}_{D/S}(\mathcal{L}|_D)\,. \tag{1.6.2.1}$$

Then $\mathrm{Norm}_{D/S}(\mathcal{L})$ is functorial for cartesian diagrams $(X' \to S', \mathcal{L}') \to (X \to S, \mathcal{L})$.

Lemma 1.6.2.2. *Let $f\colon X \to S$ be a morphism of schemes that is of finite presentation. For D a finite effective relative Cartier divisor on f, the norm functor* $\mathrm{Norm}_{D/S}$ *in (1.6.2.1) is multiplicative in $\mathcal{L}$:*

$$\mathrm{Norm}_{D/S}(\mathcal{L}_1 \otimes \mathcal{L}_2) = \mathrm{Norm}_{D/S}(\mathcal{L}_1) \otimes_{\mathcal{O}_S} \mathrm{Norm}_{D/S}(\mathcal{L}_2)\,, \tag{1.6.2.3}$$

with, for $U \subset S$ open, $V \subset X$ open, containing $f^{-1}U \cap D$ and $l_i \in \mathcal{L}_i(V)$ generating $\mathcal{L}_i|_V$,

$$\mathrm{Norm}_{D/S}(l_1 \otimes l_2) = \mathrm{Norm}_{D/S}(l_1) \otimes \mathrm{Norm}_{D/S}(l_2)\,. \tag{1.6.2.4}$$

Let D_1 and D_2 be finite effective relative Cartier divisors on f. Then the ideal sheaf $I_{D_1} I_{D_2} \subset \mathcal{O}_X$ is locally free of rank 1, the closed subscheme $D_1 + D_2$ defined by it is a finite effective relative Cartier divisor on f. The norm functor in (1.6.2.1) is additive in D:

$$\mathrm{Norm}_{(D_1+D_2)/S}(\mathcal{L}) = \mathrm{Norm}_{D_1/S}(\mathcal{L}) \otimes_{\mathcal{O}_S} \mathrm{Norm}_{D_2/S}(\mathcal{L})\,, \tag{1.6.2.5}$$

with, for $U \subset S$ open, $V \subset X$ open, containing $f^{-1}U \cap (D_1+D_2)$ and $l \in \mathcal{L}(V)$ generating $\mathcal{L}|_{D_1+D_2}$,

$$\mathrm{Norm}_{(D_1+D_2)/S}(l) = \mathrm{Norm}_{D_1/S}(l) \otimes \mathrm{Norm}_{D_2/S}(l)\,. \tag{1.6.2.6}$$

Proof. Let D_1 and D_2 be as stated. If $V \subset X$ is open, and f_i generates $I_{D_i}|_V$, then $f_1 f_2$ generates $(I_{D_1} I_{D_2})|_V$, and this element of $\mathcal{O}_X(V)$ is not a zero-divisor because f_1 and f_2 are not. To show that $D_1 + D_2$ is finite over S, we replace S by an affine open of it, and then reduce to the noetherian case, using the assumption that f is of finite presentation. Then, $(D_1 + D_2)_{\mathrm{red}}$ is the image of $D_{1,\mathrm{red}} \coprod D_{2,\mathrm{red}} \to X$, and therefore is proper. Hence $D_1 + D_2$ is proper over S, and quasi-finite over S, hence finite over S. The short exact sequence

$$\begin{array}{ccccc} I_{D_2}/I_{D_1+D_2} & \hookrightarrow & \mathcal{O}_{D_1+D_2} & \twoheadrightarrow & \mathcal{O}_{D_2} \\ \| & & & & \\ (I_{D_2})|_{D_1} & & & & \end{array} \tag{1.6.2.7}$$

shows that $\mathcal{O}_{D_1+D_2}$ is locally free as $\mathcal{O}_S$-module, of rank the sum of the ranks of the $\mathcal{O}_{D_i}$. So $D_1 + D_2$ is a finite effective relative Cartier divisor on $X \to S$.

We prove (1.6.2.5), by proving the required statement about sheaves of groups. The diagram

(1.6.2.8)

$$\begin{array}{ccccccc} & & & \overset{\mathrm{Norm}_{(D_1+D_2)/S}}{\curvearrowright} & & & \\ \mathcal{O}^\times_{D_1+D_2} & \longrightarrow & \mathcal{O}^\times_{D_1} \times \mathcal{O}^\times_{D_2} & \xrightarrow{\mathrm{Norm}_{D_1/S} \times \mathrm{Norm}_{D_2/S}} & \mathcal{O}^\times_S \times \mathcal{O}^\times_S & \xrightarrow{\cdot} & \mathcal{O}^\times_S \\ u & \longmapsto & & & & & \mathrm{Norm}_{D_1/S}(u)\mathrm{Norm}_{D_2/S}(u) \end{array}$$

commutes because multiplication by u on $\mathcal{O}_{D_1+D_2}$ preserves the short exact sequence (1.6.2.7), multiplying on the sub and quotient by its images in $\mathcal{O}^\times_{D_1}$ and in $\mathcal{O}^\times_{D_2}$; note that the sub is an invertible $\mathcal{O}_{D_1}$-module. □

1.6.3 Explicit description of the Poincaré torsor of a smooth curve

Let g be in $\mathbb{Z}_{\geq 1}$, let S be a scheme, and $\pi\colon C \to S$ be a proper smooth curve, with geometrically connected fibres of genus g, with a section $b \in C(S)$. Let $J \to S$ be its

jacobian. On $C \times_S J$ we have $\mathcal{L}^{\mathrm{univ}}$, the universal invertible $\mathcal{O}$-module of degree zero on C, rigidified at b.

Let $d \geq 0$, and $C^{(d)}$ the dth symmetric power of $C \to S$ (we note that the quotient $C^d \to C^{(d)}$ is finite, locally free of rank $d!$, and commutes with base change on S). Then on $C \times_S C^{(d)}$ we have D, the universal effective relative Cartier divisor on C of degree d. Hence, on $C \times_S J \times_S C^{(d)}$ we have their pullbacks D_J and $\mathcal{L}^{\mathrm{univ}}_{C^{(d)}}$, giving us

$$\mathcal{N}_d := \mathrm{Norm}_{D_J/(J\times_S C^{(d)})}(\mathcal{L}^{\mathrm{univ}}_{C^{(d)}})\,. \tag{1.6.3.1}$$

This invertible $\mathcal{O}$-module $\mathcal{N}_d$ on $J \times_S C^{(d)}$, rigidified at the zero-section of J, gives us a morphism of S-schemes $C^{(d)}$ to $\mathrm{Pic}_{J/S}$. The point db (the divisor d times the base point b) in $C^{(d)}(S)$ is mapped to 0, precisely because $\mathcal{L}^{\mathrm{univ}}$ is rigidified at b, and 1.6.2.5. Hence there is a unique morphism $\square\colon C^{(d)} \to J^\vee = \mathrm{Pic}^0_{J/S}$ such that the pullback of the Poincaré bundle P on $J \times J^\vee$ by $(\mathrm{id}, \square)\colon J \times C^{(d)} \to J \times J^\vee$, with its rigidifications, is the same as $\mathcal{N}_d$. The following proposition tells us what the morphism $\square$ is, and the next section tells us what the induced isomorphism is between the fibres of $\mathcal{N}_d$ at points of $J \times C^{(d)}$ with the same image in $J \times_S J$.

Proposition 1.6.3.2. *The pullback of P by $(j_b, j_b^{*,-1})\colon C \times_S J \to J \times_S J^\vee$ together with its rigidifications at b and 0, is equal to $\mathcal{L}^{\mathrm{univ}}$.*

Let d be in $\mathbb{Z}_{\geq 0}$. The morphism $\square\colon C^{(d)} \to J^\vee = \mathrm{Pic}^0_{J/S}$ is the composition of first $\Sigma\colon C^{(d)} \to J$, sending, for every S-scheme T, each point D in $C^{(d)}(T)$ to the class of $\mathcal{O}_{C_T}(D - db)$ twisted by the pullback from T that makes it rigidified at b, followed by $j_b^{*,-1}\colon J \to J^\vee$. Summarised in a diagram, with $\mathcal{M} := (\mathrm{id} \times j_b^{*,-1})^* P$:

$$\begin{array}{ccccccc} \mathcal{L}^{\mathrm{univ}} & \longleftarrow & P & \longrightarrow & \mathcal{M} & \xrightarrow{\widetilde{\mathrm{id}\times\Sigma}} & \mathcal{N}_d \\ C \times_S J & \xrightarrow{j_b \times j_b^{*,-1}} & J \times_S J^\vee & \xleftarrow{\mathrm{id}\times j_b^{*,-1}} & J \times_S J & \xleftarrow{\mathrm{id}\times\Sigma} & J \times_S C^{(d)}\,. \end{array} \tag{1.6.3.3}$$

Then $\mathcal{M}$, with its rigidifications at $\{0\} \times_S J$ and $J \times_S \{0\}$, is symmetric. For $T \to S$, x in $J(T)$ given by an invertible $\mathcal{O}$-module $\mathcal{L}$ on C_T rigidified at b, and $y = \Sigma(D)$ in $J(T)$ given by an effective relative divisor D of degree d on C_T we have

$$P\left(x, j_b^{*,-1}(y)\right) = \mathcal{M}(x, y) = \mathrm{Norm}_{D/T}(\mathcal{L})\,. \tag{1.6.3.4}$$

For c_1 and c_2 in $C(S)$, we have

$$\mathcal{M}\left(j_b(c_1), j_b(c_2)\right) = c_2^*\left(\mathcal{O}_C(c_1 - b)\right) \otimes b^*\left(\mathcal{O}_C(b - c_1)\right)\,, \tag{1.6.3.5}$$

and, as invertible $\mathcal{O}$-modules on $C \times_S C$, with Δ the diagonal and $\mathrm{pr}_\emptyset\colon C \times_S C \to S$ the structure morphism, we have

$$(j_b \times j_b)^* \mathcal{M} = \mathcal{O}(\Delta) \otimes \mathrm{pr}_1^* \mathcal{O}(-b) \otimes \mathrm{pr}_2^* \mathcal{O}(-b) \otimes \mathrm{pr}_\emptyset^* b^* T_{C/S}\,. \tag{1.6.3.6}$$

For $d > 2g-2$, $\widetilde{\mathrm{id}\times\Sigma}$ gives $\mathcal{N}_d$ a descent datum along $\mathrm{id}\times\Sigma$ that gives $\mathcal{M}$ on $J\times_S J$. For T an S-scheme, $x\in J(S)$ given by $\mathcal{L}$ on C_T, rigidified at b, D_1 and D_2 in $C^{(d_1)}(S)$ and $C^{(d_2)}(S)$, the isomorphism

$$\mathcal{M}(x,\Sigma(D_1+D_2)) = \mathcal{M}(x,\Sigma(D_1))\otimes\mathcal{M}(x,\Sigma(D_2)) \tag{1.6.3.7}$$

corresponds, via $\widetilde{\mathrm{id}\times\Sigma}$, to

$$\begin{aligned}\mathcal{N}_{d_1+d_2}(x,D_1+D_2) &= \mathrm{Norm}_{(D_1+D_2)/T}(\mathcal{L}) = \mathrm{Norm}_{D_1/T}(\mathcal{L})\otimes\mathrm{Norm}_{D_2/T}(\mathcal{L})\\ &= \mathcal{N}_{d_1}(x,D_1)\otimes\mathcal{N}_{d_2}(x,D_2)\,,\end{aligned} \tag{1.6.3.8}$$

using Lemma 1.6.2.2.

For T an S-scheme and x_1 and x_2 in $J(T)$ given by $\mathcal{O}$-modules $\mathcal{L}_1$ and $\mathcal{L}_2$ on C_T, rigidified at b, and D in $C^{(d)}(T)$, the isomorphism

$$\mathcal{M}(x_1+x_2,\Sigma(D)) = \mathcal{M}(x_1,\Sigma(D))\otimes\mathcal{M}(x_2,\Sigma(D)) \tag{1.6.3.9}$$

corresponds, via $\widetilde{\mathrm{id}\times\Sigma}$, to

$$\begin{aligned}\mathcal{N}_d(x_1+x_2,D) &= \mathrm{Norm}_{D/T}(\mathcal{L}_1\otimes\mathcal{L}_2) = \mathrm{Norm}_{D/T}(\mathcal{L}_1)\otimes\mathrm{Norm}_{D/T}(\mathcal{L}_2)\\ &= \mathcal{N}_d(x_1,D)\otimes\mathcal{N}_d(x_2,D)\,,\end{aligned} \tag{1.6.3.10}$$

using Lemma 1.6.2.2.

Proof. Let T be an S-scheme, and x be in $J(T)$. Then x corresponds to the invertible $\mathcal{O}$-module $(\mathrm{id}\times x)^*\mathcal{L}^{\mathrm{univ}}$ on C_T, rigidified at b. Let $z := j_b^{*,-1}(x)$ in $J^\vee(T)$. Then $j_b^*(z) = x$, meaning that the pullback of $(\mathrm{id}\times z)^*P$ on J_T rigidified at 0 by j_b equals $(\mathrm{id}\times x)^*\mathcal{L}^{\mathrm{univ}}$ on C_T rigidified at b. Taking $T := J$ and x the tautological point gives the first claim of the proposition.

The symmetry of $\mathcal{M}$ with its rigidifications follows from [76], (2.7.1) and Lemma 2.7.5, and (2.7.7), using 1.2.9.

Now we prove (1.6.3.4). So let T and x be as above, and $y = \Sigma(D)$ in $J(T)$ given by a relative divisor D of degree d on C_T. As $C^d\to C^{(d)}$ is finite and locally free of rank $d!$, we may and do suppose that D is a sum of sections, say $D = \sum_{i=1}^d(c_i)$, with $c_i\in C(T)$. Then we have, functorially:

$$\begin{aligned}P(x,j_b^{*,-1}(y)) &= P(y,j_b^{*,-1}(x)) = P(\Sigma(D),j_b^{*,-1}(x))\\ &= P\left(\sum_i j_b(c_i), j_b^{*,-1}(x)\right) = \bigotimes_i P(j_b(c_i),j_b^{*,-1}(x))\\ &= \bigotimes_i \mathcal{L}^{\mathrm{univ}}(c_i,x) = \bigotimes_i \mathcal{L}(c_i) = \mathrm{Norm}_{D/T}(\mathcal{L})\,.\end{aligned} \tag{1.6.3.11}$$

Identities (1.6.3.5) and (1.6.3.6) follow directly from (1.6.3.4).

Now we prove the claimed compatibility between (1.6.3.9) and (1.6.3.10). We do this by considering the case where $\mathcal{L}$ is universal, that is, base changing to J_T and x the universal point. Then, on J_T, we have 2 isomorphisms from $\mathrm{Norm}_{(D_1+D_2)/J_T}(\mathcal{L})$ to $\mathrm{Norm}_{D_1/J_T}(\mathcal{L})\otimes\mathrm{Norm}_{D_2/J_T}(\mathcal{L})$. These differ by an element of $\mathcal{O}(J_T)^\times = \mathcal{O}(T)^\times$. Hence it suffices to check that this element equals 1 at $0 \in J(T)$. This amounts to checking that the 2 isomorphisms are equal for $\mathcal{L} = \mathcal{O}_{C_T}$ with the standard rigidification at b. Then, both isomorphisms are the multiplication map $\mathcal{O}_T \otimes_{\mathcal{O}_T} \mathcal{O}_T \to \mathcal{O}_T$.

The compatibility between (1.6.3.7) and (1.6.3.8) is proved analogously. □

Remark 1.6.3.12. From Proposition 1.6.3.2 one easily deduces, in that situation, for T an S-scheme, x in $J(T)$ given by an invertible $\mathcal{O}$-module $\mathcal{L}$ on C_T, and D_1 and D_2 effective relative Cartier divisors on C_T, of the same degree, a canonical isomorphism

$$\mathcal{M}(x, \Sigma(D_1) - \Sigma(D_2)) = \mathrm{Norm}_{D_1/T}(\mathcal{L}) \otimes \mathrm{Norm}_{D_2/T}(\mathcal{L})^{-1}\,, \tag{1.6.3.13}$$

satisfying the analogous compatibilities as in Proposition 1.6.3.2. No rigidification of $\mathcal{L}$ at b is needed. In fact, for $\mathcal{L}_0$ an invertible $\mathcal{O}_T$-module, we have $\mathrm{Norm}_{D_1/T}(\pi^*\mathcal{L}_0) = \mathcal{L}_0^{\otimes d}$, where $\pi\colon C_T \to T$ is the structure morphism and d is the degree of D_1. Hence the right hand side of (1.6.3.13) is independent of the choice of $\mathcal{L}$, given x.

1.6.4 Explicit isomorphism for norms along equivalent divisors

Let g be in $\mathbb{Z}_{\geq 1}$, let S be a scheme, and $p\colon C \to S$ be a proper smooth curve, with geometrically connected fibres of genus g, with a section $b \in C(S)$. Let D_1, D_2 be effective relative Cartier divisors of degree d on C, that we also view as elements of $C^{(d)}(S)$. Recall from Proposition 1.6.3.2 the morphism $\Sigma\colon C^{(d)} \to J$. Then $\Sigma(D_1) = \Sigma(D_2)$ if and only if D_1, D_2 are linearly equivalent in the following sense: locally on S, there exists an f in $\mathcal{O}_C(U)^\times$, with $U := C \setminus (D_1 \cup D_2)$, such that $f\cdot\colon \mathcal{O}_U \to \mathcal{O}_U$ extends to an isomorphism $f\cdot\colon \mathcal{O}_C(D_1) \to \mathcal{O}_C(D_2)$. In this case, we define $\mathrm{div}(f) = D_2 - D_1$. Proposition 1.6.3.2 gives us, for each invertible $\mathcal{O}$-module $\mathcal{L}$ of degree 0 on C rigidified at b (viewed as an element of $J(S)$) specific isomorphisms

$$\begin{aligned}\mathrm{Norm}_{D_1/S}(\mathcal{L}) &= \mathcal{N}_d(\mathcal{L}, D_1) = \mathcal{M}(\mathcal{L}, \Sigma(D_1)) = \mathcal{M}(\mathcal{L}, \Sigma(D_2)) = \mathcal{N}_d(\mathcal{L}, D_2)\\ &= \mathrm{Norm}_{D_2/S}(\mathcal{L})\,.\end{aligned} \tag{1.6.4.1}$$

Now we describe explicitly this isomorphism $\mathrm{Norm}_{D_1/S}(\mathcal{L}) \to \mathrm{Norm}_{D_2/S}(\mathcal{L})$. To do so we first describe *an* isomorphism

$$\phi_{\mathcal{L},D_1,D_2}\colon \mathrm{Norm}_{D_1/S}(\mathcal{L}) \longrightarrow \mathrm{Norm}_{D_2/S}(\mathcal{L}) \tag{1.6.4.2}$$

that is functorial for Cartesian diagrams $(C' \to S', \mathcal{L}', D_1', D_2') \to (C \to S, \mathcal{L}, D_1, D_2)$ and then we prove that *this* isomorphism is the one in (1.6.4.1).

We construct $\phi_{\mathcal{L},D_1,D_2}$ locally on S and the functoriality of the construction takes care of making it global. So, suppose that f is as above: $f \in \mathcal{O}_C(U)^\times$, and $f\cdot\colon \mathcal{O}_U \to \mathcal{O}_U$ extends to an isomorphism $f\cdot\colon \mathcal{O}_C(D_1) \to \mathcal{O}_C(D_2)$. Let $n \in \mathbb{Z}$ with $n > 2g-2+2d$. Then $p_*(\mathcal{L}(nb)) \to p_*\mathcal{L}(nb)|_{D_1+D_2}$ and $p_*(\mathcal{O}_C(nb)) \to p_*\mathcal{O}_C(nb)|_{D_1+D_2}$ are surjective, and (still localising on S) $p_*(\mathcal{L}(nb))$ and $p_*(\mathcal{O}_C(nb))$ are free $\mathcal{O}_S$-modules and $\mathcal{L}(nb)|_{D_1+D_2}$ and $\mathcal{O}_C(nb)|_{D_1+D_2}$ are free $\mathcal{O}_{D_1+D_2}$-modules of rank 1. Then we have l_0 in $(\mathcal{L}(nb))(C)$ and l_1 in $(\mathcal{O}_C(nb))(C)$ restricting to generators on $D_1 + D_2$. Let $D^- := \mathrm{div}(l_1)$ and $D^+ := \mathrm{div}(l_0)$, and let $V := C \setminus (D^+ + D^-)$. Note that V contains $D_1 + D_2$ and that U contains $D^+ + D^-$. Then, on V, $l := l_0/l_1$ is in $\mathcal{L}(V)$, generates $\mathcal{L}|_{D_1+D_2}$, and multiplication by l is an isomorphism $\cdot l\colon \mathcal{O}_C(D^+ - D^-) \to \mathcal{L}$, that is, $\mathrm{div}(l) = D^+ - D^-$. Let

(1.6.4.3)
$$f(\mathrm{div}(l)) = f(D^+ - D^-) := \mathrm{Norm}_{D^+/S}(f|_{D^+}) \cdot \mathrm{Norm}_{D^-/S}(f|_{D^-})^{-1} \in \mathcal{O}_S(S)^\times\,,$$

and let $\phi_{\mathcal{L},l,f}$ be the isomorphism, given in terms of generators

(1.6.4.4)
$$\begin{aligned} \phi_{\mathcal{L},l,f}\colon \mathrm{Norm}_{D_1/S}(\mathcal{L}) &\longrightarrow \mathrm{Norm}_{D_2/S}(\mathcal{L}) \\ \mathrm{Norm}_{D_1/S}(l) &\longmapsto f(\mathrm{div}(l))^{-1} \cdot \mathrm{Norm}_{D_2/S}(l)\,. \end{aligned}$$

Now suppose that we made other choices n', l_0', l_1'. Then we get $D^{-\prime}$, $D^{+\prime}$, V', l' and $\phi_{\mathcal{L},l',f}$. Then there is a unique function $g \in \mathcal{O}_C(V \cap V')^\times$ such that $l' = gl$ in $\mathcal{L}(V \cap V')$. Then

(1.6.4.5)
$$\begin{aligned} \phi_{\mathcal{L},l',f}(\mathrm{Norm}_{D_1/S}(l)) &= \phi_{\mathcal{L},l',f}(\mathrm{Norm}_{D_1/S}(g^{-1}l')) \\ &= \phi_{\mathcal{L},l',f}(g^{-1}(D_1)\mathrm{Norm}_{D_1/S}(l')) \\ &= g^{-1}(D_1)\cdot\phi_{\mathcal{L},l',f}(\mathrm{Norm}_{D_1/S}(l')) \\ &= g^{-1}(D_1)\cdot f(\mathrm{div}(l'))^{-1}\cdot\mathrm{Norm}_{D_2/S}(l') \\ &= g^{-1}(D_1)\cdot f(\mathrm{div}(gl))^{-1}\cdot\mathrm{Norm}_{D_2/S}(gl) \\ &= g^{-1}(D_1)\cdot f(\mathrm{div}(g) + \mathrm{div}(l))^{-1}\cdot g(D_2)\cdot\mathrm{Norm}_{D_2/S}(l) \\ &= g^{-1}(D_1)\cdot f(\mathrm{div}(g))^{-1}\cdot g(D_2)\cdot f(\mathrm{div}(l))^{-1}\cdot\mathrm{Norm}_{D_2/S}(l) \\ &= g(\mathrm{div}(f))\cdot f(\mathrm{div}(g))^{-1}\cdot\phi_{\mathcal{L},l,f}(\mathrm{Norm}_{D_1/S}(l)) \\ &= \phi_{\mathcal{L},l,f}(\mathrm{Norm}_{D_1/S}(l))\,, \end{aligned}$$

where, in the last step, we used Weil reciprocity, in a generality for which we do not know a reference. The truth in this generality is clear from the classical case by reduction to the universal case, in which the base scheme is integral: take a suitable level structure

on J, then consider the universal curve with this level structure, and the universal 4-tuple of effective divisors with the necessary conditions. We conclude that $\phi_{\mathcal{L},l,f} = \phi_{\mathcal{L},l',f}$.

Now suppose that f' is in $\mathcal{O}_C(U)^\times$ with $\mathrm{div}(f') = \mathrm{div}(f)$. Then there is a unique $u \in \mathcal{O}_S(S)^\times$ such that $f' = u{\cdot}f$, and since $\mathcal{L}$ has degree 0 on C

$$\begin{aligned}\phi_{\mathcal{L},l,f'}\left(\mathrm{Norm}_{D_1/S}(l)\right) &= (u{\cdot}f)(\mathrm{div}(l))^{-1}{\cdot}\mathrm{Norm}_{D_2/S}(l)\\ &= u^{-\deg(\mathrm{div}(l))} f(\mathrm{div}(l))^{-1}{\cdot}\mathrm{Norm}_{D_2/S}(l)\\ &= f(\mathrm{div}(l))^{-1}{\cdot}\mathrm{Norm}_{D_2/S}(l) = \phi_{\mathcal{L},l,f}\left(\mathrm{Norm}_{D_1/S}(l)\right)\ .\end{aligned} \tag{1.6.4.6}$$

Hence $\phi_{\mathcal{L},l,f'} = \phi_{\mathcal{L},l,f}$. We define

$$\phi_{D_1,D_2,\mathcal{L}}\colon \mathrm{Norm}_{D_1/S}(\mathcal{L}) \longrightarrow \mathrm{Norm}_{D_2/S}(\mathcal{L}) \tag{1.6.4.7}$$

as the isomorphism $\phi_{\mathcal{L},l,f}$ in (1.6.4.4) for any local choice of f and l.

Lemma 1.6.4.8. *With the assumptions as in the beginning of Section 1.6.4, the isomorphism $\phi_{\mathcal{L},D_1,D_2}$ in (1.6.4.7) is equal to the isomorphism in (1.6.4.1).*

Proof. We do this, as in the proof of Proposition 1.6.3.2, by considering the case of the universal $\mathcal{L}$, that is, we base change via $J \to S$, and then restricting to $0 \in J(S)$. This amounts to checking that the 2 isomorphisms are equal for $\mathcal{L} = \mathcal{O}_C$ with the standard rigidification at b. In this case, $\mathrm{Norm}_{D_i/S}(\mathcal{O}_C) = \mathcal{O}_S$, with $\mathrm{Norm}_{D_i/S}(1) = 1$. Hence $\phi_{D_1,D_2,\mathcal{O}_C} = \phi_{\mathcal{O}_C,1,f}$ is the identity on $\mathcal{O}_S$ (use (1.6.4.4)). The other isomorphism is the identity on $\mathcal{O}_S$ because of the rigidifications of $\mathcal{M}$ and $\mathcal{N}_d$ on $0 \times J$ and $0 \times C^{(d)}$. □

1.6.5 Symmetry of the Norm for divisors on smooth curves

Let $C \to S$ be a proper and smooth curve with geometrically connected fibres. For D_1, D_2 effective relative Cartier divisors on C we define an isomorphism

$$\phi_{D_1,D_2}\colon \mathrm{Norm}_{D_1/S}(\mathcal{O}_C(D_2)) \longrightarrow \mathrm{Norm}_{D_2/S}(\mathcal{O}_C(D_1)) \tag{1.6.5.1}$$

that is functorial for cartesian diagrams $(C'/S', D_1', D_2') \to (C/S, D_1, D_2)$.

If suffices to define this isomorphism in the universal case, that is, over the scheme that parametrises all D_1 and D_2. Let d_1 and d_2 be in $\mathbb{Z}_{\geq 0}$, and let $U := C^{(d_1)} \times_S C^{(d_2)}$, and let D_1 and D_2 be the universal divisors on C_U. Then we have the invertible $\mathcal{O}_U$-modules $\mathrm{Norm}_{D_1/U}(\mathcal{O}_C(D_2))$ and $\mathrm{Norm}_{D_2/U}(\mathcal{O}_C(D_1))$. The image of $D_1 \cap D_2$ in U is closed, let U^0 be its complement. Then, over U^0, D_1 and D_2 are disjoint, and the restrictions of $\mathrm{Norm}_{D_1/U}(\mathcal{O}_C(D_2))$ and $\mathrm{Norm}_{D_2/U}(\mathcal{O}_C(D_1))$ are generated by $\mathrm{Norm}_{D_1/U}(1)$ and $\mathrm{Norm}_{D_2/U}(1)$, and there is a unique isomorphism $(\phi_{D_1,D_2})_{U^0}$ that sends $\mathrm{Norm}_{D_1/U}(1)$ to $\mathrm{Norm}_{D_2/U}(1)$.

We claim that this isomorphism extends to an isomorphism over U. To see it, we base change by $U' \to U$, where $U' = C^{d_1} \times_S C^{d_2}$, then $U' \to U$ is finite, locally free of rank $d_1!{\cdot}d_2!$. Then $D_1 = P_1 + \cdots + P_{d_1}$ and $D_2 = Q_1 + \cdots + Q_{d_2}$ with the P_i and Q_j in $C(U')$. The complement of the inverse image U'^0 in U' of U^0 is the union of the pullbacks $D_{i,j}$ under $\mathrm{pr}_{i,j}\colon U' \to C \times_S C$ of the diagonal, that is, the locus where $P_i = Q_j$. Each $D_{i,j}$ is an effective relative Cartier divisor on U', isomorphic as S-scheme to $C^{d_1+d_2-1}$, hence smooth over S. Now

$$\mathrm{Norm}_{D_1/U'}(\mathcal{O}(D_2)) = \bigotimes_{i,j} P_i^*\mathcal{O}(Q_j)\,, \quad \mathrm{Norm}_{D_2/U'}(\mathcal{O}(D_1)) = \bigotimes_{i,j} Q_j^*\mathcal{O}(P_i)\,, \tag{1.6.5.2}$$

and, on U'^0,

$$\mathrm{Norm}_{D_1/U'}(1) = \bigotimes_{i,j} 1\,, \quad \mathrm{Norm}_{D_2/U'}(1) = \bigotimes_{i,j} 1\,, \quad \text{in } \mathcal{O}(U'^0). \tag{1.6.5.3}$$

On the open U', the divisor of the tensor-factor 1 at (i,j), both in $\mathrm{Norm}_{D_1/U'}(1)$ and in $\mathrm{Norm}_{D_2/U'}(1)$, is $D_{i,j}$. Therefore, the isomorphism $(\phi_{D_1,D_2})_{U^0}$ extends, uniquely, to an isomorphism ϕ_{D_1,D_2} over U', which descends uniquely to U.

Our description of ϕ_{D_1,D_2} allows us to compute it in the trivial case where D_1 and D_2 are disjoint. One should be a bit careful in other cases. For example, when $d_1 = d_2 = 1$ and $P = Q$, we have $P^*\mathcal{O}_C(Q) = P^*\mathcal{O}_C(P)$ is the tangent space of $C \to S$ at P, and hence also at Q, but $\phi_{P,Q}$ is multiplication by -1 on that tangent space. The reason for that is that the switch automorphism on $C \times_S C$ induces -1 on the normal bundle of the diagonal.

Lemma 1.6.5.4. *Let b be an S-point on C. Because of the symmetry in Proposition 1.6.3.2, using (1.6.3.13), for D_1, D_2 relative effective divisors on C of degree d_1, d_2 over S we have the following diagram of isomorphisms defining ψ_{D_1,D_2}*

$$\begin{array}{ccc} \mathcal{M}(\Sigma(D_2),\Sigma(D_1)) & = & \mathrm{Norm}_{D_1/S}(\mathcal{O}_C(D_2 - d_2 b)) \otimes b^*\mathcal{O}_C(D_2 - d_2 b)^{-d_1} \\ \| & & \downarrow{\scriptstyle \psi_{D_1,D_2}} \\ \mathcal{M}(\Sigma(D_1),\Sigma(D_2)) & = & \mathrm{Norm}_{D_2/S}(\mathcal{O}_C(D_1 - d_1 b)) \otimes b^*\mathcal{O}_C(D_1 - d_1 b)^{-d_2}\,. \end{array}$$

Then

$$\psi_{D_1,D_2} = \phi_{D_1,D_2} \otimes \phi^{-1}_{D_1,d_2 b} \otimes \phi^{-1}_{d_1 b,D_2} \otimes \phi_{d_1 b,d_2 b}\,. \tag{1.6.5.5}$$

Moreover the isomorphisms ϕ_{D_1,D_2}, and consequently ψ_{D_1,D_2}, are compatible with addition of divisors, that is, under (1.6.3.10) and (1.6.3.8), for every triple D_1, D_2, D_3 of relative Cartier divisors on C we have

$$\phi_{D_1+D_2,D_3} = \phi_{D_1,D_3} \otimes \phi_{D_2,D_3}\,, \quad \phi_{D_1,D_2+D_3} = \phi_{D_1,D_2} \otimes \phi_{D_1,D_3}\,. \tag{1.6.5.6}$$

Proof. It is enough to prove it in the universal case, that is, when D_1 and D_2 are the universal divisors on C_U, and there we know that there exists a u in $\mathcal{O}_U(U)^\times = \mathcal{O}_S(S)^\times$ such that

$$u \cdot \psi_{D_1,D_2} = \phi_{D_1,D_2} \otimes \phi^{-1}_{D_1,d_2b} \otimes \phi^{-1}_{d_1b,D_2} \otimes \phi_{d_1b,d_2b}\,. \tag{1.6.5.7}$$

Since the symmetry in Proposition 1.6.3.2 is compatible with the rigidification at the point $(0,0) \in (J \times J)(S)$, then ψ_{d_1b,d_2b} is the identity on $\mathcal{O}_U$, as well as the right hand side of (1.6.5.5) when $D_i = d_ib$. Hence $u = u(d_1b, d_2b) = 1$, proving (1.6.5.5).

Now we prove (1.6.5.6). As for (1.6.5.5), it is enough to prove it in the universal case and then we can reduce to the case where $D_1 = d_1b$, $D_2 = d_2b$ and $D_3 = d_3b$ for d_i positive integers where we have

$$\begin{aligned} \phi_{d_1b+d_2b,d_3b} &= \phi_{d_1b,d_3b} \otimes \phi_{d_2b,d_3b} = (-1)^{(d_1+d_2)d_3}\,, \\ \phi_{d_1b,d_2b+d_3b} &= \phi_{d_1b,d_2b} \otimes \phi_{d_1b,d_3b} = (-1)^{d_1(d_2+d_3)}\,. \end{aligned} \tag{1.6.5.8}$$

□

1.6.6 Explicit residue disks and partial group laws

Let C be a smooth, proper, geometrically connected curve over $\mathbb{Z}/p^2$, with a $b \in C(\mathbb{Z}/p^2)$, let g be the genus, and let $\mathcal{M}$ be as in Proposition 1.6.3.2. Let $D = D^+ - D^-$ and $E = E^+ - E^-$ be relative Cartier divisors of degree 0 on C. For each α in $\mathcal{M}^\times(\mathbb{F}_p)$ whose image in $(J \times J)(\mathbb{F}_p)$ is given by (D, E) we parametrise $\mathcal{M}^\times(\mathbb{Z}/p^2)_\alpha$, under the assumption that there exists a non-special split reduced divisor of degree g on $C_{\mathbb{F}_p}$.

Let $b_1, \dots, b_g$ be points in $C(\mathbb{Z}/p^2)$ with distinct images $\overline{b}_i$ in $C(\mathbb{F}_p)$ and such that $h^0(C_{\mathbb{F}_p}, \overline{b}_1 + \cdots + \overline{b}_g) = 1$, and let $b_{g+1}, \dots, b_{2g}$ in $C(\mathbb{Z}/p^2)$ be such that the $\overline{b}_{g+i}$ are distinct and $h^0(C_{\mathbb{F}_p}, \overline{b}_{g+1} + \cdots + \overline{b}_{2g}) = 1$. Then the maps

(1.6.6.1)

$$\begin{aligned} f_1 \colon C^g &\longrightarrow J\,, \quad (c_1, \dots, c_g) \longmapsto [\mathcal{O}_C(c_1 + \cdots + c_g - (b_1 + \cdots + b_g) + D)] \\ f_2 \colon C^g &\longrightarrow J\,, \quad (c_1, \dots, c_g) \longmapsto [\mathcal{O}_C(c_1 + \cdots + c_g - (b_{g+1} + \cdots + b_{2g}) + E)]\,, \end{aligned}$$

are étale respectively in $(\overline{b_1}, \dots, \overline{b_g}) \in C^g(\mathbb{F}_p)$ and $(\overline{b_{g+1}}, \dots, \overline{b_{2g}}) \in C^g(\mathbb{F}_p)$, hence give bijections $C^g(\mathbb{Z}/p^2)_{(\overline{b_1},\dots,\overline{b_g})} \to J(\mathbb{Z}/p^2)_{\overline{D}}$ and $C^g(\mathbb{Z}/p^2)_{(\overline{b_{g+1}},\dots,\overline{b_{2g}})} \to J(\mathbb{Z}/p^2)_{\overline{E}}$. For each point $c \in C(\mathbb{F}_p)$ we choose

$$\begin{aligned} &x_{D,c} \in \mathcal{O}_C(-D)_c \text{ a generator}\,, \\ &x_c \in \mathcal{O}_{C,c} \text{ generating, together with } p, \text{ the maximal ideal of } \mathcal{O}_{C,c}. \end{aligned} \tag{1.6.6.2}$$

For each $i = 1, \dots, 2g$ we choose x_{b_i} so that $x_{b_i}(b_i) = 0$. For each $(\mathbb{Z}/p^2)$-point $c \in C(\mathbb{Z}/p^2)$ with image $\overline{c}$ in $C(\mathbb{F}_p)$ and for each $\lambda \in \mathbb{F}_p$ let c_λ be the unique point

in $C(\mathbb{Z}/p^2)_{\overline{c}}$ with $x_{\overline{c}}(c_\lambda) = \lambda p$. Then the map $\lambda \mapsto c_\lambda$ is a bijection $\mathbb{F}_p \to C(\mathbb{Z}/p^2)_{\overline{c}}$ hence the maps f_1, f_2 induce bijections

$$\begin{aligned} &\mathbb{F}_p^g \longrightarrow J(\mathbb{Z}/p^2)_{\overline{D}}\,, \quad \lambda \longmapsto D_\lambda := D + (b_{1,\lambda_1} - b_1) + \cdots + (b_{g,\lambda_g} - b_g) \\ &\mathbb{F}_p^g \longrightarrow J(\mathbb{Z}/p^2)_{\overline{E}}\,, \quad \mu \longmapsto E_\mu := E + (b_{g+1,\mu_1} - b_{g+1}) + \cdots + (b_{2g,\mu_g} - b_{2g})\,. \end{aligned} \tag{1.6.6.3}$$

Hence $\mathcal{M}^\times(\mathbb{Z}/p^2)_{\overline{D},\overline{E}}$ is the union of $\mathcal{M}^\times(D_\lambda, E_\mu)$ as λ and μ vary in $\mathbb{F}_p^g$ and by Proposition 1.6.3.2 and Remark 1.6.3.12 we have

$$\begin{aligned} \mathcal{M}(D_\lambda, E_\mu) =& \mathrm{Norm}_{E^+/(\mathbb{Z}/p^2)}(\mathcal{O}_C(D_\lambda)) \otimes \mathrm{Norm}_{E^-/(\mathbb{Z}/p^2)}(\mathcal{O}_C(D_\lambda))^{-1} \otimes \\ &\otimes \bigotimes_{i=1}^{g} \left(b_{g+i,\mu_i}^* \mathcal{O}_C(D_\lambda) \otimes b_{g+i}^* \mathcal{O}_C(D_\lambda)^{-1} \right)\,. \end{aligned} \tag{1.6.6.4}$$

For each $i \in \{1, \ldots, g\}$, $c \in C(\mathbb{Z}/p^2)$ and $\lambda \in \mathbb{F}_p$ we define $x_i(c, \lambda) := 1$ if $\overline{c} \neq \overline{b}_i$ and $x_i(c, \lambda) := x_{b_i} - \lambda p$ if $\overline{c} = \overline{b}_i$, so that $c^* x_i(c, \lambda)^{-1}$ generates $c^* \mathcal{O}(b_{i,\lambda})$. Then, for each $c \in C(\mathbb{Z}/p^2)$ and each $\lambda \in \mathbb{F}_p^g$,

$$c^* \left(x_{D,c}^{-1} \cdot \prod_{i=1}^{g} \frac{x_i(c,0)}{x_i(c,\lambda_i)} \right) \quad \text{generates } c^* \mathcal{O}_C(D_\lambda)\,. \tag{1.6.6.5}$$

We write $E^\pm = E^{0,\pm} + \cdots + E^{g,\pm}$ so that $E^{0,\pm}$ is disjoint from $\{\overline{b}_1, \ldots, \overline{b}_g\}$, and $E^{i,\pm}$, restricted to $C_{\mathbb{F}_p}$, is supported on $\overline{b}_i$. Let $x_{D,E}$ be a generator of $\mathcal{O}_C(-D)$ in a neighborhood of $E^+ \cup E^-$. Then, for each λ in $\mathbb{F}_p^g$,

$$\mathrm{Norm}_{E^{0,\pm}/(\mathbb{Z}/p^2)}(x_{D,E}^{-1}) \otimes \bigotimes_{i=1}^{g} \mathrm{Norm}_{E^{i,\pm}/(\mathbb{Z}/p^2)} \left(x_{D,E}^{-1} \cdot \frac{x_{b_i}}{x_{b_i} - \lambda_i p} \right) \tag{1.6.6.6}$$

generates $\mathrm{Norm}_{E^\pm/(\mathbb{Z}/p^2)}(\mathcal{O}_C(D_\lambda))$. By (1.6.6.4), (1.6.6.5) and (1.6.6.6) we see that, for λ and μ in $\mathbb{F}_p^g$,

(1.6.6.7)

$$\begin{aligned} s_{D,E}(\lambda,\mu) :=& \mathrm{Norm}_{E^{0,+}/(\mathbb{Z}/p^2)}(x_{D,E}^{-1}) \otimes \bigotimes_{i=1}^{g} \mathrm{Norm}_{E^{i,+}/(\mathbb{Z}/p^2)} \left(x_{D,E}^{-1} \cdot \frac{x_{b_i}}{x_{b_i} - \lambda_i p} \right) \otimes \\ &\otimes \mathrm{Norm}_{E^{0,-}/(\mathbb{Z}/p^2)}(x_{D,E}^{-1})^{-1} \otimes \bigotimes_{i=1}^{g} \mathrm{Norm}_{E^{i,-}/(\mathbb{Z}/p^2)} \left(x_{D,E}^{-1} \cdot \frac{x_{b_i}}{x_{b_i} - \lambda_i p} \right)^{-1} \otimes \\ &\otimes \bigotimes_{i=1}^{g} \left(b_{g+i,\mu_i}^* \left(x_{D,b_{g+i}}^{-1} \cdot \prod_{j=1}^{g} \frac{x_j(b_{g+i,\mu_i},0)}{x_j(b_{g+i,\mu_i},\lambda_j)} \right) \otimes b_{g+i}^* \left(x_{D,b_{g+i}}^{-1} \cdot \prod_{j=1}^{g} \frac{x_j(b_{g+i},0)}{x_j(b_{g+i},\lambda_j)} \right)^{-1} \right) \end{aligned}$$

generates the free rank one $\mathbb{Z}/p^2$-module $\mathcal{M}(D_\lambda, E_\mu)$. The fibre $\mathcal{M}^\times(\overline{D}, \overline{E})$ over $(\overline{D}, \overline{E})$ in $(J \times J)(\mathbb{F}_p)$ is an $\mathbb{F}_p^\times$-torsor, containing $\overline{s_{D,E}(0,0)}$, hence in bijection with $\mathbb{F}_p^\times$ by sending ξ in $\mathbb{F}_p^\times$ to $\xi \cdot \overline{s_{D,E}(0,0)}$. Using that $(\mathbb{Z}/p^2)^\times = \mathbb{F}_p^\times \times (1 + p\mathbb{F}_p)$, we conclude the following lemma.

Lemma 1.6.6.8. *With the assumptions and definitions from the start of Section 1.6.6, we have, for each $\xi \in \mathbb{F}_p^\times$, a parametrisation of the mod p^2 residue polydisk of $\mathcal{M}^\times$ at $\xi \cdot \overline{s_{D,E}(0,0)}$ by the bijection*

$$\mathbb{F}_p^g \times \mathbb{F}_p^g \times \mathbb{F}_p \longrightarrow \mathcal{M}^\times(\mathbb{Z}/p^2)_{\xi \cdot \overline{s_{D,E}(0,0)}}, \quad (\lambda, \mu, \tau) \longmapsto (1+p\tau)\cdot\xi\cdot s_{D,E}(\lambda,\mu)\,.$$

Using this parametrization it easy to describe the two partial group laws on $\mathcal{M}^\times(\mathbb{Z}/p^2)$ when one of the two points we are summing lies over $(\overline{D}, \overline{E})$ and the other lies over $(\overline{D}, 0)$ or $(0, \overline{E})$. To compute the group law in $J(\mathbb{Z}/p^2)$ we notice that for each $c \in C(\mathbb{Z}/p^2)$ such that $x_c(c) = 0$ and for each $\lambda, \mu \in \mathbb{F}_p$ we have

$$\frac{x_c^2}{(x_c - \lambda p)(x_c - \mu p)} = \frac{x_c^2}{x_c^2 - \lambda p x_c - \mu p x_c} = \frac{x_c}{x_c - (\lambda + \mu)p} \tag{1.6.6.9}$$

and since these rational functions generate $\mathcal{O}_C(c_\lambda - c + c_\mu - c)$ and $\mathcal{O}_C(c_{\lambda+\mu} - c)$ in a neighborhood of c, we have the *equality* of relative Cartier divisors on C

$$(c_\lambda - c) + (c_\mu - c) = c_{\lambda+\mu} - c\,. \tag{1.6.6.10}$$

Hence, under the definition for $\lambda \in \mathbb{F}_p^g$ of

(1.6.6.11)

$$D_\lambda^0 := (b_{1,\lambda_1} - b_1) + \cdots + (b_{g,\lambda_g} - b_g)\,, \quad E_\lambda^0 := (b_{g+1,\lambda_1} - b_{g+1}) + \cdots + (b_{2g,\lambda_g} - b_{2g})\,,$$

we have, for all $\lambda, \mu \in \mathbb{F}_p^g$, that $D_\lambda + D_\mu^0 = D_{\lambda+\mu}$ and $E_\lambda + E_\mu^0 = E_{\lambda+\mu}$. Definition 1.6.6.7, applied with $(D, 0)$ and $(0, E)$, with $x_{0,E} = 1$ and, for every $c \in C(\mathbb{F}_p)$, with $x_{0,c} = 1$, gives, for all λ, μ in $\mathbb{F}_p^g$, the elements

$$s_{D,0}(\lambda,\mu) \in \mathcal{M}^\times(D_\lambda, E_\mu^0)\,, \quad s_{0,E}(\lambda,\mu) \in \mathcal{M}^\times(D_\lambda^0, E_\mu)\,. \tag{1.6.6.12}$$

With these definitions, we have the following lemma for the partial group laws of $\mathcal{M}$.

Lemma 1.6.6.13. *With the assumptions and definitions from the start of Section 1.6.6, we have, for all $\lambda, \lambda_1, \lambda_2, \mu, \mu_1, \mu_2$ in $\mathbb{F}_p^g$, that*

$$\begin{aligned} s_{D,0}(\lambda,\mu_1) +_2 s_{D,E}(\lambda,\mu_2) &= s_{D,0}(\lambda,\mu_1) \otimes s_{D,E}(\lambda,\mu_2) = s_{D,E}(\lambda,\mu_1+\mu_2) \\ s_{0,E}(\lambda_1,\mu) +_1 s_{D,E}(\lambda_2,\mu) &= s_{D,0}(\lambda_1,\mu) \otimes s_{D,E}(\lambda_2,\mu) = s_{D,E}(\lambda_1+\lambda_2,\mu)\,, \end{aligned}$$

and, consequently, for all $\tau_1, \tau_2 \in \mathbb{F}_p$ and $\xi_1, \xi_2 \in \mathbb{F}_p^\times$, that

(1.6.6.14)

$$\begin{aligned} \xi_1(1+\tau_1 p)\cdot s_{D,0}(\lambda,\mu_1) +_2 \xi_2(1+\tau_2 p)\cdot s_{D,E}(\lambda,\mu_2) &= \xi_1(1+\tau_1 p)\xi_2(1+\tau_2 p)\cdot s_{D,E}(\lambda,\mu_1+\mu_2) \\ &= \xi_1\xi_2(1+(\tau_1+\tau_2)p)\cdot s_{D,E}(\lambda,\mu_1+\mu_2)\,, \\ \xi_1(1+\tau_1 p)\cdot s_{0,E}(\lambda_1,\mu) +_1 \xi_2(1+\tau_2 p)\cdot s_{D,E}(\lambda_2,\mu) &= \xi_1\xi_2(1+(\tau_1+\tau_2)p)\cdot s_{D,E}(\lambda_1+\lambda_2,\mu)\,. \end{aligned}$$

Proof. This follows from (1.6.6.9) and (1.6.6.10), together with the equivalence of (1.6.3.7) and (1.6.3.8) and the equivalence of (1.6.3.9) and (1.6.3.10) in Proposition 1.6.3.2. □

We end this section with one more lemma.

Lemma 1.6.6.15. *The parametrization in Lemma 1.6.6.8 is the inverse of a bijection given by parameters on $\mathcal{M}^\times$ analogously to (1.3.1).*

Proof. Let $\mathcal{Q}$ be the pullback of $\mathcal{M}$ by $f_1 \times f_2$ with f_1 and f_2 as in (1.6.6.1). Then the lift $\widetilde{f_1 \times f_2} \colon \mathcal{Q}^\times \to \mathcal{M}^\times$ is étale at any point $\beta \in \mathcal{Q}(\mathbb{F}_p)$ lying over $\overline{b} = (b_1, \dots, b_{2g}) \in C^{2g}(\mathbb{F}_p)$ and induces a bijection between $\mathcal{Q}^\times(\mathbb{Z}/p^2)_{\overline{b}}$ and $\mathcal{M}^\times(\mathbb{Z}/p^2)_{(\overline{D},\overline{E})}$. In particular we can interpret $s_{D,E}(\lambda,\mu)$ as a section of $\mathcal{Q}(b_{1,\lambda_1}, \dots b_{2g,\mu_g})$ and we can interpret the parametrization in Lemma 1.6.6.8 as a parametrization of $Q^\times(\mathbb{Z}/p^2)_{\overline{\xi s_{D,E}(0,0)}}$. It is then enough to prove that the parametrization in Lemma 1.6.6.8 is the inverse of a bijection given by parameters on $\mathcal{Q}^\times$. It comes from the definition of c_ν for $c \in C(\mathbb{Z}/p^2)$ and $\nu \in \mathbb{F}_p$, that the maps $\lambda_i, \mu_i \colon C^{2g}(\mathbb{Z}/p^2)_{\overline{b}} \to \mathbb{F}_p$ are given by parameters in $\mathcal{O}_{C^{2g},\overline{b}}$ divided by p. In order to see that also the coordinate $\tau \colon \mathcal{Q}^\times(\mathbb{Z}/p^2)_{\xi s_{D,E}(0,0)} \to \mathbb{F}_p$ is given by a parameter divided by p it is enough to prove that there is an open subset $U \subset C^{2g}$ containing $\overline{b}$ and a section s trivializing $\mathcal{Q}|_U$ such that $s_{D,E}(\lambda,\mu) = s(b_{1,\lambda_1}, \dots, b_{2g,\mu_g})$. Remark 1.6.3.12 and (1.6.5.1) give that

(1.6.6.16)

$$\begin{aligned}\mathcal{Q} = &\bigotimes_{i,j=1}^{g} \Big((\pi_i, \pi_{g+j})^* \mathcal{O}_{C\times C}(\Delta) \Big) \\ &\otimes \bigotimes_{i=1}^{g} \Big(\pi_i^* \mathcal{O}_C(E - (b_{g+1} + \cdots + b_{2g})) \otimes \pi_{g+i}^* \mathcal{O}_C(D - (b_1 + \cdots + b_g)) \Big) \\ &\otimes \mathrm{Norm}_{E/\mathbb{Z}/p^2}(\mathcal{O}_C(D - (b_1 + \cdots + b_g))) \otimes \bigotimes_{i=1}^{g} b_{g+i}^* \mathcal{O}_C(D - (b_1 + \cdots + b_g))^{-1}\end{aligned}$$

where $\Delta \subset C \times C$ is the diagonal and π_i is the i-th projection $C^g \times C^g \to C$. We can prove that there is an open subset $U \subset C^g \times C^g$ containing b and a section s trivializing $\mathcal{Q}|_U$ such that $s_{D,E}(\lambda,\mu) = s(b_{1,\lambda_1}, \dots, b_{2g,\mu_g})$, by trivializing each factor of the above tensor product in a neighborhood of b. Let us see it, for example, for the pieces of the form $(\pi_i, \pi_{g+j})^* \mathcal{O}_{C\times C}(\Delta)$. Let π_1, π_2 be the two projections $C \times C \to C$ and let us consider the divisor Δ: for each pair of points $c_1, c_2 \in C(\mathbb{F}_p)$ the invertible $\mathcal{O}$-module $\mathcal{O}_{C\times C}(-\Delta)$ is generated by the section $x_{\Delta,c_1,c_2} := 1$ in a neighborhood of (c_1, c_2) if $c_1 \neq c_2$, while it is generated by the section $x_{\Delta,c_1,c_2} := \pi_1^* x_{c_1} - \pi_2^* x_{c_2}$ in a neighborhood of (c_1, c_2) if $c_1 = c_2$. If we now take $c_1 = b_i, c_2 = b_{g+j} \in C(\mathbb{F}_p)$ we deduce there exists a neighborhood U of (b_i, b_{g+j}) such that $x^{-1}_{\Delta,b_i,b_{g+j}}$ generates $\mathcal{O}_{C\times C}(\Delta)|_U$. For each $\lambda, \mu \in \mathbb{F}_p^g$ the point $(b_{i,\lambda_i}, b_{g+j,\mu_j})$ lies in $U(\mathbb{Z}/p^2)$ and the

canonical isomorphism $(b_{i,\lambda_i}, b_{g+j,\mu_j})^*\mathcal{O}_{C\times C}(\Delta) = b^*_{g+j,\mu_j}\mathcal{O}_C(b_{i,\lambda_i})$ sends the generating section $(b_{i,\lambda_i}, b_{j,\mu_j})^* x^{-1}_{\Delta,c_1,c_2}$ to $b^*_{j,\mu_j} x_i(b_{g+j}, \lambda_i)^{-1}$, which is a factor in (1.6.6.7). This gives a section $s_{i,j}$ trivializing $\Big((\pi_i, \pi_{g+j})^*\mathcal{O}_{C\times C}(\Delta)\Big)$ in a neighborhood of b. With similar choices we can find sections trivializing the other factors in (1.6.6.16) in a neighborhood of b and tensoring all such sections we get a section s such that $s_{D,E}(\lambda, \mu) = s(b_{1,\lambda_1}, \ldots, b_{2g,\mu_g})$. □

1.6.7 Extension of the Poincaré biextension over Néron models

Let C over $\mathbb{Z}$ be a curve as in Section 1.2. Let q be a prime number that divides n. We also write C for $C_{\mathbb{Z}_q}$. Let J be the Néron model over $\mathbb{Z}_q$ of $\mathrm{Pic}^0_{C/\mathbb{Q}_q}$, and J^0 its fibre-wise connected component of 0. On $(J \times_{\mathbb{Z}_q} J)_{\mathbb{Q}_q}$ we have $\mathcal{M}$ as in Proposition 1.6.3.2, rigidified at $0 \times J_{\mathbb{Q}_q}$ and at $J_{\mathbb{Q}_q} \times 0$.

Proposition 1.6.7.1. *The invertible $\mathcal{O}$-module $\mathcal{M}$ on $(J \times_{\mathbb{Z}_q} J)_{\mathbb{Q}_q}$, with its rigidifications, extends uniquely to an invertible $\mathcal{O}$-module $\widetilde{\mathcal{M}}$ with rigidifications on $J \times_{\mathbb{Z}_q} J^0$. The biextension structure on $\mathcal{M}^\times$ extends uniquely to a biextension structure on $\widetilde{\mathcal{M}}^\times$.*

Proof. First of all, $J \times_{\mathbb{Z}_q} J^0$ is regular, hence Weil divisors and Cartier divisors are the same, and every invertible $\mathcal{O}$-module on $(J \times_{\mathbb{Z}_q} J^0)_{\mathbb{Q}_q}$ has an extension to an invertible $\mathcal{O}$-module on $J \times_{\mathbb{Z}_q} J^0$. So let $\mathcal{M}'$ be an extension of $\mathcal{M}$. Any extension $\mathcal{M}''$ of $\mathcal{M}$ is then of the form $\mathcal{M}'(D)$, with D a divisor on $J \times_{\mathbb{Z}_q} J^0$ with support in $(J \times_{\mathbb{Z}_q} J^0)_{\mathbb{F}_q}$. Such D are $\mathbb{Z}$-linear combinations of the irreducible components of the $D_i \times_{\mathbb{F}_q} J^0_{\mathbb{F}_q}$, where the D_i are the irreducible components of $J_{\mathbb{F}_q}$. Now $\mathcal{M}'|_{J\times 0}$ extends $\mathcal{M}|_{J_{\mathbb{Q}_q}\times 0}$, hence the rigidification of $\mathcal{M}|_{J_{\mathbb{Q}_q}\times 0}$ is a rational section of $\mathcal{M}'|_{J\times 0}$ whose divisor is a $\mathbb{Z}$-linear combination of the D_i. It follows that there is exactly one D as above such that the rigidification of $\mathcal{M}$ extends to a rigidification of $\mathcal{M}'(D)$ on $J \times 0$. That rigidification is compatible with a unique rigidification of $\mathcal{M}'(D)$ on $0 \times J^0$. We denote this extension $\mathcal{M}'(D)$ of $\mathcal{M}$ to $J \times_{\mathbb{Z}_q} J^0$ by $\widetilde{\mathcal{M}}$.

Let us now prove that the $\mathbb{G}_{\mathrm{m}}$-torsor $\widetilde{\mathcal{M}}^\times$ on $J \times_{\mathbb{Z}_q} J^0$ has a unique biextension structure, extending that of $\mathcal{M}^\times$. Over $J \times_{\mathbb{Z}_q} J \times_{\mathbb{Z}_q} J^0$ we have the invertible $\mathcal{O}$-modules whose fibres, at a point (x, y, z) (with values in some $\mathbb{Z}_q$-scheme) are $\widetilde{\mathcal{M}}(x + y, z)$ and $\widetilde{\mathcal{M}}(x, z) \otimes \widetilde{\mathcal{M}}(y, z)$. The biextension structure of $\mathcal{M}^\times$ gives an isomorphism between the restrictions of these over $\mathbb{Q}_q$, that differs from an isomorphism over $\mathbb{Z}_q$ by a divisor with support over $\mathbb{F}_q$. The compatibility with the rigidification of $\widetilde{\mathcal{M}}$ over $J \times_{\mathbb{Z}_q} 0$ proves that this divisor is zero. The other partial group law, and the required properties of them follow in the same way. We have now shown that $\widetilde{\mathcal{M}}^\times$ extends the biextension $\mathcal{M}^\times$. □

1.6.8 Explicit description of the extended Poincaré bundle

Let C over $\mathbb{Z}$ be a curve as in Section 1.2. Let q be a prime number that divides n. We also write C for $C_{\mathbb{Z}_q}$. By [68], Corollary 9.1.24, C is cohomologically flat over $\mathbb{Z}_q$, which means that for all $\mathbb{Z}_q$-algebras A, $\mathcal{O}(C_A) = A$. Another reference for this is [86], (6.1.4), (6.1.6) and (7.2.1).

The relative Picard functor $\mathrm{Pic}_{C/\mathbb{Z}_q}$ sends a $\mathbb{Z}_q$-scheme T to the set of isomorphism classes of $(\mathcal{L}, \mathrm{rig})$ with $\mathcal{L}$ an invertible $\mathcal{O}$-module on C_T and rig a rigidification at b. By cohomological flatness, such objects are rigid. But if the action of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ on the set of irreducible components of $C_{\overline{\mathbb{F}}_q}$ is non-trivial, then $\mathrm{Pic}_{C/\mathbb{Z}_q}$ is not representable by a $\mathbb{Z}_q$-scheme, only by an algebraic space over $\mathbb{Z}_q$ (see [86], Proposition 5.5). Therefore, to not be annoyed by such inconveniences, we pass to $S := \mathrm{Spec}(\mathbb{Z}_q^{\mathrm{unr}})$, the maximal unramified extension of $\mathbb{Z}_q$. Then $\mathrm{Pic}_{C/S}$ is represented by a smooth S-scheme, and on $C \times_S \mathrm{Pic}_{C/S}$ there is a universal pair $(\mathcal{L}^{\mathrm{univ}}, \mathrm{rig})$ ([86], Proposition 5.5, and Section 8.0). We note that $\mathrm{Pic}_{C/S} \to S$ is separated if and only if $C_{\overline{\mathbb{F}}_q}$ is irreducible.

Let $\mathrm{Pic}^{[0]}_{C/S}$ be the open part of $\mathrm{Pic}_{C/S}$ where $\mathcal{L}^{\mathrm{univ}}$ is of total degree zero on the fibres of $C \to S$. It contains the open part $\mathrm{Pic}^{0}_{C/S}$ where $\mathcal{L}^{\mathrm{univ}}$ has degree zero on all irreducible components of $C_{\overline{\mathbb{F}}_q}$.

Let E be the closure of the 0-section of $\mathrm{Pic}_{C/S}$, as in [86]. It is contained in $\mathrm{Pic}^{[0]}_{C/S}$. By [86], Proposition 5.2, E is represented by an S-group scheme, étale.

By [86], Theorem 8.1.4, or [22], Theorem 9.5.4, the tautological morphism $\mathrm{Pic}^{[0]}_{C/S} \to J$ is surjective (for the étale topology) and its kernel is E, and so $J = \mathrm{Pic}^{[0]}_{C/S}/E$. Also, the composition $\mathrm{Pic}^{0}_{C/S} \to \mathrm{Pic}^{[0]}_{C/S} \to J$ induces an isomorphism $\mathrm{Pic}^{0}_{C/S} \to J^0$.

Let C_i, $i \in I$, be the irreducible components of $C_{\overline{\mathbb{F}}_q}$. Then, as divisors on C, we have

$$C_{\overline{\mathbb{F}}_q} = \sum_{i \in I} m_i C_i \,. \tag{1.6.8.1}$$

For $\mathcal{L}$ an invertible $\mathcal{O}$-module on $C_{\overline{\mathbb{F}}_q}$, its multidegree is defined as

$$\mathrm{mdeg}(\mathcal{L})\colon I \to \mathbb{Z}, \quad i \mapsto \deg_{C_i}(\mathcal{L}|_{C_i})\,, \tag{1.6.8.2}$$

and its total degree is then

$$\deg(\mathcal{L}) = \sum_{i \in I} m_i \deg_{C_i}(\mathcal{L}|_{C_i})\,. \tag{1.6.8.3}$$

The multidegree induces a surjective morphism of groups

$$\mathrm{mdeg}\colon \mathrm{Pic}_{C/S}(S) \to \mathbb{Z}^I\,. \tag{1.6.8.4}$$

Now let $d \in \mathbb{Z}^I$ be a sufficiently large multidegree so that every invertible $\mathcal{O}$-module $\mathcal{L}$ on $C_{\overline{\mathbb{F}}_q}$ with $\mathrm{mdeg}(\mathcal{L}) = d$ satisfies $\mathrm{H}^1(C_{\overline{\mathbb{F}}_q}, \mathcal{L}) = 0$ and has a global section whose divisor is finite. Let $\mathcal{L}_0$ be an invertible $\mathcal{O}$-module on C, rigidified at b, with $\mathrm{mdeg}(\mathcal{L}_0) = d$. Then over $C \times_S J^0$ we have the invertible $\mathcal{O}$-module $\mathcal{L}^{\mathrm{univ}} \otimes \mathcal{L}_0$, and its pushforward $\mathcal{E}$ to J^0. Then $\mathcal{E}$ is a locally free $\mathcal{O}$-module on J^0. Let E be the geometric vector bundle over J^0 corresponding to $\mathcal{E}$. Then over E, $\mathcal{E}$ has its universal section. Let $U \subset E$ be the open subscheme where the divisor of this universal section is finite over J^0. The J^0-group scheme $\mathbb{G}_{\mathrm{m}}$ acts freely on U. We define $V := U/\mathbb{G}_{\mathrm{m}}$. As the $\mathbb{G}_{\mathrm{m}}$-action preserves the invertible $\mathcal{O}$-module and its rigidification, the morphism $U \to J^0$ factors through $U \to V$ and gives a morphism $\Sigma_{\mathcal{L}_0} \colon V \to J^0$. Then on $C \times_S V$ we have the universal effective relative Cartier divisor D^{univ} on $C \times_S V \to V$ of multidegree d, and $\mathcal{L}^{\mathrm{univ}} \otimes \mathcal{L}_0$ together with its rigidification at b is (uniquely) isomorphic to $\mathcal{O}_{C\times_S V}(D^{\mathrm{univ}}) \otimes_{\mathcal{O}_V} b^*\mathcal{O}_{C\times_S V}(-D^{\mathrm{univ}})$ with its tautological rigidification at b, in a diagram:

$$\mathcal{L}^{\mathrm{univ}} \otimes \mathcal{L}_0 \xlongequal{} \mathcal{O}_{C\times_S V}(D^{\mathrm{univ}}) \otimes_{\mathcal{O}_V} b^*\mathcal{O}_{C\times_S V}(-D^{\mathrm{univ}})\,. \tag{1.6.8.5}$$

Then $\Sigma_{\mathcal{L}_0}$ sends, for T an S-scheme, a T-point D on C_T to the invertible $\mathcal{O}$-module $\mathcal{O}_{C_T}(D) \otimes_{\mathcal{O}_T} b^*\mathcal{O}_{C_T}(-D) \otimes_{\mathcal{O}_C} \mathcal{L}_0^{-1}$ with its rigidification at b. Let s_0 be in $\mathcal{L}_0(C)$ such that its divisor D_0 is finite over S, and let $v_0 \in V(S)$ be the corresponding point.

On $\mathrm{Pic}^{[0]}_{C/S} \times_S V \times_S C$ we have the universal $\mathcal{L}^{\mathrm{univ}}$ from $\mathrm{Pic}^{[0]}_{C/S}$ with rigidification at b, and the universal divisor D^{univ}. Then on $\mathrm{Pic}^{[0]}_{C/S} \times_S V$ we have the invertible $\mathcal{O}$-module $\mathcal{N}_{q,d}$ whose fibre at a T-point $(\mathcal{L}, \mathrm{rig}, D)$ is $\mathrm{Norm}_{D/T}(\mathcal{L}) \otimes_{\mathcal{O}_T} \mathrm{Norm}_{D_0/T}(\mathcal{L})^{-1}$, canonically trivial on $\mathrm{Pic}^{[0]}_{C/S} \times_S v_0$:

$$\mathcal{N}_{q,d} \colon \left(\mathrm{Pic}^{[0]}_{C/S} \times_S V\right)(T) \ni (\mathcal{L}, \mathrm{rig}, D) \longmapsto \mathrm{Norm}_{D/T}(\mathcal{L}) \otimes_{\mathcal{O}_T} \mathrm{Norm}_{D_0/T}(\mathcal{L})^{-1}\,. \tag{1.6.8.6}$$

Any global regular function on the integral scheme $\mathrm{Pic}^{[0]}_{C/S} \times_S V$ is constant on the generic fibre, hence in $\mathbb{Q}_q^{\mathrm{unr}}$, and restricting it to $(0, v_0)$ shows that it is in $\mathbb{Z}_q^{\mathrm{unr}}$, and if it is 1 on $\mathrm{Pic}^{[0]}_{C/S} \times_S v_0$, it is equal to 1. Therefore trivialisations on $\mathrm{Pic}^{[0]}_{C/S} \times_S v_0$ rigidify invertible $\mathcal{O}$-modules on $\mathrm{Pic}^{[0]}_{C/S} \times_S V$.

The next proposition generalises [76], Corollary 2.8.6 and Lemma 2.7.11.2: there, $C \to S$ is nodal (but not necessarily regular), and the restriction of $\mathcal{M}$ to $J^0 \times_S J^0$ is described.

Proposition 1.6.8.7. *In the situation of Section 1.6.8, the pullback of the invertible $\mathcal{O}$-module $\mathcal{M}$ on $J \times_{\mathbb{Z}_q^{\mathrm{unr}}} J^0$ to $\mathrm{Pic}^{[0]}_{C/\mathbb{Z}_q^{\mathrm{unr}}} \times_{\mathbb{Z}_q^{\mathrm{unr}}} V$ by the product of the quotient map* $\mathrm{quot} \colon \mathrm{Pic}^{[0]}_{C/\mathbb{Z}_q^{\mathrm{unr}}} \to J$ *and the map $\Sigma_{\mathcal{L}_0} \colon V \to J^0$ is $\mathcal{N}_{q,d}$, compatible with their rigidifica-*

tions at $J \times 0$ and $\mathrm{Pic}^{[0]}_{C/\mathbb{Z}_q^{\mathrm{unr}}} \times v_0$. In a diagram:

$$\begin{array}{ccccc} P^{\times} & \longleftarrow & \mathcal{M}^{\times} & \longleftarrow & \mathcal{N}^{\times}_{q,d} \\ \downarrow & & \downarrow & & \downarrow \\ J \times_{\mathbb{Z}_q^{\mathrm{unr}}} J^{\vee,0} & \xleftarrow[\mathrm{id}\times j_b^{*,-1}]{} & J \times_{\mathbb{Z}_q^{\mathrm{unr}}} J^0 & \xleftarrow[\mathrm{quot}\times\Sigma_{\mathcal{L}_0}]{} & \mathrm{Pic}^{[0]}_{C/\mathbb{Z}_q^{\mathrm{unr}}} \times_{\mathbb{Z}_q^{\mathrm{unr}}} V\,. \end{array} \tag{1.6.8.8}$$

For T any $\mathbb{Z}_q^{\mathrm{unr}}$-scheme, for x in $J(T)$ given by an invertible $\mathcal{O}$-module $\mathcal{L}$ on C_T rigidified at b, and y in $J^0(T) = \mathrm{Pic}^0_{C/\mathbb{Z}_q^{\mathrm{unr}}}(T)$ given by the difference $D = D^+ - D^-$ of effective relative Cartier divisors on C_T of the same multidegree, we have

$$P(x, j_b^{*,-1}(y)) = \mathcal{M}(x,y) = \mathrm{Norm}_{D^+/T}(\mathcal{L}) \otimes_{\mathcal{O}_T} \mathrm{Norm}_{D^-/T}(\mathcal{L})^{-1}\,.$$

Proof. The scheme $\mathrm{Pic}^{[0]}_{C/\mathbb{Z}_q^{\mathrm{unr}}} \times_{\mathbb{Z}_q^{\mathrm{unr}}} V$ is smooth over $\mathbb{Z}_q^{\mathrm{unr}}$ ad connected, hence regular and integral, and since $V_{\overline{\mathbb{F}}_q}$ is irreducible, the irreducible components of $(\mathrm{Pic}^{[0]}_{C/\mathbb{Z}_q^{\mathrm{unr}}} \times_{\mathbb{Z}_q^{\mathrm{unr}}} V)_{\overline{\mathbb{F}}_q}$ are the $P^i \times_{\overline{\mathbb{F}}_q} V_{\overline{\mathbb{F}}_q}$, with P^i the irreducible components of $(\mathrm{Pic}^{[0]}_{C/\mathbb{Z}_q^{\mathrm{unr}}})_{\overline{\mathbb{F}}_q}$, with i in $\pi_0((\mathrm{Pic}^{[0]}_{C/\mathbb{Z}_q^{\mathrm{unr}}})_{\overline{\mathbb{F}}_q})$, which, by the way, equals the kernel of $\mathbb{Z}^I \to \mathbb{Z}$, $x \mapsto \sum_{j\in I} m_j x_j$. We now prove the first claim. Both $\mathcal{N}_{q,d}$ and the pullback of $\mathcal{M}$ are rigidified on $\mathrm{Pic}^{[0]}_{C/\mathbb{Z}_q^{\mathrm{unr}}} \times v_0$. Below we will give, after inverting q, an isomorphism α from $\mathcal{N}_{q,d}$ to the pullback of $\mathcal{M}$ that is compatible with the rigidifications. Then there is a unique divisor D_α on $\mathrm{Pic}^{[0]}_{C/\mathbb{Z}_q^{\mathrm{unr}}} \times_{\mathbb{Z}_q^{\mathrm{unr}}} V$, supported on $(\mathrm{Pic}^{[0]}_{C/\mathbb{Z}_q^{\mathrm{unr}}} \times_{\mathbb{Z}_q^{\mathrm{unr}}} V)_{\overline{\mathbb{F}}_q}$, such that α is an isomorphism from $\mathcal{N}_{q,d}(D_\alpha)$ to the pullback of $\mathcal{M}$. Let i be in $\pi_0((\mathrm{Pic}^{[0]}_{C/\mathbb{Z}_q^{\mathrm{unr}}})_{\overline{\mathbb{F}}_q})$, and let x be in $\mathrm{Pic}^{[0]}_{C/\mathbb{Z}_q^{\mathrm{unr}}}(\mathbb{Z}_q^{\mathrm{unr}})$ specialising to an $\overline{\mathbb{F}}_q$-point of P^i, then restricting α to (x_i, v_0) and using the compatibility of α (over $\mathbb{Q}_q^{\mathrm{unr}}$) with the rigidifications, gives that the multiplicity of $P^i \times V_{\overline{\mathbb{F}}_q}$ in D_α is zero. Hence D_α is zero.

Let us now give, over $(\mathrm{Pic}^{[0]}_{C/\mathbb{Z}_q^{\mathrm{unr}}} \times_{\mathbb{Z}_q^{\mathrm{unr}}} V)_{\mathbb{Q}_q^{\mathrm{unr}}}$, an isomorphism α from $\mathcal{N}_{q,d}$ to the pullback of $\mathcal{M}$. Note that $(\mathrm{Pic}^{[0]}_{C/\mathbb{Z}_q^{\mathrm{unr}}})_{\mathbb{Q}_q^{\mathrm{unr}}} = J_{\mathbb{Q}_q^{\mathrm{unr}}}$, and that $V_{\mathbb{Q}_q^{\mathrm{unr}}} = C^{(|d|)}_{\mathbb{Q}_q^{\mathrm{unr}}}$, where $|d| = \sum_i m_i d_i$ is the total degree given by the multidgree d. For T a $\mathbb{Q}_q^{\mathrm{unr}}$-scheme, $x \in J(T)$ given by $\mathcal{L}$ an invertible $\mathcal{O}_{C_T}$-module rigidified at b, and $v \in V(T)$ given by a relative Cartier divisor D of degree $|d|$ on C_T, we have, using Proposition 1.6.3.2 and (1.6.8.6), the following isomorphisms (functorial in T), respecting the rigidifications at $v = v_0$:

$$\begin{aligned} \mathcal{M}(x, \Sigma_{\mathcal{L}_0}(v)) &= \mathcal{M}(x, \Sigma(v) - \Sigma(v_0)) = \mathcal{M}(x, \Sigma(v)) \otimes \mathcal{M}(x, \Sigma(v_0))^{-1} \\ &= \mathrm{Norm}_{D/T}(\mathcal{L}) \otimes_{\mathcal{O}_T} \mathrm{Norm}_{D_0/T}(\mathcal{L})^{-1} = \mathcal{N}_{q,d}(x, v)\,. \end{aligned} \tag{1.6.8.9}$$

This finishes the proof of the first claim of the Proposition. The second claim follows directly from the definition of $\mathcal{N}_{q,d}$, plus the compatibility at the end of Proposition 1.6.3.2. □

1.6.9 Integral points of the extended Poincaré torsor

Let C over $\mathbb{Z}$ be a curve as in Section 1.2. Given a point $(x,y) \in (J \times J^0)(\mathbb{Z})$ we want to describe explicitly the free $\mathbb{Z}$-module $\mathcal{M}(x,y)$ when x is given by an invertible $\mathcal{O}$-module $\mathcal{L}$ of total degree 0 on C rigidified at b and y is given as a relative Cartier divisor D on C of total degree 0 with the property that there exists a unique divisor V whose support is disjoint from b and contained in the bad fibres of $C \to \mathrm{Spec}(\mathbb{Z})$ such that $\mathcal{O}(D+V)$ has degree zero when restricted to every irreducible component of any fibre of $C \to \mathrm{Spec}(\mathbb{Z})$. Since $\mathcal{M}(x,y)$ is a free $\mathbb{Z}$-module of rank 1 then it is a submodule of $\mathcal{M}(x,y)[1/n]$ and writing $D = D^+ - D^-$ as a difference of relative effective Cartier divisors, Proposition 1.6.3.2, with $S = \mathrm{Spec}(\mathbb{Z}[1/n])$, gives

$$\mathcal{M}(x,y)[1/n] = \left(\mathrm{Norm}_{D^+/\mathbb{Z}}(\mathcal{L}) \otimes_{\mathbb{Z}} \mathrm{Norm}_{D^-/\mathbb{Z}}(\mathcal{L})^{-1}\right)[1/n] \tag{1.6.9.1}$$

and consequently there exist unique integers e_q, for q varying among the primes dividing n, such that, as submodules of $\left(\mathrm{Norm}_{D^+/\mathbb{Z}}(\mathcal{L}) \otimes_{\mathbb{Z}} \mathrm{Norm}_{D^-/\mathbb{Z}}(\mathcal{L})^{-1}\right)[1/n]$,

$$\mathcal{M}(x,y) = \left(\prod_{q|n} q^{e_q}\right) \cdot \left(\mathrm{Norm}_{D^+/\mathbb{Z}}(\mathcal{L}) \otimes_{\mathbb{Z}} \mathrm{Norm}_{D^-/\mathbb{Z}}(\mathcal{L})^{-1}\right) . \tag{1.6.9.2}$$

We write $V = \sum_{q|n} V_q$ where V_q is a divisor supported on $C_{\mathbb{F}_q}$. For every prime q dividing n let $C_{i,q}, i \in I_q$ the irreducible components of $C_{\mathbb{F}_q}$ with multiplicity $m_{i,q}$ and let $V_{i,q}$ be the integers so that $V_q = \sum_{i \in I_q} V_{i,q} C_{i,q}$.

Proposition 1.6.9.3. *The integers in (1.6.9.2) are given by*

$$e_q = -\sum_{i \in I_q} V_{i,q} \deg_{\mathbb{F}_q}(\mathcal{L}|_{C_{i,q}}) .$$

Proof. For every q dividing n let H_q be an effective relative Cartier divisor on $C_{\mathbb{Z}_q}$ whose complement U_q is affine (recall that C is projective over $\mathbb{Z}$, take a high degree embedding and a hyperplane section that avoids chosen closed points $c_{i,q}$ on the $C_{i,q}$). The Chinese remainder theorem, applied to the $\mathcal{O}_C(U_q)$-module $(\mathcal{O}_C(D+V))(U_q)$ and the (distinct) closed points $c_{i,q}$, provides an element f_q of $(\mathcal{O}_C(D+V))(U_q)$ that generates $\mathcal{O}_C(D+V)$ at all $c_{i,q}$. Let $D_q = D_q^+ - D_q^-$ be the divisor of f_q as rational section of $\mathcal{O}_C(D+V)$. Then D_q^+ and D_q^- are finite over $\mathbb{Z}_q$, and f_q is a rational function on $C_{\mathbb{Z}_q}$ with

$$\mathrm{div}(f_q) = (D_q^+ - D_q^-) - (D+V) = (D_q^+ + D^-) - (D^+ + D_q^-) - V . \tag{1.6.9.4}$$

This linear equivalence, restricted to $\mathbb{Q}_q$, gives the isomorphism (1.6.4.7)

$$\phi\colon \mathrm{Norm}_{(D^+ + D_q^-)/\mathbb{Q}_q}(\mathcal{L}) \longrightarrow \mathrm{Norm}_{(D_q^+ + D^-)/\mathbb{Q}_q}(\mathcal{L}) . \tag{1.6.9.5}$$

Tensoring with $\mathrm{Norm}_{(D^-+D_q^-)/\mathbb{Q}_q}(\mathcal{L})^{-1}$ we obtain the isomorphism

(1.6.9.6)

$$\phi\otimes\mathrm{id}\colon \mathrm{Norm}_{D^+/\mathbb{Q}_q}(\mathcal{L})\otimes\mathrm{Norm}_{D^-/\mathbb{Q}_q}(\mathcal{L})^{-1}\longrightarrow \mathrm{Norm}_{D_q^+/\mathbb{Q}_q}(\mathcal{L})\otimes\mathrm{Norm}_{D_q^-/\mathbb{Q}_q}(\mathcal{L})^{-1}$$

using the identifications

(1.6.9.7)

$$\mathrm{Norm}_{D^+/\mathbb{Q}_q}(\mathcal{L})\otimes\mathrm{Norm}_{D^-/\mathbb{Q}_q}(\mathcal{L})^{-1}=\mathrm{Norm}_{(D^++D_q^-)/\mathbb{Q}_q}(\mathcal{L})\otimes\mathrm{Norm}_{(D^-+D_q^-)/\mathbb{Q}_q}(\mathcal{L})^{-1}$$

$$\mathrm{Norm}_{D_q^+/\mathbb{Q}_q}(\mathcal{L})\otimes\mathrm{Norm}_{D_q^-/\mathbb{Q}_q}(\mathcal{L})^{-1}=\mathrm{Norm}_{(D_q^++D^-)/\mathbb{Q}_q}(\mathcal{L})\otimes\mathrm{Norm}_{(D^-+D_q^-)/\mathbb{Q}_q}(\mathcal{L})^{-1}\,.$$

Using the same method as for getting the rational section f_q of $\mathcal{O}_C(D+V)$, we get a rational section l of $\mathcal{L}$ with the support of $\mathrm{div}(l)$ finite over $\mathbb{Z}_q$ and disjoint from the supports of D and D_q, and from the intersections of different $C_{i,q}$ and $C_{j,q}$. By Proposition 1.6.8.7, and the choice of l,

(1.6.9.8)

$$\mathcal{M}(x,y)_{\mathbb{Z}_q}=\mathrm{Norm}_{D_q^+/\mathbb{Z}_q}(\mathcal{L})\otimes\mathrm{Norm}_{D_q^-/\mathbb{Z}_q}(\mathcal{L})^{-1}=\mathbb{Z}_q\cdot\mathrm{Norm}_{D_q^+/\mathbb{Z}_q}(l)\otimes\mathrm{Norm}_{D_q^-/\mathbb{Z}_q}(l)^{-1}\,,$$

and

$$\mathrm{Norm}_{D^+/\mathbb{Z}_q}(\mathcal{L})\otimes\mathrm{Norm}_{D^-/\mathbb{Z}_q}(\mathcal{L})^{-1}=\mathbb{Z}_q\cdot\mathrm{Norm}_{D^+/\mathbb{Z}_q}(l)\otimes\mathrm{Norm}_{D^-/\mathbb{Z}_q}(l)^{-1}\,. \tag{1.6.9.9}$$

By (1.6.4.4), we have that $\phi\otimes\mathrm{id}$ maps

$$\mathrm{Norm}_{D^+/\mathbb{Q}_q}(l)\otimes\mathrm{Norm}_{D^-/\mathbb{Q}_q}(l)^{-1}$$

to

$$f_q(\mathrm{div}(l))^{-1}\cdot\mathrm{Norm}_{D_q^+/\mathbb{Q}_q}(l)\otimes\mathrm{Norm}_{D_q^-/\mathbb{Q}_q}(l)^{-1}\,. \tag{1.6.9.10}$$

Comparing with (1.6.9.2), we conclude that

$$e_q=v_q(f_q(\mathrm{div}(l)))\,. \tag{1.6.9.11}$$

We write $\mathrm{div}(l)=\sum_j n_jD_j$ as a sum of prime divisors. These D_j are finite over $\mathbb{Z}_q$, disjoint from the support of the horizontal part of $\mathrm{div}(f_q)$, that is of D_q-D, and each of them meets only one of the $C_{i,q}$, say $C_{s(j),q}$. Then, for each j, $f_q^{m_{s(j),q}}$ and $q^{-V_{s(j),q}}$ have the same multiplicity along $C_{s(j),q}$, and consequently they differ multiplicatively by a unit on a neighborhood of D_j. Then we have

(1.6.9.12)

$$\begin{aligned}v_q(f_q(D_j))&=\frac{v_q(f_q^{m_{s(j),q}}(D_j))}{m_{s(j),q}}=\frac{v_q(q^{-V_{s(j),q}}(D_j))}{m_{s(j),q}}=\frac{v_q\left(\mathrm{Norm}_{D_j/\mathbb{Z}_q}(q^{-V_{s(j),q}})\right)}{m_{s(j),q}}\\&=\frac{-V_{s(j),q}\deg_{\mathbb{Z}_q}(D_j)}{m_{s(j),q}}=\frac{-V_{s(j),q}\cdot(D_j\cdot C_{\mathbb{F}_q})}{m_{s(j),q}}=\frac{-V_{s(j),q}\cdot(D_j\cdot m_{s(j),q}C_{s(j),q})}{m_{s(j),q}}\\&=-V_{s(j),q}(D_j\cdot C_{s(j)})=-V_q\cdot D_j\,.\end{aligned}$$

We get

$$\begin{aligned} e_q &= v_q(f_q(\mathrm{div}(l))) = -V_q \cdot \mathrm{div}(l) = -\sum_{i \in I_q} V_{i,q}(C_i \cdot \mathrm{div}(l)) \\ &= -\sum_{i \in I_q} V_{i,q} \deg_{\mathbb{F}_q}(\mathcal{L}|_{C_{i,q}})\,. \end{aligned} \tag{1.6.9.13}$$

□

1.7 Description of the map from the curve to the torsor

The situation is as in Section 1.2. The aim of this section is to give descriptions of all morphisms in the diagram (1.2.12), in terms of invertible $\mathcal{O}$-modules on $(C \times C)_{\mathbb{Q}}$ and extensions of them over $C \times U$, to be used for doing computations when applying Theorem 1.4.12. The main point is that each $\mathrm{tr}_{c_i} \circ f_i$ is described in (1.7.4) as a morphism (of schemes) $\alpha_{\mathcal{L}_i} \colon J_{\mathbb{Q}} \to J_{\mathbb{Q}}$ with $\mathcal{L}_i$ an invertible $\mathcal{O}$-module on $C \times U$, and that Proposition 1.7.8 describes $(\widetilde{j_b})_i \colon C_{\mathbb{Z}[1/n]} \to T_i$.

We describe the morphism $\widetilde{j_b} \colon U \to T$ in terms of invertible $\mathcal{O}$-modules on $C \times C^{\mathrm{sm}}$. Since T is the product, over J, of the $\mathbb{G}_{\mathrm{m}}$-torsors $T_i := (\mathrm{id}, m \cdot \circ \mathrm{tr}_{c_i} \circ f_i)^* P^{\times}$ this amounts to describing, for each i, the morphism $(\widetilde{j_b})_i \colon U \to T_i$. Note that $\mathrm{tr}_{c_i} \circ f_i \colon J_{\mathbb{Q}} \to J_{\mathbb{Q}}$ is a morphism of groupschemes composed with a translation, and that all morphisms of schemes $\alpha \colon J_{\mathbb{Q}} \to J_{\mathbb{Q}}$ are of this form. From now on we fix one such i and omit it from our notation.

Let $\alpha \colon J_{\mathbb{Q}} \to J_{\mathbb{Q}}$ be a morphism of schemes, let $\mathcal{L}_\alpha$ be the pullback of $\mathcal{M}$ (see (1.6.3.3)) to $C_{\mathbb{Q}} \times C_{\mathbb{Q}}$ via $j_b \times (\alpha \circ j_b)$, and let $T_\alpha := (\mathrm{id}, \alpha)^* \mathcal{M}^{\times}$ on $J_{\mathbb{Q}}$:

$$\begin{array}{ccccc} & & T_\alpha & \longrightarrow & \mathcal{M}^{\times} \\ & & \downarrow & \swarrow & \\ C_{\mathbb{Q}} & \xrightarrow{j_b} & J_{\mathbb{Q}} & \xrightarrow{(\mathrm{id},\alpha)} & (J \times J)_{\mathbb{Q}} \\ \downarrow{\scriptstyle \mathrm{diag}} & & & & \uparrow{\scriptstyle j_b \times \mathrm{id}} \\ (C \times C)_{\mathbb{Q}} & \xrightarrow{\mathrm{id} \times j_b} & (C \times J)_{\mathbb{Q}} & \xrightarrow{\mathrm{id} \times \alpha} & (C \times J)_{\mathbb{Q}} \\ \uparrow & & & \swarrow & \uparrow \\ \mathcal{L}_\alpha^{\times} & & \longrightarrow & & \mathcal{L}^{\mathrm{univ},\times}\,. \end{array} \tag{1.7.1}$$

Then $(b, \mathrm{id})^* \mathcal{L}_\alpha = \mathcal{O}_{C_{\mathbb{Q}}}$, $\mathcal{L}_\alpha$ is of degree zero on the fibres of $\mathrm{pr}_2 \colon (C \times C)_{\mathbb{Q}} \to C_{\mathbb{Q}}$, and: $j_b^* T_\alpha$ is trivial if and only if $\mathrm{diag}^* \mathcal{L}_\alpha$ is trivial. Note that diagram (1.7.1) without the $\mathbb{G}_{\mathrm{m}}$-torsors is commutative.

Conversely, let $\mathcal{L}$ be an invertible $\mathcal{O}$-module on $(C \times C)_{\mathbb{Q}}$, rigidified on $\{b\} \times C_{\mathbb{Q}}$, and of degree 0 on the fibres of $\mathrm{pr}_2 \colon (C \times C)_{\mathbb{Q}} \to C_{\mathbb{Q}}$. The universal property of $\mathcal{L}^{\mathrm{univ}}$ gives a unique $\beta_{\mathcal{L}} \colon C_{\mathbb{Q}} \to J_{\mathbb{Q}}$ such that $(\mathrm{id} \times \beta_{\mathcal{L}})^* \mathcal{L}^{\mathrm{univ}} = \mathcal{L}$ (compatible with rigidification at b). The Albanese property of $j_b \colon C_{\mathbb{Q}} \to J_{\mathbb{Q}}$ then gives that $\beta_{\mathcal{L}}$ extends to a unique $\alpha_{\mathcal{L}} \colon J_{\mathbb{Q}} \to J_{\mathbb{Q}}$ such that $\alpha_{\mathcal{L}} \circ j_b = \beta_{\mathcal{L}}$. Then $j_b^* T_{\alpha_{\mathcal{L}}}$ is trivial if and only if $\mathrm{diag}^* \mathcal{L}$ is trivial. We have proved the following proposition.

Proposition 1.7.2. *In the situation of Section 1.2, the above maps $\alpha \mapsto \mathcal{L}_\alpha$ and $\mathcal{L} \mapsto \alpha_{\mathcal{L}}$ are inverse maps between the sets*

> *{scheme morphisms $\alpha \colon J_{\mathbb{Q}} \to J_{\mathbb{Q}}$ such that $j_b^*(\mathrm{id}, \alpha)^* \mathcal{M}$ is trivial}*

and

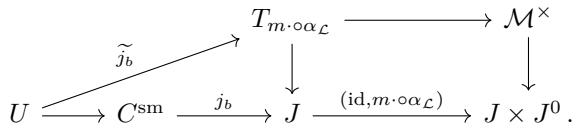
> *{invertible $\mathcal{O}$-modules $\mathcal{L}$ on $(C \times C)_{\mathbb{Q}}$, rigidified on $\{b\} \times C_{\mathbb{Q}}$, of degree 0 on the fibres of $\mathrm{pr}_2 \colon (C \times C)_{\mathbb{Q}} \to C_{\mathbb{Q}}$, and such that $\mathrm{diag}^* \mathcal{L}$ is trivial}.*

Now let $\mathcal{L}$ be in the second set of Proposition 1.7.2. Then $\mathrm{diag}^* \mathcal{L} = \mathcal{O}_{C_{\mathbb{Q}}}$, compatible with rigidifications at b. Let

$$\ell \in (\mathrm{diag}^* \mathcal{L}^\times)(C_{\mathbb{Q}}) \tag{1.7.3}$$

correspond to 1. Then $m_\cdot \circ \alpha_{\mathcal{L}}$ extends over $\mathbb{Z}$ to $m_\cdot \circ \alpha_{\mathcal{L}} \colon J \to J^0$, and the restriction of $j_b^*(m_\cdot \circ \alpha_{\mathcal{L}})^* \mathcal{M}$ on C^{sm} to U is trivial, giving a lift $\widetilde{j_b}$, unique up to sign:

(1.7.4)



The invertible $\mathcal{O}$-module $\mathcal{L}$ on $(C \times C)_{\mathbb{Q}}$ with its rigidification of $(b, \mathrm{id})^* \mathcal{L}$, extends uniquely to an invertible $\mathcal{O}$-module on $(C \times C)_{\mathbb{Z}[1/n]}$, still denoted $\mathcal{L}$.

Proposition 1.7.5. *Let S be a $\mathbb{Z}[1/n]$-scheme, let d and e be in $\mathbb{Z}_{\geq 0}$, and let $D \in C^{(d)}(S)$ and $E \in C^{(e)}(S)$. Then we have:*

$$\mathcal{M}(\Sigma(D), \alpha_{\mathcal{L}}(\Sigma(E))) = \big(\mathrm{Norm}_{D/S}(\mathrm{id}, b)^* \mathcal{L}\big)^{\otimes(1-e)} \otimes \mathrm{Norm}_{(D \times E)/S}(\mathcal{L}) \,.$$

For $x \in C(S)$ we have

$$T_{m_\cdot \circ \alpha_{\mathcal{L}}}(j_b(x)) = \mathcal{M}^\times(j_b(x), m_\cdot \alpha_{\mathcal{L}}(j_b(x))) = \mathcal{L}^{\otimes m}(x, x)^\times = (\mathbb{G}_{\mathrm{m}})_S \,.$$

Proof. We may and do assume (finite locally free base change on S) that we have x_i and y_j in $C(S)$, such that $D = \sum_i x_i$ and $E = \sum_j y_j$. Recall that, for $c \in C(S)$, $\beta_{\mathcal{L}}(c)$ in $J(S)$ is $(\mathrm{id}, c)^*\mathcal{L}$ on C_S, with its rigidification at b. Then we have:

$$\begin{aligned}\mathcal{M}(\Sigma(D), \alpha_{\mathcal{L}}(\Sigma(E))) &= \mathcal{M}(\alpha_{\mathcal{L}}(\Sigma(E)), \Sigma(D)) \\ &= \mathcal{M}\left(\beta_{\mathcal{L}}(b) + \sum_j (\beta_{\mathcal{L}}(y_j) - \beta_{\mathcal{L}}(b)), \sum_i j_b(x_i)\right) \\ &= \left(\bigotimes_i \mathcal{L}(x_i, b)^{\otimes(1-e)}\right) \otimes \bigotimes_{i,j} \mathcal{L}(x_i, y_j)\,.\end{aligned} \tag{1.7.5.1}$$

from which the desired equality follows.

Now we prove the second claim. Let x be in $C(S)$. The first equality holds by definition. Taking $D = E = x$ in what we just proved, gives the second equality, and the third comes from the rigidification at b. □

Now let $\mathcal{L}$ be any extension of $\mathcal{L}$ with its rigidification of $(b, \mathrm{id})^*\mathcal{L}$ from $(C \times C)_{\mathbb{Z}[1/n]}$ to $C \times U$. For q dividing n, let W_q be the valuation along $U_{\mathbb{F}_q}$ of the rational section ℓ of $\mathrm{diag}^*\mathcal{L}$ on U. Then ℓ, multiplied by the product, over the primes q dividing n, of q^{-W_q}, generates $\mathrm{diag}^*\mathcal{L}$ on U:

$$\left(\prod_{q|n} q^{-W_q}\right) \cdot \ell \in (\mathrm{diag}^*\mathcal{L}^\times)(U)\,. \tag{1.7.6}$$

There is a unique divisor V on $C \times U$ with support disjoint from $(b, \mathrm{id})U$ and contained in the $(C \times U)_{\mathbb{F}_q}$ with q dividing n, such that

$$\mathcal{L}^m := \mathcal{L}^{\otimes m}(V) \quad \text{on } C \times U \tag{1.7.7}$$

has multidegree 0 on the fibres of $\mathrm{pr}_2 \colon C \times U \to U$. Then $\mathcal{L}^m$ is the pullback of $\mathcal{L}^{\mathrm{univ}}$ via $\mathrm{id} \times (m\cdot \circ \alpha_{\mathcal{L}} \circ j_b) \colon C \times U \to C \times J^0$. Its restriction $\mathcal{L}^m|_{C^{\mathrm{sm}} \times U}$ is then the pullback of $\mathcal{M}$ via $j_b \times (m\cdot \circ \alpha_{\mathcal{L}} \circ j_b) \colon C^{\mathrm{sm}} \times U \to J \times J^0$, because on $C^{\mathrm{sm}} \times J^0$ the restriction of $\mathcal{L}^{\mathrm{univ}}$ and $(j_b \times \mathrm{id})^*\mathcal{M}$ are equal (both are rigidified after $(b, \mathrm{id})^*$ and equal over $\mathbb{Z}[1/n]$; here we use that, for all $q|n$, $J^0_{\mathbb{F}_q}$ is geometrically connected). Hence, on U we have $j_b^* T_{m\cdot\circ\alpha_{\mathcal{L}}} = \mathrm{diag}^*(\mathcal{L}^{\otimes m}(V)^\times)$, compatible with rigidifications at $b \in U(\mathbb{Z}[1/n])$. Our trivialisation $\widetilde{j_b}$ on U of $T_{m\cdot\circ\alpha_{\mathcal{L}}}$ is therefore a generating section of $\mathcal{L}^{\otimes m}$, multiplied by the product over the q dividing n, of the factors q^{-V_q}, where V_q is the multiplicity in V of the prime divisor $(U \times U)_{\mathbb{F}_q}$. This means that we have proved the following proposition.

Proposition 1.7.8. *For x and S as in Proposition 1.7.5, we have the following description of $\widetilde{j_b}$:*

$$\widetilde{j_b}(x) = \left(\prod_{q|n} q^{-mW_q - V_q}\right) \cdot \ell^{\otimes m} \quad \text{in } (T_{m\cdot\circ\alpha_{\mathcal{L}}}(j_b(x)))(S) = \mathcal{L}^{\otimes m}(x,x)^{\times}(S).$$

1.8 An example with genus 2, rank 2, and 14 points

The example that we are going to treat is the quotient of the modular curve $X_0(129)$ by the action of the group of order 4 generated by the Atkin-Lehner involutions w_3 and w_{43}. An equation for this quotient is given in the table in [53], and Magma has shown that that equation and the equations below give isomorphic curves over $\mathbb{Q}$.

Let C_0 be the curve over $\mathbb{Z}$ obtained from the following closed subschemes of $\mathbb{A}^2_{\mathbb{Z}}$

$$\begin{aligned} V_1 :&\quad y^2 + y = x^6 - 3x^5 + x^4 + 3x^3 - x^2 - x\,, \\ V_2 :&\quad w^2 + z^3 w = 1 - 3z + z^2 + 3z^3 - z^4 - z^5 \end{aligned}$$

by glueing the open subset of V_1 where x is invertible with the open subset of V_2 where z is invertible using the identifications $z = 1/x$, $w = y/x^3$. The scheme C_0 can be also described as a subscheme of the line bundle $\mathcal{L}_3$ associated to the invertible $\mathcal{O}$-module $\mathcal{O}_{\mathbb{P}^1_{\mathbb{Z}}}(3)$ on $\mathbb{P}^1_{\mathbb{Z}}$ with homogeneous coordinates X, Z: the map $\mathcal{O}_{\mathbb{P}^1_{\mathbb{Z}}}(3) \to \mathcal{O}_{\mathbb{P}^1_{\mathbb{Z}}}(6)$ sending a section Y to $Y \otimes Y + Z^3 \otimes Y$ induces a map ϕ from $\mathcal{L}_3$ to the line bundle $\mathcal{L}_6$ associated to $\mathcal{O}(6)$; then C_0 is isomorphic to the inverse image by ϕ of the section $s := X^6 - 3X^5Z + X^4Z^2 + 3X^3Z^3 - X^2Z^4 - XZ^5$ of $\mathcal{L}_6$ and since the map ϕ is finite of degree 2 then C_0 is finite of degree 2 over $\mathbb{P}^1_{\mathbb{Z}}$. Hence C_0 is proper over $\mathbb{Z}$ and it is moreover smooth over $\mathbb{Z}[1/n]$ with $n = 3 \cdot 43$. The generic fiber of C_0 is a curve of genus $g = 2$, labeled 5547.b.16641.1 on `www.lmfdb.org`. The only point where C_0 is not regular is the point $P_0 = (3, x-2, y-1)$ contained in V_1 and the blow up C of C_0 in P_0 is regular.

In the rest of the article we apply our geometric method to the curve C and we prove that $C(\mathbb{Z})$ contains exactly 14 elements. We use the same notation as in Sections 1.2 and 1.4.

The fiber $C_{\mathbb{F}_{43}}$ is absolutely irreducible while $C_{\mathbb{F}_3}$ is the union of two geometrically irreducible curves, a curve of genus 0 that lies above the point P_0 and that we call K_0, and a curve of genus 1 that we call K_1. We define $U_0 := C \setminus K_1$ and $U_1 := C \setminus K_0$ so that $C(\mathbb{Z}) = C^{\mathrm{sm}}(\mathbb{Z}) = U_0(\mathbb{Z}) \cup U_1(\mathbb{Z})$ and both U_0 and U_1 satisfy the hypothesis on U in Section 1.2. We have $K_0 \cdot K_1 = 2$ and consequently the self-intersections of K_0 and K_1 are both equal to -2. We deduce that all the fibers of J over $\mathbb{Z}$ are connected except

for $J_{\mathbb{F}_3}$ which has group of connected components equal to $\mathbb{Z}/2\mathbb{Z}$. Hence,

$$m = 2\,. \tag{1.8.0.1}$$

The automorphism group of C is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$, generated by the automorphisms ι and η lifting the extension to C_0 of

$$\iota, \eta\colon V_1 \longrightarrow V_1\,, \quad \iota\colon (x,y) \longmapsto (x, -1-y)\,, \quad \eta\colon (x,y) \longmapsto (1-x, -1-y)\,.$$

The quotients $E_1 := C_{\mathbb{Q}}/\eta$ and $E_2 := C_{\mathbb{Q}}/(\iota \circ \eta)$ are curves of genus 1 and the two projections $C \to E_i$ induce an isogeny $J \to \mathrm{Pic}^0(E_1) \times \mathrm{Pic}^0(E_2)$. The elliptic curves $\mathrm{Pic}^0(E_i)$ are not isogenous and $\rho = 2$.

1.8.1 The torsor on the jacobian

Let $\infty, \infty_- \in C(\mathbb{Z})$ be the lifts of $(0,1), (0,-1) \in V_2(\mathbb{Z}) \subset C_0(\mathbb{Z})$ and let us fix the base point $b = \infty$ in $C(\mathbb{Z})$. Following Section 1.7 we describe a $\mathbb{G}_{\mathrm{m}}$-torsor $T \to J$ and maps $\widetilde{j_{b,i}}\colon U_i \to T$ using invertible $\mathcal{O}$-modules on $C \times C^{\mathrm{sm}}$. The torsor $T = (\mathrm{id}, m\cdot \circ\, \alpha)^*\mathcal{M}^\times$ only depends on the scheme morphism $\alpha\colon J_{\mathbb{Q}} \to J_{\mathbb{Q}}$, which, by Proposition 1.7.2, is uniquely determined by an invertible $\mathcal{O}$-module $\mathcal{L}$ on $(C \times C)_{\mathbb{Q}}$, rigidified on $\{b\} \times C_{\mathbb{Q}}$, of degree 0 on the fibres of $\mathrm{pr}_2\colon (C \times C)_{\mathbb{Q}} \to C_{\mathbb{Q}}$, and such that $\mathrm{diag}^*\mathcal{L}$ is trivial.

We now look for a non-trivial $\mathcal{O}$-module $\mathcal{L}$ with these properties using the homomorphism $\eta^*\colon J_{\mathbb{Q}} \to J_{\mathbb{Q}}$, which does not belong to $\mathbb{Z} \subset \mathrm{End}(J_{\mathbb{Q}})$. We can take α of the form $\mathrm{tr}_c[\circ](n_1\cdot\eta^* + n_2\cdot\mathrm{id})$, where $\mathrm{id}\colon J_{\mathbb{Q}} \to J_{\mathbb{Q}}$ is the identity map, n_i are integers and c lies in $J(\mathbb{Q})$. Using the map $\alpha \mapsto \mathcal{L}_\alpha := (j_b \times (j_b \circ \alpha))^*\mathcal{M}$ in Proposition 1.7.2, the $\mathcal{O}$-module $\mathcal{L}_{\mathrm{tr}_c}$ is isomorphic to $\mathcal{O}_{C_{\mathbb{Q}}\times C_{\mathbb{Q}}}(\mathrm{pr}_1^* D)$, the $\mathcal{O}$-module $\mathcal{L}_{\eta^*}$ is isomorphic to $\mathcal{O}_{C_{\mathbb{Q}}\times C_{\mathbb{Q}}}(\Gamma_{\eta,\mathbb{Q}} - \mathrm{pr}_1^*\eta^*(b) - \mathrm{pr}_2^*\eta(b))$ and the $\mathcal{O}$-module $\mathcal{L}_{\mathrm{id}}$ is isomorphic to $\mathcal{O}_{C_{\mathbb{Q}}\times C_{\mathbb{Q}}}(\mathrm{diag}(C_{\mathbb{Q}}) - \mathrm{pr}_1^*(b) - \mathrm{pr}_2^*(b))$, where D is a divisor on $C_{\mathbb{Q}}$ representing c, the maps pr_i are the projections $C_{\mathbb{Q}} \times C_{\mathbb{Q}} \to C_{\mathbb{Q}}$ and Γ_η is the graph of the map $\eta\colon C \to C$. Hence, we can take $\mathcal{L}$ of the form $\mathcal{O}_{C_{\mathbb{Q}}\times C_{\mathbb{Q}}}(n_1\Gamma_{\eta,\mathbb{Q}} + n_2\mathrm{diag}(C_{\mathbb{Q}}) + \mathrm{pr}_1^* D_1 + \mathrm{pr}_2^* D_2)$ for some integers n_i and some divisors D_i on $C_{\mathbb{Q}}$. Among the $\mathcal{O}$-modules of this form satisfying the needed properties, we choose

$$\mathcal{L} := \mathcal{O}_{C_{\mathbb{Q}}\times C_{\mathbb{Q}}}(\Gamma_{\eta,\mathbb{Q}} - \mathrm{pr}_1^*(\infty_-) - \mathrm{pr}_2^*(\infty)) = \mathcal{O}_{C_{\mathbb{Q}}\times C_{\mathbb{Q}}}(\Gamma_{\eta,\mathbb{Q}} - \infty_- \times C_{\mathbb{Q}} - C_{\mathbb{Q}} \times \infty)$$

trivialised on $b \times C_{\mathbb{Q}}$ through the section

$$l_b := 2 \quad \text{in } ((b,\mathrm{id})^*\mathcal{L})(C_{\mathbb{Q}}) = \mathcal{O}_{C_{\mathbb{Q}}}(\eta(b) - b)(C_{\mathbb{Q}}) = \mathcal{O}_{C_{\mathbb{Q}}}(C_{\mathbb{Q}})\,.$$

For every $\overline{\mathbb{Q}}$-point Q on $C_{\mathbb{Q}}$ the $\mathcal{O}_{C_{\overline{\mathbb{Q}}}}$-module $(\mathrm{id}, Q)^*\mathcal{L}$ is isomorphic to $\mathcal{O}_{C_{\overline{\mathbb{Q}}}}(\eta(Q) - \infty_-)$, hence

$$\alpha_{\mathcal{L}} = \mathrm{tr}_c \circ f\,, \quad \text{with } f = \eta_* \text{ and } c = [D_0]\,, D_0 := \infty - \infty_-\,.$$

When restricted to the diagonal $\mathcal{L}$ is trivial since, compatibly with the trivialisation at (b,b),

$$\mathrm{diag}^*\mathcal{L} = \mathcal{O}_{C_{\mathbb{Q}}}(\infty_- + \infty - \infty_- - \infty) = \mathcal{O}_{C_{\mathbb{Q}}}\,.$$

In particular, the global section $l := 1$ of $\mathcal{O}_{C_{\mathbb{Q}}}$ gives a rigidification of $\mathrm{diag}^*\mathcal{L}$ that we write as

$$\mathrm{diag}^*\mathcal{L} = l \cdot \mathcal{O}_{C_{\mathbb{Q}}}\,.$$

Following Proposition 1.7.8 and the discussion preceding it, we choose the extension of $\mathcal{L}$ over $C \times C^{\mathrm{sm}}$

$$\mathcal{L} := \mathcal{O}_{C\times C^{\mathrm{sm}}}(\Gamma_\eta|_{C\times C^{\mathrm{sm}}} - \infty_- \times C^{\mathrm{sm}} - C \times \infty)\,,$$

trivialised along $b \times C^{\mathrm{sm}}$ through the section $l_b = 2$ (the points ∞_- and b have a simple intersection over the prime 2). By Proposition 1.7.5, the torsor $T := T_{m\cdot\circ\alpha_{\mathcal{L}}}$ on J, with $m = 2$ as explained before Equation (1.8.0.1), satisfies, for S a $\mathbb{Z}[1/n]$-scheme and x in $C(S)$, using the trivialisation given by l and l_b

$$\begin{aligned} T(j_b(x)) &= \mathcal{M}^\times(j_b(x), m\cdot\alpha_{\mathcal{L}}(j_b(x))) = \mathcal{M}^\times(j_b(x), (\mathrm{id},x)^*\mathcal{L}^{\otimes m}) \\ &= x^*(\mathrm{id},x)^*\mathcal{L}^{\otimes m,\times} \otimes b^*(\mathrm{id},x)^*\mathcal{L}^{\otimes -m,\times} \\ &= \mathcal{L}^{\otimes m,\times}(x,x) \otimes \mathcal{L}^{\otimes m,\times}(b,x)^{-1} = \mathcal{L}^{\otimes m,\times}(x,x) = \mathcal{O}_S^\times\,. \end{aligned} \tag{1.8.1.1}$$

Using Proposition 1.7.8 we now compute $\widetilde{j_{b,0}}$ and $\widetilde{j_{b,1}}$. Since l generates $\mathrm{diag}^*(\mathcal{L})$ on the whole C^{sm}, we have $W_3 = W_{43} = 0$. The invertible $\mathcal{O}$-module $\mathcal{L}^{\otimes m}$ has multidegree 0 over all the fibers $C \times U_1 \to U_1$, hence in order to compute $\widetilde{j_{b,1}}$ we must take $V = 0$ in (1.7.7), giving $V_3 = V_{43} = 0$. Hence for S and x as in (1.8.1.1), assuming moreover that 2 is invertible on S,

$$\widetilde{j_{b,1}}(x) = l^2 \otimes l_b^{-2} = \frac{1}{4}(x^*1) \otimes (b^*1)^{-1} \quad \text{in} \tag{1.8.1.2}$$

$$T(j_b(x)) = x^*(\mathrm{id},x)^*\mathcal{L}^{\otimes m,\times} \otimes b^*(\mathrm{id},x)^*\mathcal{L}^{\otimes -m,\times} = x^*\mathcal{O}_{C_S}(\eta\, x - \infty_-)^\times \otimes b^*\mathcal{O}_{C_S}(\eta\, x - \infty_-)^\times,$$

where the last equality in (1.8.1.2) makes sense if the image of x is disjoint from ∞, ∞_- in C_S.

The restriction $\mathcal{L}^{\otimes m}$ to $C \times U_0$ has multidegree 0 over all the fibers $C \times U_0 \to U_0$ of characteristic not 3, while if we consider a fiber of characteristic 3 it has degree 2 over K_0 and degree -2 over K_1. Hence for computing $\widetilde{j_{b,0}}$ we take $V = K_0 \times (K_0 \cap U_0)$ in (1.7.7) giving $V_{43} = 0$, $V_3 = 1$. Hence for S and x as in (1.8.1.1), assuming moreover that 2 is invertible on S,

$$\widetilde{j_{b,0}}(x) = \frac{1}{3}l^2 \otimes l_b^{-2} = \frac{1}{12}(x^*1) \otimes (b^*1)^{-1} \quad \text{in} \tag{1.8.1.3}$$

$$T(j_b(x)) = x^*(\mathrm{id}, x)^*\mathcal{L}^{\otimes m,\times} \otimes b^*(\mathrm{id}, x)^*\mathcal{L}^{\otimes -m,\times} = x^*\mathcal{O}_{C_S}(\eta\, x - \infty_-)^\times \otimes b^*\mathcal{O}_{C_S}(\eta\, x - \infty_-)^\times,$$

where the last equality in (1.8.1.3) makes sense if the image of x is disjoint from ∞, ∞_- in C_S.

1.8.2 Some integral points on the biextension

On C_0 we have the following integral points that lift uniquely to elements of $C(\mathbb{Z})$

$$\infty = (0,1)\,, \quad \infty_- := (0,-1) \quad \text{in } V_2(\mathbb{Z})\,,$$
$$\alpha := (1,0)\,, \quad \beta := \eta(\alpha) = (0,-1)\,, \quad \gamma := (2,1)\,, \quad \delta := \eta(\gamma) = (-1,-2) \quad \text{in } V_1(\mathbb{Z})\,.$$

Computations in Magma confirm that $J(\mathbb{Z})$ is a free $\mathbb{Z}$-module of rank $r = 2$ generated by

$$G_1 := \gamma - \alpha\,, \quad G_2 := \alpha + \infty_- - 2\infty\,.$$

The points in $T(\mathbb{Z})$ are a subset of points of $\mathcal{M}^\times(\mathbb{Z})$ that can be constructed, using the two group laws, from the points in $\mathcal{M}^\times(G_i, m{\cdot}f(G_j))(\mathbb{Z})$ and $\mathcal{M}^\times(G_i, m{\cdot}D_0)(\mathbb{Z})$ for $i, j \in \{1,2\}$. Let us compute in detail $\mathcal{M}^\times(G_1, m \cdot f(G_1))(\mathbb{Z})$. As explained in Proposition 1.6.9.3, we have

$$\begin{aligned}\mathcal{M}(G_1, m{\cdot}f(G_1))^\times &= \mathcal{M}^\times(\gamma - \alpha, 2\delta - 2\beta)\\ &= 3^{e_3}43^{e_{43}} \cdot \mathrm{Norm}_{(2\delta)/\mathbb{Z}}(\mathcal{O}_C(\gamma{-}\alpha)) \otimes \mathrm{Norm}_{(2\beta)/\mathbb{Z}}(\mathcal{O}_C(\gamma{-}\alpha))^{-1}\\ &= 3^{e_3}43^{e_{43}} \cdot (2\delta - 2\beta)^*\mathcal{O}_C(\gamma - \alpha)\end{aligned}$$

where, given a scheme S, an invertible $\mathcal{O}$-module $\mathcal{L}$ on C_S and a divisor $D_+ - D_- = \sum_i n_i P_i$ on C_S that is sum of S-points, we define the invertible $\mathcal{O}_S$-module

$$\left(\sum_i n_i P_i\right)^* \mathcal{L} := \bigotimes_i P_i^*\mathcal{L}^{n_i} = \mathrm{Norm}_{D_+/S}(\mathcal{L}) \otimes \mathrm{Norm}_{D_-/S}(\mathcal{L})^{-1}\,.$$

Since $C_{\mathbb{F}_{43}}$ is irreducible then $2f(G_1)$ has already multidegree 0 over 43, hence $e_{43} = 0$. If we look at $C_{\mathbb{F}_3}$ then $2f(G_1)$ does not have multidegree 0, while $2f(G_1) + K_0$ has multidegree 0; hence, by Proposition 1.6.9.3,

$$e_3 = -\deg_{\mathbb{F}_3} \mathcal{O}_C(\gamma - \alpha)|_{K_0} = -1\,.$$

Notice that over $\mathbb{Z}[\frac{1}{2}]$ the divisor G_1 is disjoint from β and δ (to see that it is disjoint from $\delta = (-1,-2,1)$ over the prime 3 one needs to look at local equations of the blow up) thus $\beta^*\mathcal{O}_C(\gamma - \alpha)$ and $\delta^*\mathcal{O}_C(\gamma - \alpha)$ are generated by β^*1 and δ^*1 over $\mathbb{Z}[\frac{1}{2}]$. Thus there are integers e_β, e_δ such that $\beta^*\mathcal{O}_C(\gamma - \alpha)$ and $\delta^*\mathcal{O}_C(\gamma - \alpha)$ are generated by $\beta^*2^{e_\beta}$

and $\delta^* 2^{e_\delta}$ over $\mathbb{Z}$. Looking at the intersections between β, γ, α and δ we compute that $e_\beta = -1$ and $e_\delta = 1$ hence

$$\mathcal{M}(G_1, m \cdot f(G_1)) = 3^{-1} \cdot (\delta^* 2)^2 \otimes (\beta^* 2^{-1})^{-2} \cdot \mathbb{Z} = 2^4 \cdot 3^{-1} \cdot (\delta^* 1)^2 \otimes (\beta^* 1) \cdot \mathbb{Z} \quad \text{and}$$
$$Q_{1,1} := \pm 2^4 \cdot 3^{-1} \cdot (\delta^* 1)^2 \otimes (\beta^* 1)^{-2} \in \mathcal{M}^\times_{G_1, m \cdot f(G_1)}(\mathbb{Z}) \,.$$

With analogous computations we see that

$$\begin{aligned}
Q_{2,1} &:= 2^{-2} \cdot (\delta^* 1)^2 \otimes (\beta^* 1)^{-2} && \text{generates } \mathcal{M}_{G_2, m \cdot f(G_1)} \\
Q_{1,2} &:= 2^{-2} \cdot (\beta^* 1)^2 \otimes (\infty^*_- 1)^2 \otimes (\infty^* 1)^{-4} && \text{generates } \mathcal{M}_{G_1, m \cdot f(G_2)} \\
Q_{2,2} &:= 2^{18} \cdot (\beta^* 1)^2 \otimes (\infty^*_- x)^2 \otimes (\infty^* z^2)^{-4} && \text{generates } \mathcal{M}_{G_2, m \cdot f(G_2)} \\
Q_{1,2} &:= (\infty^* 1)^2 \otimes (\infty^*_- 1)^{-2} && \text{generates } \mathcal{M}_{G_1, m \cdot D_0} \\
Q_{2,0} &:= 2^{-12} \cdot (\infty^* z^2)^2 \otimes (\infty^*_- x)^{-2} && \text{generates } \mathcal{M}_{G_2, m \cdot D_0} \,.
\end{aligned}$$

1.8.3 Some residue disks of the biextension

Let p be a prime of good reduction for C. Given the divisors

$$D := \alpha - \infty \,, \quad E := 2\beta - 2\infty_- = (m \cdot \circ \operatorname{tr}_c \circ \eta_*)(D) \quad \text{in } \operatorname{Div}(C_{\mathbb{Z}/p^2})$$

we use Lemma 1.6.6.8 to give parameters on the residue disks in $\mathcal{M}^\times(\mathbb{Z}/p^2)_{\overline{D}, \overline{E}}$ and $T(\mathbb{Z}/p^2)_{\overline{D}}$, with $\overline{D}, \overline{E}$ the images of D, E in $\operatorname{Div}(C_{\mathbb{F}_p})$.

We choose the "base points" $b_1 = \alpha, b_2 = \infty$, $b_3 = \beta, b_4 = \infty$, so that $b_1 \neq b_2$, $b_3 \neq b_4$ and $h^0(C_{\mathbb{F}_p}, b_1 + b_2) = h^0(C_{\mathbb{F}_p}, b_3 + b_4) = 1$. As in Equation (1.6.6.2), we define $x_\alpha = x - 1$, $x_\infty = z$, $x_\beta = x$ and $x_{D,\beta} = x_{D,\infty_-} = 1$, $x_{D,\infty} = z^{-1}$. For Q in $\{\infty, \beta, \alpha\}$ and $a \in \mathbb{F}_p$ let Q_a be the unique $\mathbb{Z}/p^2$-point of C that is congruent to Q modulo p and such that $x_Q(Q_a) = ap \in \mathbb{Z}/p^2$. We have the bijections

$$\begin{aligned}
&\mathbb{F}_p^2 \longrightarrow J(\mathbb{Z}/p^2)_{\overline{D}} \,, \quad \lambda \longmapsto D_\lambda := D + \alpha_{\lambda_1} - \alpha + \infty_{\lambda_2} - \infty = \alpha_{\lambda_1} + \infty_{\lambda_2} - 2\infty \\
&\mathbb{F}_p^2 \longrightarrow J(\mathbb{Z}/p^2)_{\overline{E}} \,, \quad \mu \longmapsto E_\mu := E + \beta_{\mu_1} - \beta + \infty_{\mu_2} - \infty = \beta + \beta_{\mu_1} + \infty_{\mu_2} - \infty - 2\infty_- \,.
\end{aligned}$$

Following (1.6.6.7) for $\lambda, \mu \in \mathbb{F}_p^2$ we define

$$s_{D,E}(\lambda, \mu) := (\beta^* 1) \otimes (\beta^*_{\mu_1} 1) \otimes (\infty^*_{\mu_2} \frac{z^2}{z - \lambda_2 p}) \otimes (\infty^* \frac{z^2}{z - \lambda_2 p})^{-1} \otimes (\infty^*_- 1)^{-2}$$

that, by Proposition 1.6.3.2 and Remark 1.6.3.12, generates $E_\mu^* \mathcal{O}_{C_{\mathbb{Z}/p^2}}(D_\lambda) = \mathcal{M}_{D_\lambda, E_\mu}$. The points in $\mathcal{M}^\times(\mathbb{F}_p)$ projecting to $(\overline{D}, \overline{E})$ are in bijection with the elements ξ in $\mathbb{F}_p^\times$ and are exactly the points $\xi \cdot s_{D,E}(0,0)$. Using $(\mathbb{Z}/p^2)^\times = \mathbb{F}_p^\times \times (1 + p\mathbb{F}_p)$, for each $\xi \in \mathbb{F}_p^\times$ we parametrise the residue disk of $\xi \cdot s_{D,E}(0,0)$ using bijection in Lemma 1.6.6.8

$$\mathbb{F}_p^5 \longrightarrow \mathcal{M}^\times(\mathbb{Z}/p^2)_{\xi \cdot s_{D,E}(0,0)} \,, \quad (\lambda_1, \lambda_2, \mu_1, \mu_2, \tau) \longmapsto (1 + p\tau) \xi \cdot s_{D,E}((\lambda_1, \lambda_2), (\mu_1, \mu_2)) \,.$$

Since $(m\cdot\circ \mathrm{tr}_c\circ f)(D_\lambda)=E_{-2\lambda}$ then we have

$$T(\mathbb{Z}/p^2)_{\overline{D}}=\bigcup_{\lambda\in\mathbb{F}_p^2} T_{D_\lambda}(\mathbb{Z}/p^2)=\bigcup_{\lambda\in\mathbb{F}_p^2}\mathcal{M}^\times_{D_\lambda,E_{-2\lambda}}(\mathbb{Z}/p^2)\,.$$

As ξ varies in $\mathbb{F}_p^\times$ the point $\xi\cdot s_{D,E}(0,0)$ varies in all the points in $\mathcal{M}^\times(\mathbb{F}_p)$ projecting to $(\overline{D},\overline{E})$ and we have the following bijection induced by parameters in $\xi\cdot s_{D,E}(0,0)$

(1.8.3.1)

$$\mathbb{F}_p^3\longrightarrow T(\mathbb{Z}_p)_{\xi s_{D,E}(0,0)}\,,\quad (\lambda_1,\lambda_2,\tau)\longmapsto (1+\tau p)\cdot\xi\cdot s_{D,E}((\lambda_1,\lambda_2),(-2\lambda_1,-2\lambda_2))\,.$$

If we apply (1.8.1.2) and (1.8.1.3) to $Q=\alpha_\lambda$ and we use the symmetry of the Poincaré torsor explained in Proposition 1.6.3.2 and made explicit in Lemma 1.6.5.4 we obtain the following description of $\widetilde{j_{b,i}}$ on $C(\mathbb{Z}/p^2)_{\alpha_{\mathbb{F}_p}}$ when $p\neq 2$

$$\widetilde{j_{b,1}}(\alpha_\lambda)=(1/4)\cdot s_{D,E}((\lambda,0),(-2\lambda,0))\,,\quad \widetilde{j_{b,0}}(Q)=(1/12)\cdot s_{D,E}((\lambda,0),(-2\lambda,0))\,.$$

If $p=5$ then 18 and -1 are $(p-1)$-th roots of unity in $(\mathbb{Z}/p^2)^\times$, thus $1/4=(-1)(1+p)$ and $1/12=3(1+2p)$ in $(\mathbb{Z}/p^2)^\times=\mathbb{F}_p^\times\times(1+p\mathbb{F}_p)$, hence

(1.8.3.2)

$$\widetilde{j_{b,1}}(\alpha_\lambda)=-(1+p)\cdot s_{D,E}((\lambda,0),(-2\lambda,0))\,,\quad \widetilde{j_{b,0}}(Q)=18\cdot(1+2p)\cdot s_{D,E}((\lambda,0),(-2\lambda,0))\,.$$

Since it is useful for computing the map $\kappa_\mathbb{Z}$ in the residue disks of $T(\mathbb{Z}/p^2)$ projecting to $\overline{D}$, we also apply Lemma 1.6.6.8 to the residue disks of $\mathcal{M}^\times(\mathbb{Z}/p^2)$ lying over $(\overline{D},0)$, $(0,\overline{E})$ and $(0,0)$. Hence for $\lambda,\mu\in\mathbb{F}_p^2$ we define the divisors on $C_{\mathbb{Z}/p^2}$

$$D^0_\lambda:=\alpha_{\lambda_1}-\alpha+\infty_{\lambda_2}-\infty\,,\quad E^0_\mu:=\beta_{\mu_1}-\beta+\infty_{\mu_2}-\infty$$

and the sections

$$\begin{aligned}
s_{D,0}(\lambda,\mu)&:=(\beta^*_{\mu_1}1)\otimes(\infty^*_{\mu_2}\frac{z^2}{z-\lambda_2 p})\otimes(\beta^*1)^{-1}\otimes(\infty^*\frac{z^2}{z-\lambda_2 p})^{-1} &&\in\mathcal{M}^\times(D_\lambda,E^0_\mu)(\mathbb{Z}/p^2)\\
s_{0,E}(\lambda,\mu)&:=(\beta^*1)\otimes(\beta^*_{\mu_1}1)\otimes(\infty^*_{\mu_2}\frac{z}{z-\lambda_2 p})\otimes(\infty^*\frac{z}{z-\lambda_2 p})^{-1}\otimes(\infty^*_-1)^{-2} &&\in\mathcal{M}^\times(D^0_\lambda,E_\mu)(\mathbb{Z}/p^2)\\
s_{0,0}(\lambda,\mu)&:=(\beta^*_{\mu_1}1)\otimes(\infty^*_{\mu_2}\frac{z}{z-\lambda_2 p})\otimes(\beta^*1)^{-1}\otimes(\infty^*\frac{z}{z-\lambda_2 p})^{-1} &&\in\mathcal{M}^\times(D^0_\lambda,E^0_\mu)(\mathbb{Z}/p^2)\,.
\end{aligned}$$

1.8.4 Geometry mod p^2 of integral points

From now on $p=5$. Let $\overline{\alpha}\in C(\mathbb{Z}/p^2)$ be the image of $\alpha\in C(\mathbb{Z})$. In this subsection we compute the composition $\overline{\kappa}\colon\mathbb{Z}^2\to T(\mathbb{Z}/p^2)_{\widetilde{j_{b,1}}(\overline{\alpha})}$ of the map $\kappa_\mathbb{Z}\colon\mathbb{Z}^2\to T(\mathbb{Z}_p)_{\widetilde{j_{b,1}}(\overline{\alpha})}$ in (1.4.9) and the reduction map $T(\mathbb{Z}_p)_{\widetilde{j_{b,1}}(\overline{\alpha})}\to T(\mathbb{Z}/p^2)_{\widetilde{j_{b,1}}(\overline{\alpha})}$. With a suitable choice of parameters in $\mathcal{O}_{T,\widetilde{j_{b,1}}(\overline{\alpha})}$, the map $\kappa_\mathbb{Z}$ is described by integral convergent power series

$\kappa_1, \kappa_2, \kappa_3 \in \mathbb{Z}_p\langle z_1, z_2\rangle$ and $\overline{\kappa}$, composed with the inverse of the parametrization (1.8.3.1), is given by the images $\overline{\kappa_1}, \overline{\kappa_2}, \overline{\kappa_3}$ of $\kappa_1, \kappa_2, \kappa_3$ in $\mathbb{F}_p[z_1, z_2]$.

The divisor $j_b(\overline{\alpha})$ is equal to the image of

$$\widetilde{G_t} := e_{0,1}G_1 + e_{0,2}G_2 \text{ with } e_{0,1} := 6\,, e_{0,2} := 3$$

in $J(\mathbb{F}_p)$ and

$$\tilde{t} := Q_{1,0}^{6} \otimes Q_{2,0}^{3} \otimes Q_{1,1}^{6\cdot 6} \otimes Q_{1,2}^{6\cdot 3} \otimes Q_{2,1}^{3\cdot 6} \otimes Q_{2,2}^{3\cdot 3} \quad \text{in } \mathcal{M}^{\times}(\widetilde{D_1}\,, m\cdot(D_0 + \eta_*\widetilde{G_t}))(\mathbb{Z})$$

is a lift of $\widetilde{j_{b,1}}(\overline{\alpha})$. The kernel of $J(\mathbb{Z}) \to J(\mathbb{F}_p)$ is a free $\mathbb{Z}$-module generated by

$$\widetilde{G_1}{:=}e_{1,1}G_1 + e_{1,2}G_2\,, \quad \widetilde{G_2}{:=}e_{2,1}G_1 + e_{2,2}G_2\,, \text{ with } e_{1,1}{:=}16\,, e_{1,2}{:=}2\,, e_{2,1}{:=}0\,, e_{2,2}{:=}5\,.$$

Let $\widetilde{G_{t,2}}$ be the divisor $m(D_0+\eta_*(\widetilde{G_t}))$ representing $(m\cdot\circ\mathrm{tr}_c\circ f)(\widetilde{G_t}) \in J^0(\mathbb{Z})$. Following (1.4.1) for $i, j \in \{1, 2\}$ we define

$$P_{i,j} := \bigotimes_{m,l=1}^{2} Q_{l,m}^{e_{i,l}\cdot e_{j,m}} \qquad R_{i,\tilde{t}} := \bigotimes_{l=1}^{2} Q_{l,0}^{e_{i,l}} \otimes \bigotimes_{m,l=1}^{2} Q_{l,m}^{e_{i,l}\cdot e_{0,m}} \qquad S_{\tilde{t},j} := \bigotimes_{m,l=1}^{2} Q_{l,m}^{e_{0,l}\cdot e_{j,m}}$$

$$\downarrow \qquad\qquad \downarrow \qquad\qquad \downarrow$$

$$(\widetilde{G_i}, f(m\widetilde{G_j})) \qquad (\widetilde{G_i}, \widetilde{G_{t,2}}) \qquad (\widetilde{G_t}, f(m\widetilde{G_j}))\,.$$

Computations in $C_{\mathbb{Z}/p^2}$ show the following linear equivalences of divisors

$$\widetilde{G_t} \sim D_{0,3}\,, \quad \widetilde{G_1} \sim D^0_{4,0}\,, \quad \widetilde{G_2} \sim D^0_{0,3}$$

and applying Lemma 1.6.4.8 and the functoriality of the norm we compute

(1.8.4.1)

$$\begin{aligned}
P_{1,1} &= (1+4p)\cdot s_{0,0}((4,0),(2,0)) && \in \mathcal{M}^{\times}(\widetilde{G_1},\widetilde{G_1})(\mathbb{Z}/p^2) = \mathcal{M}^{\times}(D^0_{4,0}, E^0_{2,0})(\mathbb{Z}/p^2),\\
P_{1,2} &= (1+4p)\cdot s_{0,0}((4,0),(0,4)) && \in \mathcal{M}^{\times}(\widetilde{G_1},\widetilde{G_2})(\mathbb{Z}/p^2) = \mathcal{M}^{\times}(D^0_{4,0}, E^0_{0,4})(\mathbb{Z}/p^2),\\
P_{2,1} &= (1+4p)\cdot s_{0,0}((0,3),(2,0)) && \in \mathcal{M}^{\times}(\widetilde{G_2},\widetilde{G_1})(\mathbb{Z}/p^2) = \mathcal{M}^{\times}(D^0_{0,3}, E^0_{2,0})(\mathbb{Z}/p^2),\\
P_{2,2} &= (-1)\cdot(1+2p)\cdot s_{0,0}((0,3),(0,4)) && \in \mathcal{M}^{\times}(\widetilde{G_2},\widetilde{G_2})(\mathbb{Z}/p^2) = \mathcal{M}^{\times}(D^0_{0,3}, E^0_{0,4})(\mathbb{Z}/p^2),\\
R_{1,\tilde{t}} &= s_{0,E}((4,0),(0,4)) && \in \mathcal{M}^{\times}(\widetilde{G_1},\widetilde{G_{t,2}})(\mathbb{Z}/p^2) = \mathcal{M}^{\times}(D^0_{4,0}, E_{0,4})(\mathbb{Z}/p^2),\\
R_{2,\tilde{t}} &= (1+4p)\cdot s_{0,E}((0,3),(0,4)) && \in \mathcal{M}^{\times}(\widetilde{G_2},\widetilde{G_{t,2}})(\mathbb{Z}/p^2) = \mathcal{M}^{\times}(D^0_{0,3}, E_{0,4})(\mathbb{Z}/p^2),\\
S_{\tilde{t},1} &= s_{D,0}((0,3),(2,0)) && \in \mathcal{M}^{\times}(\widetilde{G_t},\widetilde{G_1})(\mathbb{Z}/p^2) = \mathcal{M}^{\times}(D_{0,3}, E^0_{2,0})(\mathbb{Z}/p^2),\\
S_{\tilde{t},2} &= (-1)(1+4p)\cdot s_{D,0}((0,3),(0,4)) && \in \mathcal{M}^{\times}(\widetilde{G_t},\widetilde{G_2})(\mathbb{Z}/p^2) = \mathcal{M}^{\times}(D_{0,3}, E^0_{0,4})(\mathbb{Z}/p^2),\\
\tilde{t} &= (-1)\cdot(1+2p)\cdot s_{D,E}((0,3),(0,4)) && \in \mathcal{M}^{\times}(\widetilde{G_t},\widetilde{G_{t,2}})(\mathbb{Z}/p^2) = \mathcal{M}^{\times}(D_{0,3}, E_{0,4})(\mathbb{Z}/p^2).
\end{aligned}$$

We now show these computations in the cases of $\widetilde{G_t}$ and $\tilde{t}$. The Riemann-Roch space relative to the divisor $\widetilde{G_t}+\infty+\alpha-D$ on $C_{\mathbb{Z}/p^2}$ is generated by the inverse of the rational function

$$h_1 := \frac{x^9-5x^8-2x^7+7x^6-9x^5-5x^4+14x^3+7x^2+13x+1}{15x^5-x^4+4x^3+19x^2+4x+9} + \\ + \frac{x^6+9x^5-5x^4+15x^3-5x^2+4x+14}{15x^5-x^4+4x^3+19x^2+4x+9}y$$

and indeed

$$\mathrm{div}(h_1) = \widetilde{G_t} - D_{0,3} = (6\gamma+3\infty_- -3\alpha-6\infty) - (\alpha+\infty_3-2\infty) \quad \text{in } \mathrm{Div}(C_{\mathbb{Z}/p^2})\,.$$

Hence multiplication by h_1 gives an isomorphism $\mathcal{O}_{C_{\mathbb{Z}/p^2}}(\widetilde{G_t}) \to \mathcal{O}_{C_{\mathbb{Z}/p^2}}(D_{0,3})$ and by functoriality of the norm we get

$$\begin{aligned}
&\delta^*\mathcal{O}_C(\widetilde{G_t}) \to \delta^*\mathcal{O}_{C_{\mathbb{Z}/p^2}}(D_{0,3}), && \delta^*1 \mapsto \delta^*(h_1) = h_1(\delta)\cdot\delta^*1 = 12\cdot\delta^*1,\\
&\beta^*\mathcal{O}_C(\widetilde{G_t}) \to \beta^*\mathcal{O}_{C_{\mathbb{Z}/p^2}}(D_{0,3}), && \beta^*1 \mapsto \beta^*(h_1) = h_1(\beta)\cdot\beta^*1 = 18\cdot\beta^*1,\\
&\infty^*\mathcal{O}_C(\widetilde{G_t}) \to \infty^*\mathcal{O}_{C_{\mathbb{Z}/p^2}}(D_{0,3}), && \infty^*z^6 \mapsto \infty^*(z^6h_1) = 13\cdot\infty^*\frac{z^2}{z-3p},\\
&\infty_-^*\mathcal{O}_C(\widetilde{G_t}) \to \infty_-^*\mathcal{O}_{C_{\mathbb{Z}/p^2}}(D_{0,3}), && \infty_-^*z^{-3} \mapsto \infty_-^*(z^{-3}h_1) = \tfrac{h_1}{z^3}(\infty_-)\cdot\infty_-^*1 = 6\cdot\infty_-^*1\,.
\end{aligned}$$

Since $\widetilde{G_{t,2}} = 12\delta+4\infty_- -6\beta-10\infty$, the above isomorphisms, tensored with the exponents, give the canonical isomorphism

$$\mathcal{M}(\widetilde{G_t},\widetilde{G_{t,2}}) = \widetilde{G_{t,2}}^*\mathcal{O}_{C_{\mathbb{Z}/p^2}}(\widetilde{G_t}) \to \widetilde{G_{t,2}}^*\mathcal{O}_{C_{\mathbb{Z}/p^2}}(D_{0,3}) = \mathcal{M}(D_{0,3},\widetilde{G_{t,2}}) \tag{1.8.4.2}$$

$$\tilde{t}=14\cdot(\delta^*1)^{12}\otimes(\beta^*1)^{-6}\otimes(\infty^*z^6)^{-10}\otimes(\infty_-^*z^{-3})^4 \mapsto \\ \mapsto 14\cdot(\delta^*1)^{12}\otimes(\beta^*1)^{-6}\otimes(\infty^*\frac{z^2}{z-3p})^{-10}\otimes(\infty_-^*1)^4\,.$$

The Riemann-Roch space relative to the divisor $\widetilde{G_{t,2}}+\infty+\alpha-E$ on $C_{\mathbb{Z}/p^2}$ is generated by the inverse of the rational function

$$h_2 := \frac{x^{17}-8x^{16}+x^{15}-4x^{14}+7x^{13}+4x^{12}+12x^{11}+x^{10}+2x^9-5x^8+x^7+3x^6+12x^5}{20x^8-6x^7} \\ + \frac{6x^4-6x^3+4x^2+10x-6++(x^{15}+6x^{14}-5x^{13}-x^{12}-2x^{11}+14x^{10}-4x^9)y}{20x^8-6x^7} \\ + \frac{(14x^8+3x^7+8x^6-6x^5-3x^4+4x^3+13x^2-x-7)y}{20x^9-6x^8}$$

and indeed

$$\mathrm{div}(h_2) = \widetilde{G_{t,2}} - E_{0,4} = (12\delta+4\infty_- -6\beta-10\infty) - (2\beta+\infty_4-\infty-\infty_-) \quad \text{in } \mathrm{Div}(C_{\mathbb{Z}/p^2})\,.$$

Following the recipe in Section 1.6.4 that describes the map (1.6.4.4), we consider the following rational section of $\mathcal{O}_{C_{\mathbb{Z}/p^2}}(D_{0,3})$

$$l := \frac{10x^4 + x^3 + 17x + 14 + (15x + 9)y}{10x^4 + 16x^3 + 7x^2 + 7x + 10}\,.$$

since it generates $\mathcal{O}_{C_{\mathbb{Z}/p^2}}(D_{0,3})$ in a neighborhood of the supports of $\widetilde{G_{t,2}}$ and $E_{0,4}$. Then

$\mathrm{div}(l) = 3\cdot(-1,1)+(17,23)+(15,10)-2\cdot(12,23)-2\cdot(5,20)-(0,1) \in \mathrm{Div}(V_{1,\mathbb{Z}/p^2})\subset\mathrm{Div}(C_{\mathbb{Z}/p^2})$.

Hence by Lemma 1.6.4.8 the canonical isomorphism

$$\mathcal{M}(D_{0,3}, \widetilde{G_{t,2}}) = \widetilde{G_{t,2}}^{\,*}\mathcal{O}_{C_{\mathbb{Z}/p^2}}(D_{0,3}) \longrightarrow E_{0,4}^*\mathcal{O}_{C_{\mathbb{Z}/p^2}}(D_{0,3}) = \mathcal{M}(D_{0,3}, E_{0,4})$$

described in Equation (1.6.4.1) sends

$$\widetilde{G_{t,2}}^{\,*} l \longmapsto h_2(\mathrm{div}(l)) \cdot E_{0,4}^* l = 14 \cdot E_{0,4}^* l\,. \tag{1.8.4.3}$$

where

$$\begin{aligned}
\widetilde{G_{t,2}}^{\,*} l &:= (\delta^* l)^{12} \otimes (\beta^* l)^{-6} \otimes (\infty^* l)^{-10} \otimes (\infty_-^* l)^4 \\
&= -(\delta^* 1)^{12} \otimes (\beta^* 1)^{-6} \otimes (\infty^* \frac{z^2}{z-3p})^{-10} \otimes (\infty_-^* 1)^4\,, \\
E_{0,4}^* l &:= (\beta^* l)^2 \otimes (\infty_4^* l) \otimes (\infty^* l)^{-1} \otimes (\infty_-^* l)^{-2} \\
&= 16\cdot(\beta^* 1)^2 \otimes (\infty_4^* \frac{z^2}{z-3p}) \otimes (\infty^* \frac{z^2}{z-3p})^{-1} \otimes (\infty_-^* 1)^{-2}\,.
\end{aligned}$$

Equations (1.8.4.2) and (1.8.4.3) imply that $\tilde{t} = -(1+2p)\cdot s_{D,E}((0,3),(0,4))$.

Let $\overline{A_{\tilde{t}}}, \overline{B_{\tilde{t}}}, \overline{C}$ and $\overline{D_{\tilde{t}}}$ be the compositions of the reduction map $\mathcal{M}^\times(\mathbb{Z}_p) \to \mathcal{M}(\mathbb{Z}/p^2)$ and respectively $A_{\tilde{t}}, B_{\tilde{t}}, C$ and $D_{\tilde{t}}$, defined in (1.4.2), (1.4.3) and (1.4.4). Using (1.6.6.14) and (1.8.4.1) we get, for n in $\mathbb{Z}^2$,

(1.8.4.4)

$$\begin{aligned}
\overline{A_{\tilde{t}}}(n) &= (-1)^{n_2}(1 + (4n_2)t) \cdot s_{D,0}((0,3),(2n_1,4n_2))\,, \\
\overline{B_{\tilde{t}}}(n) &= (1 + (4n_2)p) s_{0,E}((4n_1,3n_2),(0,4))\,, \\
\overline{C}(n) &= (-1)^{n_2^2}(1 + (4n_1^2 + (4+4)n_1n_2 + 2n_2^2)p) \cdot s_{0,0}((4n_1,3n_2),(2n_1,4n_2))\,, \\
\overline{D_{\tilde{t}}}(n) &= -(1 + (4n_1^2 + 3n_1n_2 + 2n_2^2 + 3n_2 + 2)p) \cdot s_{D,E}((4n_1,3+3n_2),(2n_1,4+4n_2)), \\
\overline{\kappa}(n) &= -(1 + (4n_1^2 + 3n_1n_2 + 2n_2^2 + 2n_2 + 2)p) \cdot s_{D,E}((n_1,3+2n_2),(3n_1,4+n_2))\,,
\end{aligned}$$

hence, using the bijection (1.8.3.1),

$$\overline{\kappa_1} = z_1\,, \quad \overline{\kappa_2} = 3 + 2z_2\,, \quad \overline{\kappa_3} = 4z_1^2 + 3z_1z_2 + 2z_2^2 + 2z_2 + 2\,. \tag{1.8.4.5}$$

1.8.5 The rational points with a specific image mod 5.

By (1.8.4.4) the image in $T(\mathbb{F}_p)$ of a point $\pm\overline{D_{\tilde{t}}}(n)$ for $n \in \mathbb{Z}^2$ is always of the form $\pm s_{D,E}(0,0)$, hence, looking at (1.8.1.3) we see that there is no point $T(\mathbb{Z})$ with reduction $\widetilde{j_{b,0}}(\overline{\alpha}) \in T(\mathbb{F}_p)$. Hence $C(\mathbb{Z})_{\overline{\alpha}} = U_1(\mathbb{Z})_{\overline{\alpha}}$.

Let $F_1, F_2 \in \mathcal{O}(\widetilde{T}_t^p)^{\wedge_p}$ be generators of the kernel of $\widetilde{j_{b,1}}^* : \mathcal{O}(\widetilde{T}_t^p)^{\wedge_p} \to \mathcal{O}(\widetilde{U}_u^p)^{\wedge_p}$ as in Section 1.4. The bijection (1.8.3.1) gives an isomorphism $\mathbb{F}_p \otimes \mathcal{O}(\widetilde{T}_t^p) = \mathbb{F}_p[\lambda_1, \lambda_2, \tau]$ and since the images $\overline{F_1}, \overline{F_2}$ of F_1, F_2 in $\mathbb{F}_p \otimes \mathcal{O}(\widetilde{T}_t^p)$ are generators of the kernel of $\widetilde{j_{b,1}}^* : \mathbb{F}_p \otimes \mathcal{O}(\widetilde{T}_t^p)^{\wedge_p} \to \mathbb{F}_p \otimes \mathcal{O}(\widetilde{U}_u^p)^{\wedge_p}$ we can suppose that

$$\overline{F_1} = \lambda_2\,, \quad \overline{F_2} = \tau - 1\,.$$

By (1.8.4.5) we have

$$\kappa^*\overline{F_1} = \overline{\kappa_2} = 3 + 2z_2\,, \quad \kappa^*\overline{F_2} = \overline{\kappa_3} - 1 = 4z_1^2 + 3z_1z_2 + 2z_2^2 + 2z_2 + 1\,.$$

Let A be $\mathbb{Z}_p\langle z_1, z_2\rangle/(\kappa^*F_1, \kappa^*F_2)$. Then the ring

$$\overline{A} := A/pA = \mathbb{F}_p[z_1, z_2]/(\kappa^*\overline{F_1}, \kappa^*\overline{F_1}) = \mathbb{F}_p[z_1, z_2]/(z_2 - 1\,, 4z_1^2 + 3z_1) \tag{1.8.5.1}$$

has dimension 2 over $\mathbb{F}_p$, hence by Theorem 1.4.12 $U(\mathbb{Z})_{\overline{\alpha}}$ contains at most 2 points. Since both

$$\alpha \quad \text{and} \quad (12/7, 20/7) \in V_1(\mathbb{Z}[1/7])$$

reduce to $\overline{\alpha}$ we deduce that $C(\mathbb{Z})_{\overline{\alpha}} = U_1(\mathbb{Z})_{\overline{\alpha}}$ is made of the these two points.

1.8.6 Determination of all rational points

Denoting $(3, -1) \in V_1(\mathbb{F}_p) \subset C(\mathbb{F}_p)$ as ε we have

$$C(\mathbb{F}_p) = \{\overline{\infty}\,, \overline{\infty_-}\,, \overline{\alpha}\,, \iota(\overline{\alpha})\,, \eta(\overline{\alpha})\,, (\iota\circ\eta)(\overline{\alpha})\,, \overline{\gamma}\,, \iota(\overline{\gamma})\,, \eta(\overline{\gamma})\,, (\iota\circ\eta)(\overline{\gamma})\,, \varepsilon\,, \iota(\varepsilon)\}\,.$$

Using that for any point Q in $C(\mathbb{F}_p)$ the condition $T(\mathbb{Z})_{\widetilde{j_{b,i}(Q)}} = \emptyset$ implies $U_i(\mathbb{Z})_Q = \emptyset$ we get

$$U_0(\mathbb{Z})_{\overline{\infty}} = U_0(\mathbb{Z})_{\overline{\infty_-}} = U_1(\mathbb{Z})_{\varepsilon} = U_1(\mathbb{Z})_{\iota(\varepsilon)} = U_1(\mathbb{Z})_{\overline{\gamma}} = U_1(\mathbb{Z})_{\eta(\overline{\gamma})} = U_1(\mathbb{Z})_{\eta(\overline{\gamma})} = U_1(\mathbb{Z})_{\iota\eta(\overline{\gamma})} = \emptyset\,.$$

Applying our method to $\overline{\infty}$ we discover that $U_1(\mathbb{Z})_{\overline{\infty}}$ contains at most 2 points and the same holds for $U_1(\mathbb{Z})_{\overline{\infty_-}}$. Moreover the action of $\langle\eta, \iota\rangle$ on $C(\mathbb{Z})$ tells that $U_1(\mathbb{Z})_{\iota(\overline{\alpha})}$, $U_1(\mathbb{Z})_{\eta(\overline{\alpha})}$ and $U_1(\mathbb{Z})_{\eta\iota(\overline{\alpha})}$ are sets containing exactly 2 elements. Hence

$$U_1(\mathbb{Z}) = U_1(\mathbb{Z})_{\overline{\alpha}} \cup U_1(\mathbb{Z})_{\iota(\overline{\alpha})} \cup U_1(\mathbb{Z})_{\eta(\overline{\alpha})} \cup U_1(\mathbb{Z})_{\eta\iota(\overline{\alpha})} \cup U_1(\mathbb{Z})_{\overline{\infty_-}} \cup U_1(\mathbb{Z})_{\overline{\infty}}$$

contains at most 12 elements. Looking at the orbits of the action of $\langle \eta, \iota \rangle$ on $U_1(\mathbb{Z})$ we see that $\#U_1(\mathbb{Z}) \equiv 2 \pmod 4$, hence $\#U_1(\mathbb{Z}) \leq 10$. Since $U_1(\mathbb{Z})$ contains ∞, ∞_- and all the images by $\langle \eta, \iota \rangle$ of $U_1(\mathbb{Z})_{\overline{\alpha}}$ we conclude that $\#U_1(\mathbb{Z}) = 10$.

Applying our method to the point $\overline{\gamma}$ we see that $U_0(\mathbb{Z})_{\overline{\gamma}}$ contains at most two points, one of them being γ. Moreover solving the equations $\kappa^* \overline{F_i} = 0$ we see that if there is another point γ' in $U_0(\mathbb{Z})_{\overline{\gamma}}$ then there exist $n_1, n_2 \in \mathbb{Z}$ such that

$$j_b(\gamma') = 39G_1 + 17G_2 + 5n_1\widetilde{G_1} + 5n_2\widetilde{G_2}\,.$$

Using the Mordell-Weil sieve (see [79]) we derive a contradiction: for all integers n_1, n_2, the image in $J(\mathbb{F}_7)$ of $39G_1+17G_2+5n_1\widetilde{G_1}+5n_2\widetilde{G_2}$ is not contained in $j_b(C(\mathbb{F}_7))$. We deduce that

$$U_0(\mathbb{Z})_{\overline{\gamma}} = \{\gamma\}\,.$$

Applying our method to to ε we see that $U_0(\mathbb{Z})_\varepsilon$ contains at most 2 points corresponding to two different solutions to the equations $\kappa^* \overline{F_i} = 0$. We can see that one of the two solutions does not lift to a point in $U_0(\mathbb{Z})_\varepsilon$ in the same way we excluded the existence of $\gamma' \in U_0(\mathbb{Z})_{\overline{\gamma}}$. Hence $U_0(\mathbb{Z})_\varepsilon$ has cardinality at most 1. Using that for every $Q \in C(\mathbb{F}_p)$ and every automorphism ω of C we have $\#U_0(\mathbb{Z})_Q = \#U_0(\mathbb{Z})_{\omega(Q)}$, we deduce that

$$U_0(\mathbb{Z}) = U_0(\mathbb{Z})_{\overline{\gamma}} \cup U_0(\mathbb{Z})_{\iota(\overline{\gamma})} \cup U_0(\mathbb{Z})_{\eta(\overline{\gamma})} \cup U_0(\mathbb{Z})_{\eta\iota(\overline{\gamma})} \cup U_0(\mathbb{Z})_\varepsilon \cup U_0(\mathbb{Z})_{\iota(\varepsilon)}$$

contains at most 6 points. Looking at the orbits of the action of $\langle \eta, \iota \rangle$ on $U_0(\mathbb{Z})$ we see that $\#U_0(\mathbb{Z}) \equiv 0 \pmod 4$, hence $\#U_4(\mathbb{Z}) \leq 4$, and since $U_0(\mathbb{Z})$ contains the orbit of γ we conclude that $\#U_0(\mathbb{Z}) = 4$. Finally

$$\#C(\mathbb{Z}) = \#U_0(\mathbb{Z}) + \#U_1(\mathbb{Z}) = 4 + 10 = 14\,.$$

1.9 Some further remarks

1.9.1 Complex uniformisations of some of the objects involved

Let C be a projective curve over $\mathbb{Q}$, smooth, and geometrically irreducible, and let g be its genus. The universal cover of $P^\times(\mathbb{C})$ is described in [16], Propositions 4.5 and 4.6. The covering space, denoted D_τ, is $\mathrm{M}_{1,g}(\mathbb{C}) \times \mathrm{M}_{g,1}(\mathbb{C}) \times \mathbb{C}$, hence a $\mathbb{C}$-vector space of dimension $2g+1$. The biextension structure on $\mathrm{M}_{1,g}(\mathbb{C}) \times \mathrm{M}_{g,1}(\mathbb{C}) \times \mathbb{C}$ is trivial, that is, for all x, x_1, x_2 in $\mathrm{M}_{1,g}(\mathbb{C})$, all y, y_1, y_2 in $\mathrm{M}_{g,1}(\mathbb{C})$, and all z_1, z_2 in $\mathbb{C}$, we have:

$$\begin{aligned}(x_1, y, z_1) +_1 (x_2, y, z_2) &= (x_1 + x_2, y, z_1 + z_2)\,,\\ (x, y_1, z_1) +_2 (x, y_2, z_2) &= (x, y_1 + y_2, z_1 + z_2)\,.\end{aligned} \tag{1.9.1.1}$$

The fundamental group $\pi_1(P^\times(\mathbb{C}),1)$ is

$$Q^u(\mathbb{Z}) := \left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1_{2g} & y \\ 0 & 0 & 1 \end{pmatrix} : x \in \mathrm{M}_{1,2g}(\mathbb{Z}),\, y \in \mathrm{M}_{2g,1}(\mathbb{Z}),\, z \in \mathbb{Z} \right\}, \tag{1.9.1.2}$$

also known as a Heisenberg group. Its action on D_τ is given in [16, (4.5.3)].

Now recall the definition of T in (1.2.12). As $\mathrm{M}_{2g,1}(\mathbb{Z})$ is the lattice of $J(\mathbb{C})$, and $\mathrm{M}_{1,2g}(\mathbb{Z})$ the lattice of $J^\vee(\mathbb{C})$, each f_i is given by an antisymmetric matrix $f_{i,\mathbb{Z}}$ in $\mathrm{M}_{2g,2g}(\mathbb{Z})$ such that for all y in $\mathrm{M}_{2g,1}(\mathbb{Z})$ we have $f_i(y) = y^t{\cdot}f_{i,\mathbb{Z}}$, and by a complex matrix $f_{i,\mathbb{C}}$ in $\mathrm{M}_{g,g}(\mathbb{C})$ such that for all v in $\mathrm{M}_{g,1}(\mathbb{C})$, for each i we have $f_i(v) = v^t{\cdot}f_{i,\mathbb{C}}$ in $\mathrm{M}_{1,g}(\mathbb{C})$. For more details about this description of the f_i see the beginning of [16, P4.7]. Then we have

$$\pi_1(T(\mathbb{C})) = \left\{ \begin{pmatrix} 1_{\rho-1} & m{\cdot}f(y) & z \\ 0 & 1_{2g} & y \\ 0 & 0 & 1 \end{pmatrix} : y \in \mathrm{M}_{2g,1}(\mathbb{Z}),\, z \in \mathrm{M}_{\rho-1,1}(\mathbb{Z}) \right\}, \tag{1.9.1.3}$$

with $m{\cdot}f(y) \in \mathrm{M}_{\rho-1,2g}(\mathbb{Z})$ with rows the $m{\cdot}y^t{\cdot}f_{i,\mathbb{Z}}$. So, $\pi_1(T(\mathbb{C}))$ is a central extension of $\mathrm{M}_{2g,1}(\mathbb{Z})$ by $\mathrm{M}_{\rho-1,1}(\mathbb{Z})$, with commutator pairing sending (y,y') to $(2my^t{\cdot}f_{i,\mathbb{Z}}{\cdot}y')_i$.

The universal covering $\widetilde{T(\mathbb{C})}$ is given by

$$\begin{aligned} \widetilde{T(\mathbb{C})} &= \{(m{\cdot}(c+f(v)), v, w) : v \in \mathrm{M}_{g,1}(\mathbb{C}),\, w \in \mathrm{M}_{\rho-1,1}(\mathbb{C})\} \\ &\subset \mathrm{M}_{\rho-1,g}(\mathbb{C}) \times \mathrm{M}_{1,g}(\mathbb{C}) \times \mathrm{M}_{\rho-1,1}(\mathbb{C})\,, \end{aligned} \tag{1.9.1.4}$$

with $m{\cdot}(c+f(v)) \in \mathrm{M}_{\rho-1,g}(\mathbb{C})$ with rows the $m{\cdot}(\widetilde{c_i}+v^t{\cdot}f_{i,\mathbb{C}})$ with $\widetilde{c_i}$ a lift of c_i in $\mathrm{M}_{1,g}(\mathbb{C})$. The action of $\pi_1(T(\mathbb{C}),1)$ on $\widetilde{T(\mathbb{C})}$ is given again, with the necessary changes, by [16, (4.5.3)].

Now that we know $\pi_1(T(\mathbb{C}),1)$ we investigate which quotient of $\pi_1(C(\mathbb{C}),b)$ it is, via $\widetilde{j_b}\colon C(\mathbb{C}) \to T(\mathbb{C})$. We consider the long exact sequence of homotopy groups induced by the $\mathbb{C}^{\times,\rho-1}$-torsor $T(\mathbb{C}) \to J(\mathbb{C})$, taking into account that $\mathbb{C}^{\times,\rho-1}$ is connected and that $\pi_2(J(\mathbb{C})) = 0$:

$$\pi_1(\mathbb{C}^{\times,\rho-1},1) \hookrightarrow \pi_1(T(\mathbb{C}),1) \twoheadrightarrow \pi_1(J(\mathbb{C}),0)\,. \tag{1.9.1.5}$$

Again, $\pi_1(T(\mathbb{C}),1)$ is a central extension of the free abelian group $\pi_1(J(\mathbb{C}),0)$ by $\mathbb{Z}^{\rho-1}$, and from the matrix description we deduce that the ith coordinate of the commutator pairing is given by $mf_i\colon \mathrm{H}_1(J(\mathbb{C}),\mathbb{Z}) \to \mathrm{H}_1(J^\vee(\mathbb{C}),\mathbb{Z}) = \mathrm{H}_1(J(\mathbb{C}),\mathbb{Z})^\vee$. The $\mathbb{Z}$-module of antisymmetric $\mathbb{Z}$-valued pairings on $\mathrm{H}_1(J^\vee(\mathbb{C}),\mathbb{Z})$ is $\bigwedge^2 \mathrm{H}^1(J(\mathbb{C}),\mathbb{Z}) = \mathrm{H}^2(J(\mathbb{C}),\mathbb{Z})$, and mf_i is the cohomology class (first Chern class) of the $\mathbb{C}^\times$-torsor T_i:

$$mf_i = c_1(T_i) \quad \text{in } \mathrm{H}^2(J(\mathbb{C}),\mathbb{Z}). \tag{1.9.1.6}$$

There is a central extension

$$\mathrm{H}_2(J(\mathbb{C}),\mathbb{Z}) \hookrightarrow E \twoheadrightarrow \pi_1(J(\mathbb{C}),0) \tag{1.9.1.7}$$

that is universal in the sense that every central extension of $\pi_1(J(\mathbb{C}),0)$ by a free abelian group arises by pushout from $\mathrm{H}_2(J(\mathbb{C}),\mathbb{Z})$. We denote

$$G := \pi_1(C(\mathbb{C}),b)\,. \tag{1.9.1.8}$$

The map $j_b\colon C \to J$ gives $G \to \pi_1(J(\mathbb{C}),0)$, and this is the maximal abelian quotient. The second quotient in the descending central series of G gives the central extension:

(1.9.1.9)

$$[G,G]/[G,[G,G]] \hookrightarrow G/[G,[G,G]] \twoheadrightarrow G/[G,G] = G^{\mathrm{ab}} = \pi_1(J(\mathbb{C}),0)\,.$$

This extension (1.9.1.9) arises from (1.9.1.7) by pushout via a morphism from $\mathrm{H}_2(J(\mathbb{C}),\mathbb{Z})$ to $[G,G]/[G,[G,G]]$:

$$\begin{array}{ccccc} \mathrm{H}_2(J(\mathbb{C}),\mathbb{Z}) & \hookrightarrow & E & \twoheadrightarrow & G^{\mathrm{ab}} \\ \downarrow & & \downarrow & & \| \\ [G,G]/[G,[G,G]] & \hookrightarrow & G/[G,[G,G]] & \twoheadrightarrow & G^{\mathrm{ab}}\,. \end{array} \tag{1.9.1.10}$$

The left vertical arrow is surjective because commutators of lifts in E of elements of G^{ab} are mapped to the commutators of lifts in $G/[G,[G,G]]$, and so give generators of $[G,G]/[G,[G,G]]$.

From the usual presentation of G with generators $\alpha_1,\beta_1,\ldots,\alpha_g,\beta_g$, with the only relation $[\alpha_1,\beta_1]\cdots[\alpha_g,\beta_g]=1$, we see that the obstruction in lifting $G \to G^{\mathrm{ab}}$ to $G \to E$ in the top row of (1.9.1.10) is the image of $[\alpha_1,\beta_1]\cdots[\alpha_g,\beta_g]$ in $\mathrm{H}_2(J(\mathbb{C}),\mathbb{Z})$. This image is a generator of the image of $\mathrm{H}_2(C(\mathbb{C}),\mathbb{Z})$ under j_b. So the pushout in (1.9.1.10) factors through the pushout by the quotient of $\mathrm{H}_2(J(\mathbb{C}),\mathbb{Z})$ by $\mathrm{H}_2(C(\mathbb{C}),\mathbb{Z})$:

$$\begin{array}{ccccc} \mathrm{H}_2(J(\mathbb{C}),\mathbb{Z})/\mathrm{H}_2(C(\mathbb{C}),\mathbb{Z}) & \hookrightarrow & E' & \twoheadrightarrow & G^{\mathrm{ab}} \\ \downarrow\!\!\downarrow & & \downarrow\!\!\downarrow & & \| \\ [G,G]/[G,[G,G]] & \hookrightarrow & G/[G,[G,G]] & \twoheadrightarrow & G^{\mathrm{ab}}\,. \end{array} \tag{1.9.1.11}$$

Using again the presentation of G we can split this morphism of extensions, and, using that $\mathrm{H}_2(J(\mathbb{C}),\mathbb{Z})/\mathrm{H}_2(C(\mathbb{C}),\mathbb{Z})$ is generated by commutators of lifts of elements of G^{ab}, conclude that all vertical arrows in (1.9.1.11) are isomorphisms.

In particular, we have that $[G,G]/[G,[G,G]]$ is the same as $\mathrm{H}_2(J(\mathbb{C}),\mathbb{Z})/\mathrm{H}_2(C(\mathbb{C}),\mathbb{Z})$. From (1.9.1.6) we see that the sub-$\mathbb{Z}$-module of $\mathrm{H}^2(J(\mathbb{C}),\mathbb{Z}(1))$ (note the Tate twist, now we take the Hodge structures into account) spanned by the mf_i is obtained in 4 steps:

take the kernel of $\mathrm{H}^2(J(\mathbb{C}),\mathbb{Z}(1)) \to \mathrm{H}^2(C(\mathbb{C}),\mathbb{Z}(1))$, take the $(0,0)$-part, then $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts, through the Galois group of a finite extension of $\mathbb{Q}$, take the invariants, then take the image of the multiplication by m on that.

Dually, this means that $\pi_1(T(\mathbb{C}),1)$ arises as the pushout

(1.9.1.12)

$$\begin{array}{ccccc} \mathrm{H}_2(J(\mathbb{C}),\mathbb{Z}(-1))/\mathrm{H}_2(C(\mathbb{C}),\mathbb{Z}(-1)) & \hookrightarrow & G/[G,[G,G]] & \twoheadrightarrow & G^{\mathrm{ab}} \\ \downarrow & & \downarrow & & \| \\ \big((\mathrm{H}_2(J(\mathbb{C}),\mathbb{Z}(-1))/\mathrm{H}_2(C(\mathbb{C}),\mathbb{Z}(-1)))_{(0,0)}\big)_{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})} & \hookrightarrow & \pi_1(T(\mathbb{C}),1) & \twoheadrightarrow & G^{\mathrm{ab}}, \end{array}$$

where the subscript $(0,0)$ means the largest quotient of type $(0,0)$, where the subscript $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ means co-invariants modulo torsion, and where the left vertical map is m times the quotient map. We repeat that the morphism from $\pi_1(C(\mathbb{C})) = G$ to $\pi_1(T(\mathbb{C}),1)$ given by the middle vertical map is induced by $\widetilde{j_b}\colon C(\mathbb{C}) \to J(\mathbb{C})$.

1.9.2 Finiteness of rational points

In this section we reprove Faltings's finiteness result [43] in the special case where $r < g + \rho - 1$. This was already done in [8], Lemma 3.2 (where the base field is either $\mathbb{Q}$ or imaginary quadratic). We begin by collecting some ingredients on good formal coordinates of the $\mathbb{G}_{\mathrm{m}}$-biextension $P^{\times,\rho-1} \to J \times J^{\vee,\rho-1}$ over $\mathbb{Q}$, and on what C looks like in such coordinates.

Formal trivialisations

Let A, B and G be connected smooth commutative group schemes over a field $k \supset \mathbb{Q}$, and let $E \to A \times B$ be a commutative G-biextension. Let a be in $A(k)$, $b \in B(k)$ and $e \in E(k)$. For $n \in \mathbb{N}$, let $A^{a,n}$ be the nth infinitesimal neighborhood of a in A, hence its coordinate ring is $\mathcal{O}_{A,a}/m_a^{n+1}$. We use similar notation for B with b, and E with e, and also for the points 0 of A, B and E, and, similarly, the formal completion of A at a is denoted by $A^{a,\infty}$, etc. We also use such notation in a relative context, for example, for the group schemes $E \to B$ and $E \to A$. We view completions as $A^{a,\infty}$ as set-valued functors on the category of local k-algebras with residue field k such that every element of the maximal ideal is nilpotent. For such a k-algebra R, $A^{a,\infty}(R)$ is the inverse image of a under $A(R) \to A(k)$. Then $A^{0,\infty}$ is the formal group of A.

We now want to show that the formal $G^{0,\infty}$-biextension $E^{0,\infty} \to A^{0,\infty} \times B^{0,\infty}$ is isomorphic to the trivial biextension (the object $G^{0,\infty} \times A^{0,\infty} \times B^{0,\infty}$ with $+_1$ given by addition on the 1st and 2nd coordinate, and $+_2$ by addition on the 1st and 3rd coordinate). As exp for $A^{0,\infty}$ gives a functorial isomorphism $T_{A/k}(0) \otimes_k \mathbb{G}_{\mathrm{a}_k}^{0,\infty} \to A^{0,\infty}$, and similarly for

B and G, it suffices to prove this triviality for $\mathbb{G}_{\mathrm{a}}^{0,\infty}$-biextensions of $\mathbb{G}_{\mathrm{a}}^{0,\infty} \times \mathbb{G}_{\mathrm{a}}^{0,\infty}$ over k. One easily checks that the group of automorphisms of the trivial $\mathbb{G}_{\mathrm{a}}^{0,\infty}$-biextension of $\mathbb{G}_{\mathrm{a}}^{0,\infty} \times \mathbb{G}_{\mathrm{a}}^{0,\infty}$ over k that induce the identity on all three $\mathbb{G}_{\mathrm{a}}^{0,\infty}$'s is $(k,+)$, with $c \in k$ acting as $(g,a,b) \mapsto (g + cab, a, b)$. As this group is commutative, it then follows that the group of automorphisms of the $G^{0,\infty}$-biextension $E^{0,\infty} \to A^{0,\infty} \times B^{0,\infty}$ that induce identity on $G^{0,\infty}$, $A^{0,\infty}$,and $B^{0,\infty}$, is equal to the k-vector space of k-bilinear maps $T_{A/k}(0) \times T_{B/k}(0) \to T_{G/k}(0)$. This indicates how to trivialise $E^{0,\infty}$. We choose a section $\tilde{e}$ of the G-torsor $E \to A \times B$ over the closed subscheme $A^{0,1} \times B^{0,1}$ of $A \times B$:

$$\begin{array}{ccc} & \overset{\tilde{e}}{\nearrow} & E \\ & & \big\downarrow \\ A^{0,1} \times B^{0,1} & \longrightarrow & A \times B\,, \end{array} \qquad \text{with } \tilde{e}(0,0) = e \text{ in } E(k).$$

Note that

$$\mathcal{O}(A^{0,1} \times B^{0,1}) = (k \oplus m_{A^{0,1}}) \otimes (k \oplus m_{B^{0,1}}) = k \oplus m_{A^{0,1}} \oplus m_{B^{0,1}} \oplus (m_{A^{0,1}} \otimes m_{B^{0,1}})\,.$$

Hence two such $\tilde{e}$ differ by a k-algebra morphism from $k \oplus m_{G^{0,2}} = k \oplus m_{G^{0,1}} \oplus \mathrm{Sym}^2 m_{G^{0,1}}$ (use the exponential map) to $k \oplus m_{A^{0,1}} \oplus m_{B^{0,1}} \oplus (m_{A^{0,1}} \otimes m_{B^{0,1}})$, hence by a triple of k-linear maps from $m_{G^{0,1}}$ to $m_{A^{0,1}}$, $m_{B^{0,1}}$, and $m_{A^{0,1}} \otimes m_{B^{0,1}}$. The linear maps $m_{G^{0,1}} \to m_{A^{0,1}}$ and $m_{G^{0,1}} \to m_{B^{0,1}}$ correspond to the differences on $A^{0,1} \times B^{0,0}$ and on $A^{0,0} \times B^{0,1}$, respectively. There are unique such linear maps such that the adjusted $\tilde{e}$ is compatible with the given trivialisations of $E \to A \times B$ over $A^{0,1} \times B^{0,0}$ and over $A^{0,0} \times B^{0,1}$. In geometric terms, $\tilde{e}$, assumed to be adjusted, is then a splitting of $T_G(0)_B \hookrightarrow T_{E/B}(0) \twoheadrightarrow T_A(0)_B$ over $B^{0,1}$ that is compatible with the already given splitting over $0 \in B(k)$, and it is also a splitting of $T_G(0)_A \hookrightarrow T_{E/A}(0) \twoheadrightarrow T_B(0)_A$ over $A^{0,1}$ that is compatible with the already given splitting over $0 \in A(k)$. The splitting over $B^{0,1}$ gives an isomorphism from $(T_G(0) \oplus T_A(0))_{B^{0,1}}$ to $(T_{E/B})_{B^{0,1}}$. So the exponential map, for $+_1$, for the pullback to $B^{0,1}$ of $E \to B$, gives an isomorphism of formal groups over $B^{0,1}$:

$$\big((T_G(0) \oplus T_A(0)) \otimes_k \mathbb{G}_{\mathrm{a}}^{0,\infty}\big)_{B^{0,1}} \hookrightarrow\!\!\!\!\rightarrow E^{0,\infty}_{B^{0,1}}\,.$$

Viewing $E^{0,\infty}_{B^{0,1}}$ as the tangent space at the zero section of the pullback to $A^{0,\infty}$ of $E \to A$, this isomorphism gives a splitting of $T_G(0)_A \hookrightarrow T_{E/A}(0) \twoheadrightarrow T_B(0)_A$ over $A^{0,\infty}$. The exponential map for $+_2$ for the pulback to $A^{0,\infty}$ of $E \to A$ then gives an isomorphism of formal groups over $A^{0,\infty}$:

$$G^{0,\infty} \times B^{0,\infty} \times A^{0,\infty} = (G^{0,\infty} \times B^{0,\infty})_{A^{0,\infty}} \hookrightarrow\!\!\!\!\rightarrow E^{0,\infty}_{A^{0,\infty}/A^{0,\infty}} = E^{0,\infty}\,,$$

where $E^{0,\infty}_{A^{0,\infty}/A^{0,\infty}}$ denotes the completion along the zero section of the pullback via $A^{0,\infty} \to A$ of $E \to A$. The compatibility between $+_1$ and $+_2$ on E ensures that this

isomorphism is an isomorphism of biextensions, with the trivial biextension structure on the left.

Now that we know what good formal coordinates at 0 in $E(k)$ are, we look at the point e in $E(k)$, over (a,b) in $(A\times B)(k)$. We produce an isomorphism $E^{0,\infty}\to E^{e,\infty}$, using the partial group laws. Let E_b be the fibre over b of $E\to B$. We choose a section

$$\begin{array}{ccc} & & E_b \\ & \overset{\tilde{e}_1}{\nearrow} & \downarrow \\ A^{a,1}\times\{b\} & \longrightarrow & A\times\{b\} \end{array} \qquad \text{with } \tilde{e}_1(a,b)=e \text{ in } E(k).$$

The exponentials for the group laws of E_b and A then give a section

$$\begin{array}{ccc} & & E_b \\ & \overset{\tilde{e}_1^{\infty}}{\nearrow} & \downarrow \\ A^{a,\infty}\times\{b\} & \longrightarrow & A\times\{b\}\,, \end{array}$$

that we view as an $A^{a,\infty}$-valued point of E_b, and as a section of the group scheme $E_{A^{a,\infty}}\to A^{a,\infty}$, with group law $+_2$. The translation by $\tilde{e}_1^{\infty}$ on this group scheme induces translation by b on $B_{A^{a,\infty}}$, and maps $(a,0)$, the 0 element of E_a, to e. Hence it induces an isomorphism of formal schemes $E^{(a,0),\infty}\to E^{e,\infty}$. In order to get an isomorphism $E^{0,\infty}\to E^{(a,0),\infty}$, we repeat the process above, but with the roles of A and B exchanged. We choose a section $\tilde{0}_2\colon\{a\}\times B^{0,1}\to E_a$ of $E_a\to\{a\}\times B$. Then the exponential for $+_2$ gives us a section $\tilde{0}_2^{\infty}\colon\{a\}\times B^{0,\infty}\to E_a$ of $E_a\to\{a\}\times B$. This $\tilde{0}_2^{\infty}$ is a section of the group scheme $E_{B^{0,\infty}}\to B^{0,\infty}$, and the translation on it by $\tilde{0}_2^{\infty}$ sends 0 in $E(k)$ to $(a,0)$, hence gives an isomorphism of formal schemes $E^{0,\infty}\to E^{(a,0),\infty}$. Composition then gives us an isomorphism $E^{0,\infty}\to E^{e,\infty}$, and the good formal coordinates on E at $0\in E(k)$ give what we call good formal coordinates at e. Similarly, we get a section $\widetilde{0}_1^{\infty}$ of $E_{A^{0,\infty}}\to A^{0,\infty}$ and a section $\widetilde{e}_2^{\infty}$ of $E_{B^{b,\infty}}\to B^{b,\infty}$ giving isomorphisms $E^{0,\infty}\to E^{(0,b),\infty}$ and $E^{(0,b),\infty}\to E^{e,\infty}$, hence by composition a 2nd isomorphism $E^{0,\infty}\to E^{e,\infty}$. These isomorphisms are equal for a unique choice of $\tilde{0}_1$ and $\tilde{e}_2$ (given the choices of $\tilde{0}_2$ and $\tilde{e}_1$).

In Section 1.9.2 we will use that these isomorphisms transport all additions that occur in (1.4.4) to additions in $E^{0,\infty}$ and therefore to additions in the trivial formal biextension.

Zariski density of the curve in formally trivial coordinates

Let C be as in the beginning of Section 1.2. Let $\widetilde{C(\mathbb{C})}$ be the inverse image of $C(\mathbb{C})$ under the universal cover $\widetilde{T(\mathbb{C})}\to T(\mathbb{C})$. Then $\widetilde{C(\mathbb{C})}$ is connected since $\widetilde{j_b}\colon C\to T$ gives a surjection on complex fundamental groups. Now we consider the complex analytic

variety $\widetilde{T(\mathbb{C})}$ as a complex algebraic variety via the bijection $\widetilde{T(\mathbb{C})} = \mathbb{C}^{g+\rho-1}$ as given in (1.9.1.4). The analytic subset $\widetilde{C(\mathbb{C})}$ contains the orbit of 0 under $\pi_1(T(\mathbb{C}), 1)$. This orbit surjects to the lattice of $J(\mathbb{C})$ in $\mathrm{M}_{g,1}(\mathbb{C})$, and over each lattice point, its fibre in $\mathrm{M}_{\rho-1,1}(\mathbb{C})$ contains a translate of $2\pi i \mathrm{M}_{\rho-1,1}(\mathbb{Z})$. Hence this orbit is Zariski dense in $\mathbb{C}^{g+\rho-1}$. It follows that the formal completion of $\widetilde{C(\mathbb{C})}$ at any of its points is Zariski dense in $\mathbb{C}^{g+\rho-1}$: if a polynomial function on $\mathbb{C}^{g+\rho-1}$ is zero on such a completion, then it vanishes on the connected component of $\widetilde{C(\mathbb{C})}$ of that point, hence on $\widetilde{T(\mathbb{C})}$.

We express our conclusion in more algebraic terms: for $c \in C(\mathbb{C})$, with images $t \in T(\mathbb{C})$ and in $P^{\times,\rho-1}(\mathbb{C})$, each polynomial in good formal coordinates at t of the biextension $P^{\times,\rho-1} \to J \times J^\vee$ over $\mathbb{C}$ that vanishes on $\widetilde{j}_b(C^{c,\infty}_{\mathbb{C}})$, vanishes on $T^{t,\infty}_{\mathbb{C}}$. This statement then also holds with $\mathbb{C}$ replaced by any subfield, or even any subring of the form $\mathbb{Z}_{(p)}$ with p a prime number, or the localisation of $\overline{\mathbb{Z}}$ (the integral closure of $\mathbb{Z}$ in $\mathbb{C}$) at a maximal ideal.

The p-adic closure in good formal coordinates

We stay in the situation of Section 1.2, but we denote $G := \mathbb{G}_{\mathrm{m}}^{\rho-1}$, $A := J$ and $B := J^{\vee,0\rho-1}$, and $E := P^{\times,\rho-1}$. Let d_G, d_A, and d_B be their dimensions: $d_G = \rho - 1$, $d_A = g$ and $d_B = (\rho-1)g$.

Let $p > 2$ be a prime number. From Section 1.9.2 and Lemma 1.5.1.1 we conclude that we can choose *formal* parameters for E at 0, over $\mathbb{Z}_{(p)}$, such that they converge on the residue polydisk $E(\mathbb{Z}_p)_{\overline{0}}$, and such that they induce the trivial biextension structure on $\mathbb{Z}_p^{d_G} \times \mathbb{Z}_p^{d_A} \times \mathbb{Z}_p^{d_B}$. We keep the notation of Section 1.9.2, for e in $E(\mathbb{Z}_p)$, lying over (a, b) in $(A \times B)(\mathbb{Z}_p)$. This e plays the role that $\widetilde{t}$ has at the beginning of Section 1.4. As explained at the end of Section 1.9.2, we may and do assume that e is in $E(\mathbb{Z}_p)_{\overline{0}}$, and hence $a \in A(\mathbb{Z}_p)_{\overline{0}}$ and $b \in B(\mathbb{Z}_p)_{\overline{0}}$.

Assume now that, as in Section 1.4, for $i, j \in \{1, \ldots, r\}$, we have x_i in $A(\mathbb{Z}_p)_{\overline{0}}$ and y_j in $B(\mathbb{Z}_p)_{\overline{0}}$, and $e_{i,j}$ in $E(\mathbb{Z}_p)_{\overline{0}}$ over (x_i, y_j), and r_i in $E(\mathbb{Z}_p)_{\overline{0}}$ over (x_i, b) and s_j in $E(\mathbb{Z}_p)_{\overline{0}}$ over (a, y_j). We denote the images of all these elements under the bijection

$$E(\mathbb{Z}_p)_{\overline{0}} \longrightarrow \mathbb{Z}_p^{d_G} \times \mathbb{Z}_p^{d_A} \times \mathbb{Z}_p^{d_B}$$

as follows:

$$\begin{aligned} x_i &\mapsto (0, x_i, 0)\,, & y_j &\mapsto (0, 0, y_j)\,, & e_{i,j} &\mapsto (g_{i,j}, x_i, y_j) \\ r_i &\mapsto (r_i', x_i, b)\,, & s_j &\mapsto (s_j', a, y_j)\,, & e &\mapsto (e', a, b)\,. \end{aligned}$$

Then, by a straightforward computation, the image of $D(n)$ as defined in (1.4.4) is

$$\left(e' + \sum_i n_i r_i' + \sum_j n_j s_j' + \sum_{i,j} n_i n_j g_{i,j},\ a + \sum_i n_i x_i,\ b + \sum_j n_j y_j \right) \quad \mathbb{Z}_p^{d_G} \times \mathbb{Z}_p^{d_A} \times \mathbb{Z}_p^{d_B}.$$

The conclusion is that in these coordinates, the map

$$\kappa\colon \mathbb{Z}_p^r \longrightarrow \mathbb{Z}_p^{d_G} \times \mathbb{Z}_p^{d_A} \times \mathbb{Z}_p^{d_B}$$

is a polynomial map, hence the Zariski closure of its image is an algebraic variety of dimension at most r.

Proof of finiteness

The proof is by contradiction. So assume that $r < g + \rho - 1$, and that $C(\mathbb{Q})$ is infinite. Let $p > 2$ be a prime number. Then there is a $u \in C(\mathbb{F}_p)$ such that the residue disk $C(\mathbb{Z}_p)_u$ contains infinitely many elements of $C(\mathbb{Q})$, hence infinitely many elements in the image of κ of Section 1.4.10. By construction, $\kappa(\mathbb{Z}_p^r)$ is contained in $T(\mathbb{Z}_p)_t$. The image of $T(\mathbb{Z}_p)_t$ in $\mathbb{Z}_p^{d_G} \times \mathbb{Z}_p^{d_A} \times \mathbb{Z}_p^{d_B}$ is $\mathbb{Z}_p^{\rho-1} \times \mathbb{Z}_p^g$, with $\mathbb{Z}_p^g$ embedded in $\mathbb{Z}_p^{d_A} \times \mathbb{Z}_p^{d_B}$ as a sub-$\mathbb{Z}_p$-module. By the previous section, the Zariski closure of $\kappa(\mathbb{Z}_p^r)$ in $\mathbb{Z}_p^{d_G} \times \mathbb{Z}_p^{d_A} \times \mathbb{Z}_p^{d_B}$ is of dimension at most r. Hence there are non-zero polynomial functions on $\mathbb{Z}_p^{\rho-1} \times \mathbb{Z}_p^g$ that are zero on infinitely many points of $C(\mathbb{Z}_p)_u$, and hence are zero on a non-empty open smaller disk. This contradicts, via a ring morphism $\mathbb{Z}_p \to \mathbb{C}$, the conclusion of Section 1.9.2.

1.9.3 The relation with p-adic heights

We want to compare the approach to quadratic Chabauty in this article to the one in [8], by answering the question: which local analytic coordinates on $T(\mathbb{Z}_p)$ and $C(\mathbb{Q}_p)$ lead to the equations, in terms of p-adic heights, for the quadratic Chabauty set $C(\mathbb{Q}_p)_2$ in [8]? Before we do this, we note that the Poincaré biextension has played a role in Arakelov theory, and in the theory of p-adic heights, since a long time: see [101], [73] and [76]. Moreover, [21] gives a detailed description how Kim's cohomological approach relates to p-adic heights in the context of $\mathbb{G}_{\mathrm{m}}$-torsors on abelian varieties.

Let $p > 2$ be a prime number of good reduction for C. We consider the Poincaré torsor as $\mathcal{M}^\times$ on $(J \times J)_{\mathbb{Q}_p}$ via (1.6.3.3), and we use the description of $\mathcal{M}^\times$ given in (1.6.3.13).

Let $\mathcal{D}$ be the subset $\mathrm{Div}^0(C_{\mathbb{Q}_p}) \times \mathrm{Div}^0(C_{\mathbb{Q}_p})$ made of pairs of divisors (D_1, D_2) having disjoint support. Let W be an isotropic complement of $\Omega^1_{C_{\mathbb{Q}_p}/\mathbb{Q}_p}(C_{\mathbb{Q}_p})$ in $\mathrm{H}^1_{\mathrm{dR}}(C_{\mathbb{Q}_p}/\mathbb{Q}_p)$ and let $\log\colon \mathbb{Q}_p^\times \to \mathbb{Q}_p$ be a group morphism extending the formal logarithm on $1 + p\mathbb{Z}_p$. With these choices made, Coleman and Gross ([28, (5.1)]) define the function (there denoted $\langle \cdot, \cdot \rangle$)

$$h_p\colon \mathcal{D} \to \mathbb{Q}_p\,,$$

the p-part of the p-adic height pairing. We define the function

$$\psi\colon \mathcal{M}^\times(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p$$

by demanding that for every effective D_1 and D_2 in $\mathrm{Div}(C_{\mathbb{Q}_p})$ of the same degree and every E in $\mathrm{Div}^0(C_{\mathbb{Q}_p})$, and every λ in $\mathbb{Q}_p^\times$, the element

$$\lambda\cdot\mathrm{Norm}_{D_1/\mathbb{Q}_p}(1)\otimes\mathrm{Norm}_{D_2/\mathbb{Q}_p}(1)^{-1}$$

in

$$\mathcal{M}^\times(\mathcal{O}_{C_{\mathbb{Q}_p}}(E),\Sigma(D_1)-\Sigma(D_2))=\Big(\mathrm{Norm}_{D_1/\mathbb{Q}_p}\mathcal{O}_{C_{\mathbb{Q}_p}}(E)\otimes\mathrm{Norm}_{D_2/\mathbb{Q}_p}\mathcal{O}_{C_{\mathbb{Q}_p}}(-E)\Big)^\times$$

is sent to

$$\psi(\lambda\cdot\mathrm{Norm}_{D_1/\mathbb{Q}_p}(1)\otimes\mathrm{Norm}_{D_2/\mathbb{Q}_p}(1)^{-1}):=h_p(D_1-D_2,E)+\log\lambda\,.$$

That this depends only on the linear equivalence classes of D_1-D_2 and E follows from (1.6.4.4), plus (see [28, Proposition 5.2]) the fact that h_p is biadditive, symmetric and, for any non-zero rational function f on $C_{\mathbb{Q}_p}$ and any D in $\mathrm{Div}^0(C_{\mathbb{Q}_p})$ with support disjoint from that of $\mathrm{div}(f)$, we have $h_p(D,\mathrm{div}(f))=\log(f(D))$. Moreover, expressing h_p in terms of a Green function G as in [20, Theorem 7.3], we deduce that, in each residue disk of $\mathcal{M}^\times(\mathbb{Z}_p)$, ψ is given by a power series. Let $\omega_1,\dots,\omega_g$ be a basis of $\Omega^1_{C_{\mathbb{Q}_p}/\mathbb{Q}_p}(C_{\mathbb{Q}_p})$. This basis gives a unique morphism of groups $\log_J\colon J(\mathbb{Q}_p)\to\mathbb{Q}_p^g$ that extends the logarithm of Lemma 1.5.1.1. We define

$$\Psi:=(\log_J\circ\mathrm{pr}_{J,1},\log_J\circ\mathrm{pr}_{J,2},\psi)\colon\mathcal{M}^\times(\mathbb{Q}_p)\longrightarrow\mathbb{Q}_p^g\times\mathbb{Q}_p^g\times\mathbb{Q}_p\,.$$

By the biadditivity of h_p, Ψ is a morphism of biextensions, with the trivial biextension structure on $\mathbb{Q}_p^g\times\mathbb{Q}_p^g\times\mathbb{Q}_p$ as in (1.9.1.1). As $p>2$, Ψ induces, from each residue polydisk to its image, a homeomorphism given by power series. Pulling back the coordinate functions on $\mathbb{Q}_p^{2g+1}$ gives, for every $x\in\mathcal{M}^\times(\mathbb{F}_p)$, coordinates on $\mathcal{M}^\times(\mathbb{Z}_p)_x$.

We describe $\widetilde{j_b}$ and κ in these coordinates. It is sufficient to describe, for each $i=1,\dots,\rho-1$, the map $\widetilde{j_{b,i}}\colon C\to T_i$, and from now on we omit the dependence on i. For each $c\in C(\mathbb{F}_p)$, on $T(\mathbb{Z}_p)_{\widetilde{j_b}(x)}$ we use the coordinates $x_1:=f^*t_1,\dots,x_g:=f^*t_g$, $z:=f^*t_{2g+1}$ where f is the map $T\to\mathcal{M}^\times$ and $t_1,\dots,t_{2g+1}$ are the coordinates on $\mathcal{M}^\times(\mathbb{Z}_p)_{\widetilde{j_b}(c)}$ we just defined. Since the map Ψ is a morphism of biextensions, for j in $\{1,\dots,g\}$, $x_j\circ\kappa$ is a polynomial of degree at most 1, and $z\circ\kappa$ is a polynomial of degree at most 2. As explained in Section 1.7, over $\mathbb{Z}_p$, $\widetilde{j_b}$ is given by a line bundle $\mathcal{L}$ over $(C\times C)_{\mathbb{Z}_p}$ rigidified along $(C\times\{b\})_{\mathbb{Z}_p}$ and along the diagonal with two sections l_b and l. Choosing a section that trivializes $\mathcal{L}$ on an open subset of $(C\times C)_{\mathbb{Z}_p}$ containing (b,b), (c,b), and (c,c) in $(C\times C)(\mathbb{F}_p)$ we get a divisor D on $(C\times C)_{\mathbb{Z}_p}$ whose support is disjoint from (c,b) and (c,c), and an isomorphism between $\mathcal{L}$ and $\mathcal{O}(D)$ on $(C\times C)_{\mathbb{Z}_p}$. After modifying D with a principal horizontal divisor and a principal vertical divisor

$D|_{C\times\{b\}}$ and $\mathrm{diag}^* D$ are both equal to the the zero divisor on $C_{\mathbb{Z}_p}$, hence l_b and l are the extensions of elements of $\mathbb{Q}_p$, interpreted as rational sections of $\mathcal{O}(D)$ on $(C\times C)_{\mathbb{Z}_p}$. By Propositions 1.7.5 and 1.7.8, there exists a unique $\lambda\in\mathbb{Q}_p^\times$ such that, for each $d\in C(\mathbb{Z}_p)_c$,

$$\widetilde{j_b}(d) = \lambda\cdot \mathrm{Norm}_{d/\mathbb{Z}_p}(1)\otimes \mathrm{Norm}_{b/\mathbb{Z}_p}(1)^{-1}\in \mathcal{M}^\times(j_b(d), D|_{\{d\}\times C})\,.$$

Since x_j is the j-th coordinate of $\log_J$ and since z is the pullback of ψ, we deduce that

$$x_1(\widetilde{j_b}(d)) = \int_b^d \omega_1, \ldots, \quad x_g(\widetilde{j_b}(d)) = \int_b^d \omega_g, \quad z(\widetilde{j_b}(d)) = h_p(d-b, D|_{\{d\}\times C}) + \log\lambda\,.$$

By [8, Proof of Theorem 1.2] and [10, Lemma 5.5], the function $d\mapsto h_p(d-b, D|_{\{d\}\times C})$ is a sum of double Coleman integrals.

It should now be easy to exactly interpret geometrically the cohomological approach, showing that in the coordinates used here, the equations for $C(\mathbb{Q}_p)_2$ are precisely equations for the intersection of $C(\mathbb{Q}_p)$ and the p-adic closure of $T(\mathbb{Z})$. For doing computations, one can do them in the geometric context of this article, or, as in [10], in terms of the étale fundamental group of C. The connection between these is then given by p-adic local systems on T.

Author contributions This project started with an idea of Edixhoven in December 2017. From then on Edixhoven and Lido worked together on the project. Section 1.8 is due entirely to Lido. Section 1.9 was written in July and August 2020.

Acknowledgements We thank Steffen Müller, Netan Dogra, Jennifer Balakrishnan, Kamal Khuri-Makdisi, Jan Vonk, Barry Mazur and Gerd Faltings for discussions and correspondence we had with them, Michael Stoll for suggesting the title of this article, Pim Spelier for his MSc thesis [98], and Sachi Hashimoto for the cartoon guide [51]. Finally, we thank the referee for their very thorough work and for making us increase the number of propositions and lemmas so that, hopefully, this article has become easier to parse and to digest.

Chapter 2

Formal biextensions and quadratic Chabauty

The proof of Theorem 1.4.10 in the previous chapter uses the formal logarithm of the two formal group laws associated to the biextension $P^{\times,\rho-1} \to J \times J^{\vee,\rho-1}$. Hence it uses that both laws are trivializable, that is they are both isomorphic to the additive law (over different bases).

In this chapter we study formal biextension laws and the main result implies that it is possible to trivialize both group laws of $P^{\times,\rho-1}$ simultaneously. We also prove that the power series defining the trivialization converge on the residue disk of the neutral element of $P^{\times,\rho-1}(\mathbb{Z}_p)$ if $p > 2$. This leads to another proof of Theorem 1.4.10. Notice that the triviality of commutative formal biextensions in characteristic zero was already treated in Section 1.9.2, but here we give a different proof, working directly with rings of power series.

2.1 Recap on formal group laws

Given a ring R, a *formal group law* of dimension d over R is a system $F = (F_1, \dots F_d)$ of power series in $2d$ indeterminates $x' = \{x'_1, \dots, x'_d\}$, $x'' = \{x''_1, \dots, x''_d\}$ such that

(I) $F(x', 0) = x'$ and $F(0, x'') = x''$;

(II) $F(x', F(x'', x''')) = F(F(x', x''), x''')$.

The first property implies that

$$F_i \equiv x'_i + x''_i \text{ mod terms of degree} \geq 2\,, \tag{2.1.1}$$

hence the substitution in the second property makes sense.

Let us rephrase this definition. Given a system of indeterminates $t = \{t_1, \dots, t_n\}$, the ring of formal power series $R[\![t]\!] = R[\![t_1, \dots, t_n]\!]$ is complete and separated with respect to the $(t_1, \dots, t_n)$-adic topology. Denoting $\hat{\otimes}_R$ the completed tensor product of linearly topologized R-modules (we give R the discrete topology), we have a unique continuous isomorphism of R-algebras

$$R[\![x'_1, \dots, x'_d, x''_1, \dots x''_d]\!] = R[\![x_1, \dots, x_d]\!] \hat{\otimes}_R R[\![x_1, \dots, x_d]\!] \tag{2.1.2}$$

sending x'_i to $x_i \otimes 1$ and x''_i to $1 \otimes x_i$. Hence, the choice of elements $F_1, \dots, F_d$ in the ring $R[\![x_1, \dots, x'_d, x''_1, \dots, x''_d]\!]$ is equivalent to the choice of a morphism of R-algebras $R[x_1, \dots, x_d] \to R[\![x_1, \dots, x_d]\!] \hat{\otimes}_R R[\![x_1, \dots, x_d]\!]$. Such a map extends to a continuous morphism of R-algebras

$$A \colon R[\![x_1, \dots, x_d]\!] \longrightarrow R[\![x_1, \dots, x_d]\!] \hat{\otimes}_R R[\![x_1, \dots, x_d]\!]$$

if and only if for each i we have $F_i(0, 0) = 0$, which is the case for formal group laws. We can also reformulate properties (I) and (II) in terms of A: denoting x the system of indeterminates $\{x_1, \dots, x_d\}$ and $e \colon R[\![x]\!] \to R$ the homomorphism evaluating power series at $x_1 = \dots = x_d = 0$, they are equivalent to the commutation of the following diagrams (2.1.3)

$$\begin{array}{ccc} R[\![x]\!] & \xrightarrow{A} & R[\![x]\!] \hat{\otimes}_R R[\![x]\!] \\ \downarrow{\scriptstyle A} & \searrow^{\mathrm{id}} & \downarrow{\scriptstyle \mathrm{id} \hat{\otimes}_R e} \\ R[\![x]\!] \hat{\otimes}_R R[\![x]\!] & \xrightarrow{e \hat{\otimes}_R \mathrm{id}} & R[\![x]\!] \end{array} \qquad \begin{array}{ccc} R[\![x]\!] & \xrightarrow{A} & R[\![x]\!] \hat{\otimes}_R R[\![x]\!] \\ \downarrow{\scriptstyle A} & & \downarrow{\scriptstyle \mathrm{id} \hat{\otimes}_R A} \\ R[\![x]\!] \hat{\otimes}_R R[\![x]\!] & \xrightarrow{A \hat{\otimes}_R \mathrm{id}} & R[\![x]\!] \hat{\otimes}_R R[\![x]\!] \hat{\otimes}_R R[\![x]\!] \end{array} .$$

Hence, by formal group law of dimension d, we also mean a continuous homomorphism of R-algebras $A \colon R[\![x_1, \dots, x_d]\!] \to R[\![x_1, \dots, x_d]\!] \hat{\otimes}_R R[\![x_1, \dots, x_d]\!]$ such that the above diagrams commute. Given two formal group laws A, B of dimensions a, b, a homomorphism between A and B is a continuous homomorphism $\phi \colon R[\![x_1, \dots, x_a]\!] \to R[\![x_1, \dots, x_b]\!]$ such that $(\phi \hat{\otimes}_R \phi) \circ A = B \circ \phi$.

We notice that the above diagrams say that $\mathrm{Spf}(R[\![x]\!])$, with multiplication given by $\mathrm{Spf}(A)$ and neutral element $\mathrm{Spf}(e)$, is a formal group scheme over R (the existence of the "inverse" morphism $\mathrm{Spf}(R[\![x]\!]) \to \mathrm{Spf}(R[\![x]\!])$ is proven in [45, P3, Proposition 1]).

Let $S \colon R[\![x]\!] \hat{\otimes}_R R[\![x]\!] \to R[\![x]\!] \hat{\otimes}_R R[\![x]\!]$ be the "symmetry" homomorphism. We say that a formal group law A is *commutative* if $S \circ A = A$. Equivalently a formal group law $F = (F_1, \dots, F_d)$ is commutative if $F(x', x'') = F(x'', x')$. An example of commutative formal group law is the *additive formal group law AD* of dimension d, defined by

$$AD(x_i) = x_i \hat{\otimes} 1 + 1 \hat{\otimes} x_i = x'_i + x''_i \, .$$

As proved in [54, Theorem 1], when $\mathbb{Q} \subset R$ the additive formal group law is the fundamental example of commutative formal group law: given a commutative formal group law

A of dimension d over a $\mathbb{Q}$-algebra R, there exists an isomorphism $\log_A\colon R[\![x]\!] \to R[\![x]\!]$ between the additive formal group law of dimension d and A. Moreover by [54, Proposition 1.6], such an isomorphism is unique when we require that it reduces to the identity modulo the ideal $(x_1, \dots, x_d)^2 \subset R[\![x]\!]$ and we refer to it as *formal logarithm of A*.

Given an R-algebra R', considered with the discrete topology, and a formal group law $A\colon R[\![x]\!] \to R[\![x]\!] \hat{\otimes}_R R[\![x]\!]$ over R, we denote $A_{R'}$ the formal group law over R' defined as $R' \hat{\otimes}_R A\colon R'[\![x]\!] \to R'[\![x]\!] \hat{\otimes}_{R'} R'[\![x]\!]$.

Finally, we recall that, given a formal group $A\colon R[\![x]\!] \to R[\![x]\!] \hat{\otimes}_R R[\![x]\!]$ of dimension a, we can talk about "points on A". Given an adic R-algebra S, namely an R-algebra which is also a separated and complete topological ring whose topology is induced by some ideal $I \subset S$, we define the set of S-valued points of A to be

$$A(S) := \mathrm{Hom}_{\mathrm{cont}}(R[\![x]\!], S) = (\mathfrak{N}_S)^a\,,$$

where $\mathfrak{N}_S$ denotes the ideal of topologically nilpotent elements in S. Since

$$\mathrm{Hom}_{\mathrm{cont}}(R[\![x]\!], S) \times \mathrm{Hom}_{\mathrm{cont}}(R[\![x]\!], S) = \mathrm{Hom}_{\mathrm{cont}}(R[\![x]\!] \hat{\otimes}_R R[\![x]\!], S)\,,$$

the formal group law A defines a group structure on $A(S)$ with neutral element $(0, \dots, 0)$. Hence A defines a covariant functor from the category of topological R-algebras to the category of groups. Vice versa suppose that A is a covariant functor from the category of adic R-algebras to the category of groups and suppose that there exists a positive integer a such that, functorially in S, we have a bijection $A(S) = (\mathfrak{N}_S)^a$ sending the neutral element to $(0, \dots, 0)$; then, by Yoneda's lemma, A is the functor of points of a formal group law. We call *formal groups* such functors.

We notice that a formal group law A is commutative if and only if for every S the group $A(S)$ is commutative. Moreover, given two formal group laws A and B, Yoneda's lemma tells us that giving a morphism between A and B is the same as giving a natural transformation between their functors of points, but going in the opposite direction.

Remark 2.1.4. One could give a more general notion of formal group by substituting $R[\![x]\!]$ with any *admissible* ring, (see Definition 7.1.2 in [41]), so that the relative tangent space of the formal group is not forced to be free. Anyway, we do not need this generality for our purposes.

2.2 Commutative formal biextension laws

One way to define a formal biextensions is by using the functorial point of view, as done in [80]. Given three formal groups

$$A, B, C\colon \text{Adic } R\text{-Algebras} \longrightarrow \text{Groups}$$

a biextension of A and B by C is a functor

$$D\colon \text{Adic } R\text{-Algebras} \longrightarrow \text{Sets}$$

such that functorially in S, the set $D(S)$ is a biextension of $A(S) \times B(S)$ by $C(S)$, in the sense of Section 1.2. Given three other formal groups F, G, H and a bi-extension K of F, G by H, a morphism between D and K is a triple of natural transformations $(A{\to}F, B{\to}G, D{\to}K)$ that commute with the (partial) group laws and with the natural transformations $D \to A \times B$ and $K \to F \times G$.

We can also give a "dual" definition, using rings of power series, which is more cumbersome, but useful in our proof of Theorem 2.2.3. Suppose we are given a ring R and three formal group laws

$$A\colon R[\![x]\!] \to R[\![x]\!] \hat{\otimes}_R R[\![x]\!]\,, \quad B\colon R[\![y]\!] \to R[\![y]\!] \hat{\otimes}_R R[\![y]\!]\,, \quad C\colon R[\![z]\!] \to R[\![z]\!] \hat{\otimes}_R R[\![z]\!]\,,$$

with $x = \{x_1, \ldots, x_a\}$, $y = \{y_1, \ldots, y_b\}$, $z = \{z_1, \ldots, z_c\}$ being system of indeterminates. A biextension of A and B by C is a pair of formal group laws

$$\begin{aligned} \mathcal{A}\colon R[\![x,y,z]\!] &\longrightarrow R[\![x,y,z]\!] \hat{\otimes}_{R[\![y]\!]} R[\![x,y,z]\!] = R[\![x',x'',y,z',z'']\!] \qquad \text{over } R[\![y]\!]\,,\\ \mathcal{B}\colon R[\![x,y,z]\!] &\longrightarrow R[\![x,y,z]\!] \hat{\otimes}_{R[\![x]\!]} R[\![x,y,z]\!] = R[\![x,y',y'',z',z'']\!] \qquad \text{over } R[\![x]\!]\,, \end{aligned}$$

such that $\mathcal{A}$ is an extension of $A\hat{\otimes}_R R[\![y]\!]$ by $C\hat{\otimes}_R R[\![y]\!]$, $\mathcal{B}$ is an extension of $B\hat{\otimes}_R R[\![x]\!]$ by $C\hat{\otimes}_R R[\![x]\!]$, and moreover $\mathcal{A}$ and $\mathcal{B}$ are compatible in the "dual sense" of (1.2.5). More explicitly we require that:

(i) the inclusion $R[\![x,y]\!] \to R[\![x,y,z]\!]$ is both a homomorphism between $A_{R[\![y]\!]}$ and $\mathcal{A}$ and also an homomorphism between $B_{R[\![x]\!]}$ and $\mathcal{B}$;

(ii) the continuous homomorphism of R-algebras $R[\![x,y,z]\!] \to R[\![y,z]\!]$ evaluating power series at $x_1{=}\ldots{=}x_a{=}0$ is a homomorphism between $\mathcal{A}$ and $C_{R[\![y]\!]}$ and the continuous homomorphism of R-algebras $R[\![x,y,z]\!] \to R[\![x,z]\!]$ evaluating power series at $y_1{=}\ldots{=}y_b{=}0$ is a homomorphism between $\mathcal{B}$ and $C_{R[\![x]\!]}$;

(iii) using the isomorphism (2.1.2), the following diagram commutes

$$\begin{array}{ccc} R[\![x,y,z]\!] & \xrightarrow{\quad\mathcal{A}\quad} & R[\![x',x',y,z',z'']\!] \\ \big\downarrow{\scriptstyle\mathcal{B}} & & \big\downarrow{\scriptstyle\mathcal{B}\hat{\otimes}\mathcal{B}} \\ R[\![x,y',y'',z',z'']\!] & \xrightarrow{\mathcal{A}\hat{\otimes}\mathcal{A}} & R[\![x',x',y',y'',z',z''z''',z^{(iv)}]\!]\,, \end{array} \tag{2.2.1}$$

where both the $(R[\![x,y,z]\!] \hat{\otimes}_{R[\![x]\!]} R[\![x,y,z]\!]) \hat{\otimes}_{R[\![y]\!]\,\hat{\otimes}_R\, R[\![y]\!]} (R[\![x,y,z]\!] \hat{\otimes}_{R[\![x]\!]} R[\![x,y,z]\!])$ and $(R[\![x,y,z]\!] \hat{\otimes}_{R[\![y]\!]} R[\![x,y,z]\!]) \hat{\otimes}_{R[\![x]\!]\,\hat{\otimes}_R\, R[\![x]\!]} (R[\![x,y,z]\!] \hat{\otimes}_{R[\![y]\!]} R[\![x,y,z]\!])$ are identified with $R[\![x',x',y',y'',z',z''z''',z^{(iv)}]\!]$, in the first case with $(z{\otimes}1){\otimes}(1{\otimes}1) \leftrightarrow z'$,

$(1\otimes z)\otimes(1\otimes 1) \leftrightarrow z''$, $(1\otimes 1)\otimes(z\otimes 1) \leftrightarrow z'''$, $(1\otimes 1)\otimes(1\otimes z) \leftrightarrow z^{(iv)}$ and in the second case with $(z\otimes 1)\otimes(1\otimes 1) \leftrightarrow z'$, $(1\otimes z)\otimes(1\otimes 1) \leftrightarrow z'''$, $(1\otimes 1)\otimes(z\otimes 1) \leftrightarrow z''$, $(1\otimes 1)\otimes(1\otimes z) \leftrightarrow z^{(iv)}$.

We call such an object $(\mathcal{A},\mathcal{B})$ a *formal biextension law*. Now suppose we are given three other formal group laws

$$H\colon R[\![u]\!] \to R[\![u]\!]\,\hat{\otimes}_R R[\![u]\!]\,, \quad J\colon R[\![v]\!] \to R[\![v]\!]\,\hat{\otimes}_R R[\![v]\!]\,, \quad K\colon R[\![w]\!] \to R[\![w]\!]\,\hat{\otimes}_R R[\![w]\!]\,,$$

and a biextension $(\mathcal{H},\mathcal{J})$ of H and J by K. Then a morphism between $(\mathcal{A},\mathcal{B})$ and $(\mathcal{H},\mathcal{J})$ is a morphism $\phi\colon R[\![x,y,z]\!] \to R[\![u,v,w]\!]$ such that

- ϕ restricts to maps $\phi^x\colon R[\![x]\!] \to R[\![u]\!]$ and $\phi^y\colon R[\![y]\!] \to R[\![v]\!]$ such that ϕ^x is a morphism between A and H and ϕ^y is a morphism between B and J;
- the following diagrams are commutative

$$\begin{array}{ccc} R[\![x,y,z]\!] & \xrightarrow{\mathcal{A}} & R[\![x,y,z]\!]\hat{\otimes}_{R[\![y]\!]}R[\![x,y,z]\!] \\ \downarrow{\scriptstyle\phi} & & \downarrow{\scriptstyle\phi\,\hat{\otimes}_{\phi^y}\,\phi} \\ R[\![u,v,w]\!] & \xrightarrow{\mathcal{H}} & R[\![u,v,w]\!]\hat{\otimes}_{R[\![v]\!]}R[\![u,v,w]\!] \end{array} \qquad \begin{array}{ccc} R[\![x,y,z]\!] & \xrightarrow{\mathcal{B}} & R[\![x,y,z]\!]\hat{\otimes}_{R[\![x]\!]}R[\![x,y,z]\!] \\ \downarrow{\scriptstyle\phi} & & \downarrow{\scriptstyle\phi\,\hat{\otimes}_{\phi^x}\,\phi} \\ R[\![u,v,w]\!] & \xrightarrow{\mathcal{J}} & R[\![u,v,w]\!]\hat{\otimes}_{R[\![u]\!]}R[\![u,v,w]\!] \end{array}$$

In this setting the functor $D{=}(\mathcal{A},\mathcal{B})$ going from topological R-algebras to sets defined as

$$(\mathcal{A},\mathcal{B})(S) = \mathrm{Hom}_{\mathrm{cont}}(R[\![x,y,z]\!],S) = \mathfrak{N}_S^{a+b+c}$$

has two partial group laws induced by $\mathcal{A}$ and $\mathcal{B}$ that make D a biextension of the functors of groups A and B by C. Vice versa if D is a biextension of the functors of groups A and B by C, then one can show that D is representable by $R[\![x,y,z]\!]$ in such a way that the natural transformation $D \to A\times B$ is induced by the inclusion $R[\![x,y]\!] \to R[\![x,y,z]\!]$ and the natural transformations $A\times C, B\times C \to D$ describing the kernels of $D \to A\times B$ are induced by the maps $R[\![x,y,z]\!] \to R[\![x,z]\!], R[\![y,z]\!]$ sending y or x to zero. This is enough to prove that every formal biextension is induced by a formal biextension law.

We say that a formal biextension law $(\mathcal{A},\mathcal{B})$ is commutative if both $\mathcal{A}$ and $\mathcal{B}$ are commutative group laws. Given additive formal group laws AD_1, AD_2, AD_3 of dimensions d_1,d_2,d_3, the additive formal biextension law of dimensions (d_1,d_2,d_3) is the commutative formal biextension law $(\mathcal{AD}_1,\mathcal{AD}_2)$ of AD_1 and AD_2 by AD_3 given by

$$\begin{aligned} &\mathcal{AD}_1(x_i) = x_i\otimes 1 + 1\otimes x_i = x_i' + x_i''\,, \quad \mathcal{AD}_2(y_i) = y_i\otimes 1 + 1\otimes y_i = y_i' + y_i''\,, \\ &\mathcal{AD}_1(z_i) = z_i\otimes 1 + 1\otimes z_i = z_i' + z_i''\,, \quad \mathcal{AD}_2(z_i) = z_i\otimes 1 + 1\otimes z_i = z_i' + z_i''\,. \end{aligned} \tag{2.2.2}$$

In the next theorem we prove that every commutative biextension over R is isomorphic to an additive biextension, if $\mathbb{Q}\subset R$.

Theorem 2.2.3. *Let R be a $\mathbb{Q}$-algebra, let $x = \{x_1, \dots, x_a\}$, $y = \{y_1, \dots, y_b\}$ and $z = \{z_1, \dots, z_c\}$ be systems of indeterminates, let*

$$A\colon R[\![x]\!] \to R[\![x]\!] \hat{\otimes}_R R[\![x]\!], \quad B\colon R[\![y]\!] \to R[\![y]\!] \hat{\otimes}_R R[\![y]\!], \quad C\colon R[\![z]\!] \to R[\![z]\!] \hat{\otimes}_R R[\![z]\!],$$

be three formal group laws over R and let $(\mathcal{A}, \mathcal{B})$ be a commutative formal biextension of A, B by C. Let $\mathcal{I} \subset R[\![x, y, z]\!]$ be the ideal $(x_1, \dots, x_a, z_1, \dots, z_c)^2 + (y_1, \dots, y_b, z_1, \dots, z_c)^2$.

Then there is a unique isomorphism $\psi\colon R[\![x, y, z]\!] \to R[\![x, y, z]\!]$ between the additive formal biextension law of dimensions (a, b, c) and $(\mathcal{A}, \mathcal{B})$ such that ψ reduces to the identity modulo $\mathcal{I}$. Moreover such a ψ restricts to $\psi|_{R[\![x]\!]} = \log_A\colon R[\![x]\!] \to R[\![x]\!]$ and $\psi|_{R[\![y]\!]} = \log_B\colon R[\![y]\!] \to R[\![y]\!]$.

Proof. We first prove the uniqueness. Since two isomorphisms between the additive formal biextension $(\mathcal{AD}_1, \mathcal{AD}_2)$ of dimensions (a, b, c) and $(\mathcal{A}, \mathcal{B})$ differ by automorphisms of $(\mathcal{AD}_1, \mathcal{AD}_2)$, it is enough to prove uniqueness in the case $(\mathcal{A}, \mathcal{B}) = (\mathcal{AD}_1, \mathcal{AD}_2)$. Let ψ be an automorphism of $(\mathcal{AD}_1, \mathcal{AD}_2)$ reducing to the identity modulo $\mathcal{I}$. By definition of homomorphism of formal biextension laws, ψ restricts to an automorphism $\psi^x\colon R[\![x]\!] \to R[\![x]\!]$ of the additive formal group law A and, by the hypothesis on ψ mod $\mathcal{I}$, ψ^x reduces to the identity modulo $(x_1, \dots, x_a)^2$. Then, by uniqueness of the formal logarithm,

$$\psi^x = \mathrm{id}_{R[\![x]\!]},$$

hence $\psi\colon R[\![x]\!][\![y, z]\!] \to R[\![x]\!][\![y, z]\!]$ is a morphism of $R[\![x]\!]$-algebras. This, together with the definition of homomorphism of formal biextension, implies that ψ is an automorphism of the additive biextension law $\mathcal{AD}_2$. Symmetrically $\psi^y := \psi|_{R[\![y]\!]} = \mathrm{id}_{R[\![y]\!]}$ and ψ is an automorphism of the additive biextension law $\mathcal{AD}_1$. Since all the homomorphisms of additive groups are linear, there exist power series $\lambda_{i,j}, \mu_{i,k} \in R[\![x]\!]$ and $\sigma_{i,j}, \tau_{i,l} \in R[\![y]\!]$ such that

$$\psi(z_i) = z_i + \sum_{j=1}^{c} \lambda_{i,j}(x) z_j + \sum_{k=1}^{b} \mu_{i,k}(x) y_k = z_i + \sum_{j=1}^{c} \sigma_{i,j}(y) z_j + \sum_{l=1}^{a} \tau_{i,l}(y) x_l.$$

We deduce that $\lambda_{i,j}(x) = \sigma_{i,j}(y)$ is constant, and since $\psi(z_i) \equiv z_i$ modulo I, we deduce that $\lambda_{i,j}(x) = \sigma_{i,j}(y) = 0$. The above equation also implies that power series $\mu_{i,j}(x)$ are linear polynomials in the x_l's. Hence $\psi(z_i) - z_i$ is a linear combination of the monomials $y_k x_l$ and, since it belongs to I, we deduce that $\psi(z_i) - z_i = 0$.

We have proved that ψ and the identity agree when evaluated on all the x_l's, y_k's and z_j's, hence, by continuity, ψ is the identity, which proves the uniqueness.

For the existence of ψ we proceed in four steps, that is we define automorphisms $\psi_1, \psi_2, \psi_3, \psi_4$ of $R[\![x, y, z]\!]$ whose composition $\psi_4 \circ \psi_3 \circ \psi_2 \circ \psi_1$ is the ψ we are looking for.

Let ψ_1 be the formal logarithm of $\mathcal{B}$. By definition we have $\psi_1^x := \psi_1|_{R[\![x]\!]} = \mathrm{id}_{R[\![x]\!]}$ and, by the explicit formulas for the formal logarithm in [54, Proposition 1.1 and Theorem 1] and the fact that $\mathcal{B}|_{R[\![y]\!]} = B$, the map $\psi_1^y := \psi_1|_{R[\![y]\!]}$ is equal to the formal logarithm of B. In particular ψ_1 restricts to an automorphism of both $R[\![x]\!]$ and $R[\![y]\!]$, hence it makes sense to define the "pullback" $(\mathcal{A}_1, \mathcal{B}_1)$ of $(\mathcal{A}, \mathcal{B})$ by ψ_1: we define $\mathcal{A}_1$ and $\mathcal{B}_1$ to be the unique maps making the following diagrams commute

(2.2.3.1)

$$\begin{array}{ccc} R[\![x,y,z]\!] & \xrightarrow{\mathcal{A}_1} & R[\![x',x'',y,z',z'']\!] \\ \downarrow{\scriptstyle \psi_1} & & \downarrow{\scriptstyle \psi_1 \hat{\otimes}_{\psi_1^y} \psi_1} \\ R[\![x,y,z]\!] & \xrightarrow{\mathcal{A}} & R[\![x',x'',y,z',z'']\!] \end{array} \qquad \begin{array}{ccc} R[\![x,y,z]\!] & \xrightarrow{\mathcal{B}_1} & R[\![x,y',y'',z',z'']\!] \\ \downarrow{\scriptstyle \psi_1} & & \downarrow{\scriptstyle \psi_1 \hat{\otimes}_{\psi_1^x} \psi_1} \\ R[\![x,y,z]\!] & \xrightarrow{\mathcal{B}} & R[\![x,y',y'',z',z'']\!] \end{array} .$$

Then $(\mathcal{A}_1, \mathcal{B}_1)$ is a biextension of certain formal group laws A_1, B_1 by C_1: indeed we define $A_1 := \mathcal{A}_1|_{R[\![x]\!]}$, $B_1 := \mathcal{A}_1|_{R[\![y]\!]}$ and we define C_1 functorially by imposing that, for every adic R-algebra S, $C_1(S)$ is the set of points in $\mathfrak{N}_S^{a+b+c}$ that project to $(0,0) \in (A_1 \times B_1)(S)$ with the group law given by $\mathcal{A}_1$; it is easy to check, sometimes using the functorial point of view and sometimes using the ring theoretic point of view, that $\mathcal{A}_1$ and $\mathcal{B}_1$ are formal groups, that they are compatible in the sense of (2.2.1), that $\mathcal{A}_1$ is an extension of $(A_1)_{R[\![y]\!]}$ by $(C_1)_{R[\![y]\!]}$ and that $\mathcal{B}_1$ is an extension of $(B_1)_{R[\![x]\!]}$ by $(C_1)_{R[\![x]\!]}$.

The definition of ψ_1 as formal logarithm implies that $\mathcal{B}_1 = \mathcal{A}\mathcal{D}_2$ as in (2.2.2) and consequently both B_1 and C_1 are additive. Since $\psi_1^x = \mathrm{id}_{R[\![x]\!]}$, then $A_1 = A$.

Now we define $\psi_2 \colon R[\![x,y,z]\!] \to R[\![x,y,z]\!]$ to be the unique continuous morphism being equal to the identity when restricted to $R[\![y,z]\!]$ and equal to the formal logarithm of $A_1 = A$ when restricted to $R[\![x]\!]$. Since ψ_2 restricts to automorphisms ψ_2^x, ψ_2^y of $R[\![x]\!], R[\![y]\!]$, we can define the pullback $(\mathcal{A}_2, \mathcal{B}_2)$ of $(\mathcal{A}_1, \mathcal{B}_1)$ by the map ψ_2, in the same way we defined the pullback $(\mathcal{A}_1, \mathcal{B}_1)$ of $(\mathcal{A}, \mathcal{B})$. Again $(\mathcal{A}_2, \mathcal{B}_2)$ is a biextension of certain formal group laws A_2, B_2 by C_2.

Since ψ_2 acts as the identity on $R[\![y,z]\!]$ we check that $\mathcal{B}_1 = \mathcal{A}\mathcal{D}_2 = \mathcal{B}_2$, hence both B_2 and C_2 are additive. The map $\psi_2^x = \log_A$ is an isomorphism between A_2 and A_1, hence A_2 is an additive formal group law. For each $i = 1, \ldots, c$ let us now look at the power series

$$\mathcal{A}_2(z_i) = \sum_{I',I'',J,K',K''} \lambda_{I',I'',J,K',K''} (x')^{I'} (x'')^{I''} y^J (z')^{K'} (z'')^{K''}.$$

The compatibility (2.2.1) between $\mathcal{B}_2 = \mathcal{A}\mathcal{D}_2$ and $\mathcal{A}_2$ implies that

$$\mathcal{A}_2(z_i)(x', x'', y'+y'', z'+z'', z'''+z^{(iv)}) = \mathcal{A}_2(z_i)(x', x'', y', z', z''') + \mathcal{A}_2(z_i)(x', x'', y'', z'', z^{(iv)}).$$

Since in the R.H.S of this equation there is no monomial multiple of $y_i' y_j''$, by expanding the series on the L.H.S we see that $\lambda_{I',I'',J,K',K''} = 0$ if $|J| \geq 2$. Analogously by looking

at monomials multiple of $z'_i z''$ or multiple of $z'_i z_j^{(iv)}$ or multiple of $z_i''' z_j^{(iv)}$, we infer that $\lambda_{I',I'',J,K',K''} = 0$ if $|K' + K''| \geq 2$. By looking at monomials multiple of $z'_i y''_j$ or multiple of $z''_i y'_j$ we infer that $\lambda_{I',I'',J,K',K''} = 0$ if $|J+K''+K'| \geq 2$. The term $(x')^{I'}(x'')^{I''}$ appears with coefficient $\lambda_{I',I'',0,0,0}$ on the left and with coefficient $2\lambda_{I',I'',0,0,0}$ the right, thus we must have $\lambda_{I',I'',0,0,0} = 0$. We have proved that the only coefficients $\lambda_{I',I'',J,K',K''} \neq 0$ are the ones with $|J + K' + K''| = 1$, hence

$$\mathcal{A}_2(z_i) = \sum_{j=1}^{b} d_{i,j}(x', x'')y_j + \sum_{j=1}^{c} f_{i,j}(x', x'')z'_j + \sum_{j=1}^{c} e_{i,j}(x', x'')z''_j. \tag{2.2.3.2}$$

with appropriate $d_{i,j} f_{i,j}, e_{i,j} \in R[\![x]\!]$. By the commutativity of $\mathcal{A}_2$, for each $j \in \{1, \ldots, c\}$ we have $f_{i,j}(x', x'') = e_{i,j}(x'', x')$. Let $f(x', x'')$ be the matrix with (i, j)-entry equal to $f_{i,j}$, let $d(x', x'')$ be the matrix with (i, j)-entry equal to $d_{i,j}$ and let $\mathcal{A}_2(z)$ be the column vector $(\mathcal{A}_2(z_1), \ldots, \mathcal{A}_2(z_d))^t$. Looking at x, y, z, z', z'' as column vectors, we can rewrite equation (2.2.3.2) as

$$\mathcal{A}_2(z) = d(x', x'') \cdot y + f(x', x'') \cdot z' + f(x'', x') \cdot z'' \,. \tag{2.2.3.3}$$

The property (2.1.1) of formal group laws implies that f is congruent to the identity matrix modulo the ideal $(x'_1, x''_1, \ldots, x'_a, x''_a)$.In particular the determinant of f is invertible in $R[\![x', x'']\!]$, hence f has an inverse with coefficients in $R[\![x', x'']\!]$. Writing down the associativity of $\mathcal{A}_2$ (the right diagram in Equation (2.1.3)), we find the identity

$$f(x', x'' + x''') = f(x' + x'', x''') \cdot f(x', x'').$$

If we plug in the values $x' \leftarrow 0$, $x'' \leftarrow x'$ and $x''' \leftarrow x''$ we immediately see that

$$f(x', x'') = g(x' + x'') \cdot g(x')^{-1} \tag{2.2.3.4}$$

where $g(x) := f(0, x) \in R[\![x]\!]^{c \times c}$, which is invertible because f is invertible. We now define the continuous automorphism

$$\psi_3 \colon R[\![x, y, z]\!] \longrightarrow R[\![x, y, z]\!] \,, \quad x \longmapsto x \,, y \longmapsto y \,, z \longmapsto g(x) \cdot z \,.$$

Again let $(\mathcal{A}_3, \mathcal{B}_3)$ be the formal biextension law obtained pulling back $(\mathcal{A}_2, \mathcal{B}_2)$ by ψ_3. We now prove that $\mathcal{B}_3 = \mathcal{AD}_2$ and that $\mathcal{A}_3$ is "almost equal" to $\mathcal{AD}_1$. Using that ψ_3 acts as the identity on $R[\![x, y]\!]$, we check that $\mathcal{B}_3(y_i) = \mathcal{AD}_2(y_i)$ and that $\mathcal{A}_3(x_i) = \mathcal{AD}_1(x_i)$.

Using the isomorphism (2.1.2) and Equation (2.2.3.4) we get

$$\begin{aligned}
\mathcal{B}_3(z) &= (\psi_3 \hat{\otimes}_{R[\![x]\!]} \psi_3) \circ \mathcal{B}_2 \circ \psi_3^{-1}(z) = (\psi_3 \hat{\otimes}_{R[\![x]\!]} \psi_3) \circ \mathcal{B}_2(g(x)^{-1} \cdot z) \\
&= (\psi_3 \hat{\otimes}_{R[\![x]\!]} \psi_3)\big(g(x)^{-1} \cdot (z' + z'')\big) = g(x)^{-1} \cdot \big(g(x) \cdot z' + g(x) \cdot z''\big) \\
&= z' + z'' = \mathcal{AD}_2(z). \\
\mathcal{A}_3(z) &= (\psi_3 \hat{\otimes}_{R[\![x]\!]} \psi_3) \circ \mathcal{A}_2 \circ \psi_3^{-1}(z) = (\psi_3 \hat{\otimes}_{R[\![x]\!]} \psi_3) \circ \mathcal{A}_2(g(x)^{-1} \cdot z) \\
&= (\psi_3 \hat{\otimes}_{R[\![x]\!]} \psi_3)\big(g(x' + x'')^{-1} \cdot \big(d(x', x'') \cdot y + f(x', x'') \cdot z' + f(x'', x') \cdot z''\big)\big) \\
&= g(x' + x'')^{-1} \cdot \big(d(x', x'') \cdot y + f(x', x'') \cdot g(x') \cdot z' + f(x'', x') \cdot g(x'') \cdot z''\big) \\
&= z' + z'' + g(x' + x'')^{-1} \cdot d(x', x'') \cdot y = \mathcal{AD}_1(z) + g(x' + x'')^{-1} \cdot d(x', x'') y.
\end{aligned}$$

By the associativity and commutativity of $\mathcal{A}_3$ we can prove the following claim.

Claim 2.2.4. *There exists a unique matrix of power series $h(x) \in R[\![x]\!]^{c \times b}$ such that*

$$g(x' + x'')^{-1} \cdot d(x', x'') = h(x' + x'') - h(x') - h(x'') \quad \textit{and} \tag{2.2.4.1}$$

$$h(0) \equiv 0 \pmod{(x_1, \ldots, x_a)^2}. \tag{2.2.4.2}$$

Proof. We define $m(x', x'') := g(x' + x'')^{-1} d(x', x'')$. When proving the claim, we can work separately on each entry $m_{i,j}$ and $h_{i,j}$, hence we can consider m as an element in $R[\![x', x'']\!]$ and h as an element in $R[\![x]\!]$, instead of considering them as matrices on the same rings.

Notice that two solutions of (2.2.4.1) differ by a (matrix of) linear polynomial(s) in the x_i's, hence the congruence (2.2.4.2) ensures uniqueness. We now prove existence.

We know that a power series $S \in R[\![x', x'']\!] = R[\![x'']\!][\![x']\!]$ is zero if and only if $S(0, x'') = 0$ and $\partial S / \partial x_i' = 0$ for each $i \in \{0, \ldots, a\}$: applying this principle to our claim we get that, for any h, Equation (2.2.4.1) holds if and only if

$$m(0, x'') = -h(0) \qquad \text{and} \tag{2.2.4.3}$$

$$\frac{\partial m}{\partial x_i'}(x', x'') = \frac{\partial h}{\partial x_i}(x' + x'') - \frac{\partial h}{\partial x_i}(x') \qquad \forall i = 1, \ldots, a. \tag{2.2.4.4}$$

Equation (2.2.4.3) is equivalent to $h(0) = 0$: indeed $m(0, x'') = 0$ because the evaluation of $\mathcal{A}_3(z)$ at $x' = z' = 0$ is equal to z'', as implied by the first property in the definition of formal group laws (the one saying that "the point 0" is the neutral element). Moreover if $h(0) = 0$, then, up to adding a (matrix of) linear polynomial(s) in the x_i's, we can suppose that h is congruent to 0 modulo $(x_1, \ldots, x_a)^2$. Hence proving our claim is equivalent solving Equation (2.2.4.4) and $h(0) = 0$, which is in turn equivalent to finding

$n_1, \dots, n_a$ being (matrices with coefficients) in $R[\![x]\!]$ such that

$$n := \sum_{i=1}^{a} n_i(x)dx_i \quad \text{is a closed form} \qquad \text{and} \tag{2.2.4.5}$$

$$\frac{\partial m}{\partial x_i'}(x', x'') = n_i(x' + x'') - n_i(x') \qquad \forall i = 1, \dots, a. \tag{2.2.4.6}$$

Indeed, given h as in Equations (2.2.4.3), (2.2.4.4) we can take $n_i = \partial h/\partial x_i$ and given $n_1, \dots, n_a$ as above, since all closed forms in $R[\![x]\!]$ are exact, there exists a unique $h \in R[\![x]\!]$ such that $h(0) = 0$ and $\partial h/\partial x_i = n_i$. We now look for such n_i's.

Associativity of the formal group law $\mathcal{A}_3$ tells us that

$$m(x' + x'', x''') + m(x', x'') = m(x', x'' + x''') + m(x'', x''').$$

Taking the partial derivative with respect to x_i', we get

$$\frac{\partial m}{\partial x_i'}(x' + x'', x''') + \frac{\partial m}{\partial x_i'}(x', x'') = \frac{\partial m}{\partial x_i'}(x', x'' + x'''). \tag{2.2.4.7}$$

Plugging the values $x' \leftarrow 0$, $x'' \leftarrow x'$ and $x''' \leftarrow x''$ in the above equation we see that

$$n_i(x) := \frac{\partial m}{\partial x_i'}(0, x)\,,$$

automatically satisfy Equation (2.2.4.6). It remains to show that, with the above definition of the n_i's, Equation (2.2.4.5) is also satisfied. Taking the derivative of Equation (2.2.4.7) with respect to x_j''' we find

$$\frac{\partial^2 m}{\partial x_j'' \partial x_i'}(x' + x'', x''') = \frac{\partial^2 m}{\partial x_j'' \partial x_i'}(x', x'' + x'''). \tag{2.2.4.8}$$

The commutativity of $\mathcal{A}_3$ implies $m(x', x'') = m(x'', x')$, and taking two derivatives we get

$$\frac{\partial^2 m}{\partial x_i'' \partial x_j'}(x', x'') = \frac{\partial^2 m}{\partial x_j'' \partial x_i'}(x'', x'). \tag{2.2.4.9}$$

Deriving the definition of n_i and specializing Equations (2.2.4.8) and (2.2.4.9) in $x' \leftarrow 0$, $x'' \leftarrow x$, $x''' \leftarrow 0$, we find that for every $i, j = 1, \dots, a$

$$\frac{\partial n_i}{\partial x_j} = \frac{\partial^2 m}{\partial x_j'' \partial x_i'}(0, x) = \frac{\partial^2 m}{\partial x_j'' \partial x_i'}(x, 0) = \frac{\partial^2 m}{\partial x_i'' \partial x_j'}(0, x) = \frac{\partial n_j}{\partial x_i},$$

proving that the form n in Equation (2.2.4.5) is closed. □

Taking h as in the claim we define the continuous automorphism

$$\psi_4 \colon R[\![x,y,z]\!] \longrightarrow R[\![x,y,z]\!]\,, \quad x \longmapsto x\,, y \longmapsto y\,, z \longmapsto z + h(x)\cdot y\,,$$

and we define $(\mathcal{A}_4, \mathcal{B}_4)$ to be the pullback of the formal biextension law $(\mathcal{A}_4, \mathcal{B}_4)$ by ψ_4. We easily check that $\mathcal{B}_4 = \mathcal{AD}_2$ and $\mathcal{A}_4(y_i) = \mathcal{AD}_1(y_i)$. Moreover, using the definition of $\mathcal{A}_4$, the formula for $\mathcal{A}_3(z)$ we previously found and the definition of h, we get

$$\begin{aligned}
\mathcal{A}_4(z) &= (\psi_4 \hat{\otimes}_{R[\![x]\!]} \psi_4) \circ \mathcal{A}_3 \circ \psi_4^{-1}(z) = (\psi_4 \hat{\otimes}_{R[\![x]\!]} \psi_4) \circ \mathcal{A}_3\big(z - h(x)\cdot y\big) \\
&= (\psi_4 \hat{\otimes}_{R[\![x]\!]} \psi_4)\big(z' + z'' + g(x'+x'')^{-1}\cdot d(x', x'')\cdot y - h(x'+x'')\cdot y\big) \\
&= (\psi_4 \hat{\otimes}_{R[\![x]\!]} \psi_4)\big(z' + z'' - h(x')\cdot y - h(x'')\cdot y\big) \\
&= z' + h(x')\cdot y + z'' + h(x'')\cdot y - h(x')\cdot y - h(x'') \\
&= z' + z'' = \mathcal{AD}_1(z)\,.
\end{aligned}$$

Hence $\mathcal{A}_4 = \mathcal{AD}_1$ and $(\mathcal{A}_4, \mathcal{B}_4)$ is the additive formal biextension law of dimensions (a, b, c).

For each $i = 1, 2, 3, 4$ we have defined $(\mathcal{A}_i, \mathcal{B}_i)$ as the pullback of $(\mathcal{A}_{i-1}, \mathcal{B}_{i-1})$ by ψ_i (here $(\mathcal{A}_0, \mathcal{B}_0) = (\mathcal{A}, \mathcal{B})$) hence, by the definition of pullback in (2.2.3.1), the map ψ_i is an isomorphism between $(\mathcal{A}_i, \mathcal{B}_i)$ and $(\mathcal{A}_{i-1}, \mathcal{B}_{i-1})$. Consequently $\psi := \psi_4 \circ \psi_3 \circ \psi_2 \circ \psi_1$ is an isomorphism between $(\mathcal{A}_4, \mathcal{B}_4) = (\mathcal{AD}_1, \mathcal{AD}_2)$ and $(\mathcal{A}_0, \mathcal{B}_0) = (\mathcal{A}, \mathcal{B})$. Moreover ψ is the identity when reduced modulo $\mathcal{I}$ since the same is true for $\psi_1, \psi_2, \psi_3, \psi_4$: for ψ_1 and ψ_2 it is true by the definition of formal logarithms, for ψ_3 it is true because $g(x) = f(0, x)$ is congruent to the identity matrix modulo the ideal $(x_1, \ldots, x_a)$ and for ψ_4 it is true because h is congruent to the zero matrix modulo the ideal $(x_1, \ldots, x_a)^2$. Finally we notice that the subrings $R[\![x]\!], R[\![y]\!] \subset R[\![x,y,z]\!]$ are stable under $\psi_1, \psi_2, \psi_3, \psi_4$ so they are also stable under ϕ, that restricts to isomorphisms

$$\begin{aligned}
\psi^x &:= \psi|_{R[\![x]\!]} = \psi_4^x \circ \psi_3^x \circ \psi_2^x \circ \psi_1^x = \mathrm{id}_{R[\![x]\!]} \circ \mathrm{id}_{R[\![x]\!]} \circ \log_A \circ \mathrm{id}_{R[\![x]\!]} = \log_A\,, \\
\psi^y &:= \psi|_{R[\![y]\!]} = \psi_4^y \circ \psi_3^y \circ \psi_2^y \circ \psi_1^y = \mathrm{id}_{R[\![y]\!]} \circ \mathrm{id}_{R[\![y]\!]} \circ \mathrm{id}_{R[\![y]\!]} \circ \log_B = \log_B\,.
\end{aligned}$$

□

2.3 Biextensions over the p-adics and convergence

Given a commutative algebraic group $G/\mathbb{Z}_p$, the formal logarithm is useful to describe the group $G(\mathbb{Z}_p)$ in a neighbourhood of its neutral element. Analogously we want to use the map ψ of Theorem 2.2.3 to describe biextensions over $\mathbb{Z}_p$, hence we are interested in the convergence and integrality of the power series determining ψ.

Let R be a $\mathbb{Z}_{(p)}$-algebra of characteristic zero equipped with a positive discrete valuation v extending the p-adic valuation on $\mathbb{Z}_{(p)}$ and such that the ideal $\{r \in R : v(r) > 0\}$ is generated by an element π. Examples of such rings are $R = \mathbb{Z}_{(p)}[\![x_1, \dots, x_d]\!]$ equipped with the p-adic valuations or the discrete valuation rings contained in finite extensions of $\mathbb{Q}_p$.

For any formal group $A\colon R[\![x]\!] \to R[\![x]\!]\hat{\otimes}R[\![x]\!]$ of dimension a we have

$$A(R) = \mathrm{Hom}_{\mathrm{cont}}(R[\![x]\!], R) = (\pi R)^a\,,$$

where $R[\![x]\!]$ is endowed with the $(x_1, \dots, x_a)$-adic topology and R with the v-adic topology. Then the elements $\tilde{x}_i := \frac{x_i}{\pi} \in (R \otimes \mathbb{Q})[\![x]\!]$ define a bijection

$$\tilde{x} = (\tilde{x}_1, \dots, \tilde{x}_a)\colon A(R) \longrightarrow R^a\,, \tag{2.3.1}$$

that suggests the definition of the following ring of "integral converging power series"

$$R\langle\tilde{x}\rangle = R\langle\tilde{x}_1, \dots, \tilde{x}_a\rangle := \left\{ \sum_{I\in\mathbb{N}^a} \lambda_I \tilde{x}^I \in R[\![\tilde{x}]\!] : \forall n \geq 0,\ \ {}^{\mathrm{almost}}\forall I,\ v(\lambda_I) \geq n \right\} \subset (R\otimes\mathbb{Q})[\![x]\!]$$

This ring resembles the one in Equation (1.3.2) and, when R is complete with respect to v, each element of $R\langle\tilde{x}\rangle$ defines a continuous function $A(R) \to R$.

If A is commutative, the formal logarithm $\log_A := \log_{A_{R\otimes\mathbb{Q}}}\colon (R\otimes\mathbb{Q})[\![x]\!] \to (R\otimes\mathbb{Q})[\![x]\!]$ helps us understanding the group $A(R)$: if π^{p-2} is a multiple of p (when R is the discrete valuation ring contained in finite extensions of $\mathbb{Q}_p$ this is equivalent to the ramification being strictly smaller than $p-1$), then for each $i \in \{1, \dots, a\}$ we have

$$\log_A(\tilde{x}_i) \in R\langle\tilde{x}\rangle\,, \quad \log_A(\tilde{x}_i) \equiv x_i \bmod \pi\,. \tag{2.3.2}$$

Hence, if R is v-adically complete, we get an isomorphism of groups

$$(\log_A(\tilde{x}_1), \dots, \log_A(\tilde{x}_a))\colon A(R) \longrightarrow (R^a, +)\,, \tag{2.3.3}$$

that is given by integral converging power series and that, using the isomorphism (2.3.1), reduces to the identity modulo v. This fact can be proven with the same arguments in the proof of Lemma 1.5.1.1, replacing $\mathcal{O}_{S,s}$ with R.

We give an analogous statement for biextensions. In such context the biextension analogous to the additive group is the biextension $(R^a \times R^b \times R^c, +_1, +_2)$ of the additive groups $(R^a, +)$, $(R^b, +)$ by $(R^c, +)$, with partial group operations

$$\begin{aligned} (r'_A, r_B, r'_C) +_1 (r''_A, r_B, r''_C) &= (r'_A + r''_A, r_B, r'_C + r''_C), \\ (r_A, r'_B, r'_C) +_2 (r_A, r''_B, r''_C) &= (r_A, r'_B + r''_B, r'_C + r''_C). \end{aligned} \tag{2.3.4}$$

Proposition 2.3.5. *Let R be a $\mathbb{Z}_{(p)}$-algebra of characteristic zero equipped with a positive discrete valuation v extending the p-adic valuation on $\mathbb{Z}_{(p)}$. Suppose that the ideal $\{r \in R : v(r) > 0\}$ is generated by an element π such that π^{p-2} is a multiple of p. Let*

$$A\colon R[\![x]\!] \to R[\![x]\!] \hat{\otimes}_R R[\![x]\!]\,, \quad B\colon R[\![y]\!] \to R[\![y]\!] \hat{\otimes}_R R[\![y]\!]\,, \quad C\colon R[\![z]\!] \to R[\![z]\!] \hat{\otimes}_R R[\![z]\!]\,,$$

be formal group laws of dimensions a, b, c, let $(\mathcal{A}, \mathcal{B})$ be a commutative formal biextension of A, B by C and let $\psi\colon (R\otimes\mathbb{Q})[\![x,y,z]\!] \to (R\otimes\mathbb{Q})[\![x,y,z]\!]$ be the map in Theorem 2.2.3.

Using the definitions $\tilde{x}_i := x_i/\pi$, $\tilde{y}_j := y_j/\pi$, $\tilde{z}_k := z_k/\pi$, we have

$$\psi(\tilde{x}_i)\,, \psi(\tilde{y}_j)\,, \psi(\tilde{z}_k)\,, \psi^{-1}(\tilde{x}_i)\,, \psi^{-1}(\tilde{y}_j)\,, \psi^{-1}(\tilde{z}_k) \in R\langle \tilde{x}, \tilde{y}, \tilde{z}\rangle \quad \textit{and}$$
$$\psi(\tilde{x}_i) \equiv \psi^{-1}(\tilde{x}_i) \equiv \tilde{x}_i\,, \quad \psi(\tilde{y}_i) \equiv \psi^{-1}(\tilde{y}_j) \equiv \tilde{y}_j\,, \quad \psi(\tilde{z}_k) \equiv \psi^{-1}(\tilde{z}_k) \equiv \tilde{z}_k \quad \textit{modulo } \pi\,.$$

Moreover, if R is v-adically complete, the power series $\psi(\tilde{x}_i), \psi(\tilde{y}_j), \psi(\tilde{z}_k)$ give an isomorphism of biextensions

$$(\mathcal{A}, \mathcal{B})(R) \longrightarrow (R^a \times R^b \times R^c, +_1, +_2)\,,$$

where $(R^a \times R^b \times R^c, +_1, +_2)$ is the additive biextension given by (2.3.4).

Proof. For an additive formal biextension law $(\mathcal{AD}_1, \mathcal{AD}_2)$ of dimensions (a, b, c), the set of R-points $(\mathcal{AD}_1, \mathcal{AD}_2)(R)$ is exactly $(R^a \times R^b \times R^c, +_1, +_2)$, hence it is enough to prove that the power series $\psi(\tilde{x}_i)$, $\psi(\tilde{y}_j)$, $\psi(\tilde{z}_k)$, $\psi^{-1}(\tilde{x}_i)$, $\psi^{-1}(\tilde{y}_j)$, $\psi^{-1}(\tilde{z}_k)$ are contained in $R\langle \tilde{x}, \tilde{y}, \tilde{z}\rangle$ and proving the congruences. This is equivalent to proving that ψ and ψ^{-1} restrict to maps $R\langle \tilde{x}, \tilde{y}, \tilde{z}\rangle \to R\langle \tilde{x}, \tilde{y}, \tilde{z}\rangle$ that modulo π reduce to the identity of $(R/\pi)[\tilde{x}, \tilde{y}, \tilde{z}]$. Moreover once it is proven for ψ it is automatically true for ψ^{-1}.

We can write $\psi = \psi_4 \circ \psi_3 \circ \psi_2 \circ \psi_1$, where the ψ_i's are the ones defined in the proof of Theorem 2.2.3, hence it is enough to prove that both ψ_1 and $\psi_4 \circ \psi_3 \circ \psi_2$ restrict to maps $R\langle \tilde{x}, \tilde{y}, \tilde{z}\rangle \to R\langle \tilde{x}, \tilde{y}, \tilde{z}\rangle$ that modulo π reduce to the identity of $(R/\pi)[\tilde{x}, \tilde{y}, \tilde{z}]$. In other words it is enough to prove that the power series $\psi_1(\tilde{x}_i)$, $\psi_4 \circ \psi_3 \circ \psi_2(\tilde{x}_i)$, $\psi_1(\tilde{y}_j)$, $\psi_4 \circ \psi_3 \circ \psi_2(\tilde{y}_j)$, $\psi_1(\tilde{z}_k)$ and $\psi_4 \circ \psi_3 \circ \psi_2(\tilde{z}_k)$ lie in $R\langle \tilde{x}, \tilde{y}, \tilde{z}\rangle$ and that they are congruent respectively to $\tilde{x}_i$, $\tilde{x}_i$, $\tilde{y}_j$, $\tilde{y}_j$, $\tilde{z}_k$ and $\tilde{z}_k$ modulo π. We know that $\psi_1 = \log_{\mathcal{B}}$, hence, using Equation (2.3.2),

$$\psi_1(\tilde{x}_i) = \tilde{x}_i\,, \psi_1(\tilde{y}_j)\,, \psi_1(\tilde{z}_k) \in R[\![x]\!]\langle \tilde{y}, \tilde{z}\rangle \subset R\langle \tilde{x}, \tilde{y}, \tilde{z}\rangle \quad \text{and}$$
$$\psi_1(\tilde{x}_i) \equiv \tilde{x}_i (\mathrm{mod}\pi)\,, \quad \psi_1(\tilde{y}_i) \equiv \tilde{y}_i (\mathrm{mod}\pi)\,, \quad \psi_1(\tilde{y}_i) \equiv \tilde{y}_i (\mathrm{mod}\pi)\,,$$

where $R[\![x]\!]\langle \tilde{y}, \tilde{z}\rangle$ is defined with respect to the π-adic valuation on $R[\![x]\!]$. We notice that $\psi_2 \circ \psi_3 \circ \psi_4$ is the identity when restricted to $R[\![y]\!]$, hence $\psi_2 \circ \psi_3 \circ \psi_4\colon R[\![y]\!][\![x,z]\!] \to R[\![y]\!][\![x,z]\!]$ is an isomorphism between the additive formal group law of dimension $a+c$ over $R[\![y]\!]$ and the formal group law $\mathcal{A}_1$ which is defined in the proof of Theorem 2.2.3; moreover

$\psi_2\circ\psi_3\circ\psi_4$ reduces to the identity modulo $(x_1,\dots,x_a,z_1,\dots,x_c)^2$. By the uniqueness of the formal logarithm, $\psi_2\circ\psi_3\circ\psi_4=\log_{\mathcal{A}_1}$, hence, using Equation (2.3.2),

$$\psi_2\circ\psi_3\circ\psi_4(\tilde{x}_i)=\tilde{x}_i\,,\psi_2\circ\psi_3\circ\psi_4(\tilde{y}_j)\,,\psi_2\circ\psi_3\circ\psi_4(\tilde{z}_k)\in R[\![y]\!]\langle\tilde{x},\tilde{z}\rangle\subset R\langle\tilde{x},\tilde{y},\tilde{z}\rangle\quad\text{and}$$
$$\psi_2\circ\psi_3\circ\psi_4(\tilde{x}_i)\equiv\tilde{x}_i(\mathrm{mod}\pi)\,,\quad\psi_2\circ\psi_3\circ\psi_4(\tilde{y}_i)\equiv\tilde{y}_i(\mathrm{mod}\pi)\,,\quad\psi_2\circ\psi_3\circ\psi_4(\tilde{y}_i)\equiv\tilde{y}_i(\mathrm{mod}\pi)\,,$$

where $R[\![y]\!]\langle\tilde{x},\tilde{z}\rangle$ is defined with respect to the π-adic valuation on $R[\![y]\!]$. □

2.4 Another proof of Theorem 1.4.10

We now use Theorem 2.2.3 and Proposition 2.3.5 to give another proof of Theorem 1.4.10. Our strategy is constructing a chart $\Phi\colon\mathbb{Z}_p^{\rho g+\rho-1}\to P^{\times,\rho-1}(\mathbb{Z}_p)_t$, such that the map $\Phi^{-1}\circ\kappa$ is given by linear and quadratic polynomials. In order to construct Φ we first establish coordinates to define a formal biextension law associated to $P^{\times,\rho-1}$, then we use the map of Theorem 2.2.3 to describe more easily the partial group operations of $P^{\times,\rho-1}(\mathbb{Z}_p)$ in a neighbourhood of the neutral element, then we make translations to work in the residue disk of t.

Let $J,(J^{\vee 0})^{\rho-1},P^{\times,\rho-1}$ and T be as in Section 1.2 and let π_J and $\pi_{(J^{\vee 0})^{\rho-1}}$ be the two projections $P^{\times,\rho-1}\to J$ and $P^{\times,\rho-1}\to(J^{\vee 0})^{\rho-1}$. Letting $0,\overline{0}$ be the neutral elements of $J(\mathbb{Z}_p),J(\mathbb{F}_p)$, we choose $y_1,\dots,y_g\in\mathcal{O}_{J,\overline{0}}$ that vanish on 0 and that, together with p, generate the maximal ideal $\mathfrak{m}\subset\mathcal{O}_{J,\overline{0}}$. The embedding $\mathbb{Z}[y_1,\dots,y_g]\to\mathcal{O}_{J,\overline{0}}$ induces an isomorphism

$$\mathbb{Z}_p[\![y]\!]=\mathbb{Z}_p[\![y_1,\dots,y_g]\!]\xrightarrow{\sim}\mathcal{O}_{J,\overline{0}}^{\wedge_{\mathfrak{m}}}\,.$$

The group operation $M_J\colon J\times J\to J$ induces a morphism of rings $\mathcal{O}_{J,\overline{0}}\to\mathcal{O}_{J,\overline{0}}\otimes\mathcal{O}_{J,\overline{0}}$ and taking completions we get a formal group law over $\mathbb{Z}_p$

$$M_J^*\colon\mathbb{Z}_p[\![y]\!]=\mathcal{O}_{J,\overline{0}}^{\wedge_{\mathfrak{m}}}\longrightarrow(\mathcal{O}_{J,\overline{0}}\otimes\mathcal{O}_{J,\overline{0}})^{\wedge_{\mathfrak{m}\otimes\mathcal{O}_{J,\overline{0}}+\mathcal{O}_{J,\overline{0}}\otimes\mathfrak{m}}}=\mathbb{Z}_p[\![y]\!]\hat{\otimes}_{\mathbb{Z}_p}\mathbb{Z}_p[\![y]\!]\,.$$

Then we have an isomorphism of groups given by the composition

$$J(\mathbb{Z}_p)_{\overline{0}}=\mathrm{Hom}_{\mathrm{loc}}(\mathcal{O}_{J,\overline{0}},\mathbb{Z}_p)=\mathrm{Hom}_{\mathrm{cont}}(\mathcal{O}_{J,\overline{0}}^{\wedge_{\mathfrak{m}}},\mathbb{Z}_p)=\mathrm{Hom}_{\mathrm{cont}}(\mathbb{Z}_p[\![y]\!],\mathbb{Z}_p)=M_J^*(\mathbb{Z}_p)\,.$$

Analogously we choose $z_1,\dots,z_{\rho g-g}\in\mathcal{O}_{(J^{\vee 0})^{\rho-1},\overline{0}}$ that vanish on 0 and that, together with p, generate the maximal ideal of $\mathcal{O}_{(J^{\vee 0})^{\rho-1},\overline{0}}$. The group operation on $(J^{\vee 0})^{\rho-1}$ induces a formal group law

$$M_{(J^{\vee 0})^{\rho-1}}^*\colon\mathbb{Z}_p[\![z_1,\dots,z_{\rho g-g}]\!]=\mathbb{Z}_p[\![z]\!]\longrightarrow\mathbb{Z}_p[\![z]\!]\hat{\otimes}_{\mathbb{Z}_p}\mathbb{Z}_p[\![z]\!]\,,$$

that describes the group $(J^{\vee 0})^{\rho-1}(\mathbb{Z}_p)_{\overline{0}}$.

The rigidification of $P^{\times,\rho-1}$ along $J \times \{0\}$ gives an element $1 \in P^{\times,\rho-1}(0,0)(\mathbb{Z}_p)$ that is the neutral element of both the groups $\pi_J^{-1}(0)(\mathbb{Z}_p)$ and $\pi_{J^{\vee 0},\rho-1}^{-1}(0)(\mathbb{Z}_p)$. We call such an element the neutral element of $P^{\times,\rho-1}(\mathbb{Z}_p)$ and we denote by $\overline{1}$ its image in $P^{\times,\rho-1}(\mathbb{F}_p)$. We choose $w_1, \dots, w_{\rho-1} \in \mathcal{O}_{P^{\times,\rho-1},\overline{1}}$ that vanish on 1 and that, together with $x_1, \dots, x_g, z_1, \dots, z_{\rho g-g}$ and p generate the maximal ideal $\mathfrak{m} \subset \mathcal{O}_{P^{\times,\rho-1},\overline{1}}$. As before we have an isomorphism

$$\mathbb{Z}_p[\![y,z,w]\!] = \mathbb{Z}_p[\![y_1,\dots,y_g,z_1,\dots,z_{\rho g-g},w_1,\dots,w_{\rho-1}]\!] \xrightarrow{\sim} \mathcal{O}^{\wedge_{\mathfrak{m}}}_{P^{\times,\rho-1},\overline{1}}$$

and the two partial group laws

$$+_1 \colon P^{\times,\rho-1} \times_{(J^{\vee 0})^{\rho-1}} P^{\times,\rho-1} \longrightarrow P^{\times,\rho-1}, \quad +_2 \colon P^{\times,\rho-1} \times_J P^{\times,\rho-1} \longrightarrow P^{\times,\rho-1},$$

and induce a biextension

$$\begin{aligned} \mathcal{M}_J^* &\colon \mathbb{Z}_p[\![y,z,w]\!] \longrightarrow \mathbb{Z}_p[\![y,z,w]\!] \hat{\otimes}_{\mathbb{Z}_p[\![z]\!]} \mathbb{Z}_p[\![y,z,w]\!], \\ \mathcal{M}_{J^{\vee 0},\rho-1}^* &\colon \mathbb{Z}_p[\![y,z,w]\!] \longrightarrow \mathbb{Z}_p[\![y,z,w]\!] \hat{\otimes}_{\mathbb{Z}_p[\![y]\!]} \mathbb{Z}_p[\![y,z,w]\!], \end{aligned}$$

of the formal group laws M_J^* and $M_{J^{\vee 0},\rho-1}^*$ by the formal group law induced by the algebraic group $\mathbb{G}_{\mathrm{m}}^{\rho-1}$. In particular $P^{\times,\rho-1}(\mathbb{Z}_p)_{\overline{1}}$ is a biextension of $J(\mathbb{Z}_p)_{\overline{0}}$ and $(J^{\vee 0})^{\rho-1}(\mathbb{Z}_p)_{\overline{0}}$ by $\mathbb{G}_{\mathrm{m}}^{\rho-1}(\mathbb{Z}_p)_{\overline{1}}$, and it is isomorphic to $(\mathcal{M}_J, \mathcal{M}_{J^{0\vee},\rho-1})(\mathbb{Z}_p)$. Applying Theorem 2.2.3 and Proposition 2.3.5 we get an isomorphism of biextensions

$$\Psi \colon (P^{\times,\rho-1}(\mathbb{Z}_p)_{\overline{1}}, +_1, +_2) \longrightarrow (\mathbb{Z}_p^g \times \mathbb{Z}_p^{\rho g-g} \times \mathbb{Z}_p^{\rho-1}, +_1, +_2),$$

given by power series in $\mathcal{O}(\widetilde{(P^{\times,\rho-1})^p_x})^{\wedge_p}$, that modulo p give a linear map between the tangent space of $P^{\times,\rho-1}$ at $\overline{1}$ and $\mathbb{F}_p^{\rho g+\rho-1}$.

We now take care of translating Ψ. Let f and m be as in Section 1.2 and let $x_{\widetilde{t}} \in J(\mathbb{Z})$, $\widetilde{t} \in T(\mathbb{Z}) \subset P^{\times,\rho-1}(\mathbb{Z})$ be as in Section 1.4. By Equations (2.3.2) and (2.3.3), the formal logarithms of (the formal group laws associated to) the algebraic groups $\pi_{(J^{\vee 0})^{\rho-1}}^{-1}(m\cdot \circ \mathrm{tr}_c \circ f(x_{\widetilde{t}}))$ and $\pi_J^{-1}(x_{\widetilde{t}})$ give isomorphisms of groups

$$\begin{aligned} \Psi_1 &\colon \left(\pi_{J^{\vee 0},\rho-1}^{-1}(m\cdot \circ \mathrm{tr}_c \circ f(x_{\widetilde{t}}))(\mathbb{Z}_p)_{\overline{1}}, +_1\right) \longrightarrow (\mathbb{Z}_p^g \times \mathbb{Z}_p^{\rho-1}, +), \\ \Psi_2 &\colon \left(\pi_J^{-1}(x_{\widetilde{t}})(\mathbb{Z}_p)_{\overline{1}}, +_2\right) \longrightarrow (\mathbb{Z}_p^{\rho g-g} \times \mathbb{Z}_p^{\rho-1}, +), \end{aligned}$$

where we denote by $\overline{1}$ the reduction modulo p of the neutral elements of the respective groups. Since $\pi_J^{-1}(x_{\widetilde{t}})$ is an extension of $(J^{\vee 0})^{\rho-1}$, the first $\rho g-g$ coordinates of Ψ_2 are given by the composition of the projection $\pi_J^{-1}(x_{\widetilde{t}})(\mathbb{Z}_p)_{\overline{1}} \to (J^{\vee 0})^{\rho-1}(\mathbb{Z}_p)_{\overline{0}}$ with the formal logarithm of $(J^{\vee 0})^{\rho-1}$. Analogously the first g coordinates of Ψ_1 are given by the composition of $\pi_{(J^{\vee 0})^{\rho-1}}^{-1}(m\cdot \circ \mathrm{tr}_c \circ f(x_{\widetilde{t}}))(\mathbb{Z}_p)_{\overline{1}} \to J(\mathbb{Z}_p)_{\overline{0}}$ with the formal

logarithm of J. By Theorem 2.2.3, analogous statements are true for the first g coordinates of Ψ and the subsequent $\rho g-g$ coordinates of Ψ. This implies that for every $(\alpha,\beta,\gamma)\in\mathbb{Z}_p^g\times\mathbb{Z}_p^{\rho g-g}\times\mathbb{Z}_p^{\rho-1}$ we have

$$\begin{aligned}\pi_J\left(\Psi^{-1}(\alpha,\beta,\gamma)\right)&=\pi_J\left(\Psi_1^{-1}(\alpha,\gamma)\right)=\pi_J\left(\Psi_1^{-1}(\alpha,0)\right),\\ \pi_{(J^{\vee 0})^{\rho-1}}\left(\Psi^{-1}(\alpha,\beta,\gamma)\right)&=\pi_{(J^{\vee 0})^{\rho-1}}\left(\Psi_2^{-1}(\beta,\gamma)\right)=\pi_{(J^{\vee 0})^{\rho-1}}\left(\Psi_2^{-1}(\beta,0)\right).\end{aligned}\tag{2.4.1}$$

Moreover, using the $\mathbb{G}_{\mathrm{m}}^{\rho-1}$-structure of $P^{\times,\rho-1}$ and the fact that both the groups $\pi_J^{-1}(0)$ and $\pi_{J^{\vee 0},\rho-1}^{-1}(0)$ are base changes of $\mathbb{G}_{\mathrm{m}}^{\rho-1}$, for every $(\alpha,\beta,\gamma)\in\mathbb{Z}_p^g\times\mathbb{Z}_p^{\rho g-g}\times\mathbb{Z}_p^{\rho-1}$ we have

$$\begin{aligned}\Psi^{-1}(\alpha,\beta,\gamma)&=\Psi^{-1}(0,\beta,\gamma)+_1\Psi^{-1}(\alpha,\beta,0)=\exp^{\rho-1}(\gamma)\cdot\Psi^{-1}(\alpha,\beta,0),\\ \Psi_1^{-1}(\alpha,\gamma)&=\Psi_1^{-1}(0,\gamma)+_1\Psi_1^{-1}(\alpha,0)=\exp^{\rho-1}(\gamma)\cdot\Psi_1^{-1}(\alpha,0),\\ \Psi_2^{-1}(\beta,\gamma)&=\Psi_2^{-1}(\beta,\gamma)+_2\Psi_2^{-1}(\beta,0)=\exp^{\rho-1}(\gamma)\cdot\Psi_2^{-1}(\beta,0),\end{aligned}$$

where $\exp^{\rho-1}\colon\mathbb{Z}_p^{\rho-1}\to\mathbb{Z}_p^{\times,\rho-1}$ is obtained taking the $(\rho-1)$-th power of

$$\exp\colon\mathbb{Z}_p\longrightarrow\mathbb{G}_{\mathrm{m}}(\mathbb{Z}_p)_{\overline{1}}=1+p\mathbb{Z}_p,$$

which is the inverse of the map (2.3.3) induced by the formal logarithm of $\mathbb{G}_{\mathrm{m}}$. By (2.4.1), we can "translate" the map Ψ by Ψ_1 and Ψ_2, obtaining the following map

$$\begin{aligned}\Phi\colon\mathbb{Z}_p^g\times\mathbb{Z}_p^{\rho g-g}\times\mathbb{Z}_p^{\rho-1}&\longrightarrow P^{\times,\rho-1}(\mathbb{Z}_p)_t\\ (\alpha,\beta,\gamma)&\longmapsto\left(\Psi^{-1}(\alpha,\beta,\gamma)+_2\Psi_1^{-1}(\alpha,0)\right)+_1\left(\Psi_2^{-1}(\beta,0)+_2\widetilde{t}\right)\\ &=\exp^{\rho-1}(\gamma)\cdot\left(\left(\Psi^{-1}(\alpha,\beta,0)+_2\Psi_1^{-1}(\alpha,0)\right)+_1\left(\Psi_2^{-1}(\beta,0)+_2\widetilde{t}\right)\right).\end{aligned}$$

Let us fix coordinates to study Φ. Let $u_1,\dots,u_{\rho g-g}$ be elements of $\mathcal{O}_{(J^{\vee 0})^{\rho-1},m\cdot\mathrm{otr}_c\circ f(j_b(u))}$ such that together with p they form a system of parameters of $\mathcal{O}_{(J^{\vee 0})^{\rho-1},m\cdot\mathrm{otr}_c\circ f(j_b(u))}$, and let us lift $v_1,\dots,v_{\rho-1}$ to elements in $\mathcal{O}_{P^{\times,\rho-1},t}$. Then $u_1,\dots,u_{\rho g-g}$, $v_1,\dots,v_{\rho-1}$ and p, together with $x_1,\dots,x_g$ defined in the statement of Theorem 1.4.10, form a a system of parameters of $\mathcal{O}_{P^{\times,\rho-1},t}$. The functions $\widetilde{x}_i:=\frac{x_i}{p}$, $\widetilde{u}_i:=\frac{u_i}{p}$ and $\widetilde{v}_i:=\frac{v_i}{p}$ give bijections with powers of $\mathbb{Z}_p$ that make the following diagram commute

$$\begin{array}{ccc}P^{\times,\rho-1}(\mathbb{Z}_p)_t & \xrightarrow{(\widetilde{x},\widetilde{u},\widetilde{v})=(\widetilde{x}_1,\dots,\widetilde{x}_g,\widetilde{u}_1,\dots,\widetilde{u}_{\rho g-g},\widetilde{v}_1,\dots,\widetilde{v}_{\rho-1})} & \mathbb{Z}_p^g\times\mathbb{Z}_p^{\rho g-g}\times\mathbb{Z}_p^{\rho-1}\\ \uparrow & & \downarrow\\ T(\mathbb{Z}_p)_t & \xrightarrow{(\widetilde{x}_1,\dots,\widetilde{x}_g,\widetilde{v}_1,\dots,\widetilde{v}_{\rho-1})} & \mathbb{Z}_p^g\times\mathbb{Z}_p^{\rho g-g}\times\mathbb{Z}_p^{\rho-1}\end{array}.$$

The biextension structure on $P^{\times,\rho-1}$ implies that Φ is a bijection and, since it is defined composing maps given by integral power series that reduce to linear polynomials

modulo p, then $(\widetilde{x},\widetilde{u},\widetilde{v})\circ\Phi$ is given by power series that reduce to linear polynomials modulo p. Hence the same is true for the inverse of $(\widetilde{x},\widetilde{u},\widetilde{v})\circ\Phi$. This and the commutativity of the above diagram imply that, in order to prove Theorem 1.4.10, it is enough to prove that the map $\Phi^{-1}\circ\kappa_{\mathbb{Z}}$ is given by $g+(\rho g-g)$ linear polynomials and $\rho-1$ quadratic polynomials in the n_i and also proving that $\Phi^{-1}(\overline{T(\mathbb{Z})_t})$ is the image of such a polynomial map. To do so we give names to the coordinates of the relevant points: for each $i,j\in\{1,\dots,r\}$ let $P_{i,j},R_{i,\widetilde{t}},S_{\widetilde{t},j}\in P^{\times,\rho-1}(\mathbb{Z})$ be as in Equation (1.4.1) and let $\alpha_i\in\mathbb{Z}_p^g$, $\beta_j\in\mathbb{Z}_p^{\rho g-g}$, $\gamma_{i,j},\gamma_{i,\widetilde{t}},\gamma_{\widetilde{t},j}\in\mathbb{Z}_p^{\rho-1}$ and $\xi_{i,j},\xi_{i,\widetilde{t}},\xi_{\widetilde{t},j}\in\mathbb{F}_p^{\times,\rho-1}\subset\mathbb{Z}_p^{\times,\rho-1}$ be such that

$$P_{i,j}=\xi_{i,j}\cdot\Psi^{-1}(\alpha_i,\beta_j,\gamma_{i,j})\,,\quad R_{i,\widetilde{t}}=\xi_{i,\widetilde{t}}\cdot\Psi_1^{-1}(\alpha_i,\gamma_{i,\widetilde{t}})\,,\quad S_{\widetilde{t},j}=\xi_{\widetilde{t},j}\cdot\Psi_2^{-1}(\beta_j,\gamma_{\widetilde{t},j})\,.$$

The maps Ψ,Ψ_1 and Ψ_2 are formal logarithms, hence they allow us to write very easily the two partial group laws, and in particular we can describe the maps A,B,C,D in Equations (1.4.2), (1.4.3) and (1.4.4) as follows

$$\begin{aligned}
A_{\widetilde{t}}(n)&=\sum_{j=1}^{r}{}_2\, n_j\cdot_2 S_{\widetilde{t},j}=\left(\prod_{j=1}^{r}\xi_{\widetilde{t},j}^{n_j}\right)\cdot\Psi_2^{-1}\left(\sum_{j=1}^{r}n_j\beta_j\,,\sum_{j=1}^{r}n_j\gamma_{\widetilde{t},j}\right)\,,\\
B_{\widetilde{t}}(n)&=\sum_{i=1}^{r}{}_1\, n_i\cdot_1 R_{i,\widetilde{t}}=\left(\prod_{i=1}^{r}\xi_{i,\widetilde{t}}^{n_i}\right)\cdot\Psi_1^{-1}\left(\sum_{i=1}^{r}n_i\alpha_i\,,\sum_{i=1}^{r}n_i\gamma_{i,\widetilde{t}}\right)\,,\\
C(n)&=\sum_{i=1}^{r}{}_1\, n_i\cdot_1\Big(\sum_{j=1}^{r}{}_2\, n_j\cdot_2 P_{i,j}\Big)\\
&=\left(\prod_{i,j=1}^{r}\xi_{i,j}^{n_in_j}\right)\cdot\Psi^{-1}\left(\sum_{i=1}^{r}n_i\alpha_i\,,\sum_{j=1}^{r}n_j\beta_j\,,\sum_{i,j=1}^{r}n_in_j\gamma_{i,j}\right)\,,\\
D_{\widetilde{t}}(n)&=\big(C(n)+_2 B_{\widetilde{t}}(n)\big)+_1\big(A_{\widetilde{t}}(n)+_2\widetilde{t}\big)\\
&=\xi(n)\cdot\Phi\left(\sum_{i=1}^{r}n_i\alpha_i\,,\sum_{j=1}^{r}n_j\beta_j\,,\sum_{i,j=1}^{r}n_in_j\gamma_{i,j}+\sum_{j=1}^{r}n_j\gamma_{\widetilde{t},j}+\sum_{i=1}^{r}n_i\gamma_{i,\widetilde{t}}\right)\,,\\
&\text{with }\xi(n):=\prod_{i,j=1}^{r}\xi_{i,j}^{n_in_j}\cdot\prod_{i=1}^{r}\xi_{i,\widetilde{t}}^{n_i}\cdot\prod_{j=1}^{r}\xi_{\widetilde{t},j}^{n_j}\in\mathbb{F}_p^{\times,\rho-1}\,.
\end{aligned}$$

For any $n\in\mathbb{Z}^r$ we have $\xi((p-1)n)=1$, hence

$$\begin{aligned}
\Phi^{-1}\circ\kappa_{\mathbb{Z}}(n)&=\Phi^{-1}(D_{\widetilde{t}}((p-1)n))\\
&=\left((p-1)\sum_{i=1}^{r}n_i\alpha_i\,,(p-1)\sum_{j=1}^{r}n_j\beta_j\,,(p-1)^2\sum_{i,j=1}^{r}n_in_j\gamma_{i,j}+(p-1)\sum_{i=1}^{r}n_i(\gamma_{i,\widetilde{t}}+\gamma_{\widetilde{t},i})\right)
\end{aligned}$$

is described by linear and quadratic polynomial in n_i and extends continuously to

$$\Phi^{-1}\circ\kappa\colon\mathbb{Z}_p^r\longrightarrow\mathbb{Z}_p^g\times\mathbb{Z}_p^{\rho g-g}\times\mathbb{Z}_p^{\rho-1}\,.$$

Finally,

$$\kappa(\mathbb{Z}^r) \subset T(\mathbb{Z})_t \subset \left(\mathbb{F}_p^{\times,\rho-1} \cdot D_{\widetilde{t}}(\mathbb{Z}^r)\right) \cap P^{\times,\rho-1}(\mathbb{Z}_p)_t = \kappa\left(\tfrac{1}{p-1}\mathbb{Z}^r\right),$$

hence

$$\kappa(\mathbb{Z}_p^r) \subset \overline{T(\mathbb{Z})_t} \subset \kappa(\mathbb{Z}_p^r).$$

Chapter 3

Automorphisms of Cartan curves

This chapter is the result of a joint work with Valerio Dose and Pietro Mercuri

We study the automorphisms of modular curves associated to Cartan subgroups of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ and certain subgroups of their normalizers. We prove that if n is large enough, all the automorphisms are induced by the ramified covering of the complex upper half-plane. We get new results for non-split curves of prime level $p \geq 13$: the curve $X_{\mathrm{ns}}^{+}(p)$ has no non-trivial automorphisms, whereas the curve $X_{\mathrm{ns}}(p)$ has exactly one non-trivial automorphism. Moreover, as an immediate consequence of our results we compute the automorphism group of $X_0^*(n) := X_0(n)/W$, where W is the group generated by the Atkin-Lehner involutions of $X_0(n)$ and n is a large enough square.

3.1 Introduction

Since the 1970s many efforts have been made to determine automorphisms of modular curves and in particular to establish whether a modular curve has other automorphisms besides the expected ones. Indeed, infinitely many automorphisms naturally arise when the curve has genus zero or one. Moreover, since the components of modular curves over $\mathbb{C}$ can be seen as compactification of quotients of the complex upper half-plane $\mathbb{H}$, some automorphisms of $\mathbb{H}$ induce automorphisms of the quotient modular curve. Such automorphisms are called *modular* and their determination is a purely group theoretic problem.

The focus has been classically placed on the modular curves $X_0(n)$ associated to a Borel subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ (e.g., upper triangular matrices), with n a positive integer. For these curves, modular automorphisms played an important role in the development of the theory of modular curves. They were determined in the seminal paper [4], with a

small gap which was later filled in a couple of different ways (see [2], [14]). Meanwhile, a complete picture about the remaining automorphisms of $X_0(n)$ has been painted through the decades by the works [83], [85], [60], [42], [52]. Also some works in this century (e.g., [5], [74], [47]) took on the case of the modular curves $X_0(p)/\langle w_p\rangle$ and $X_0(p^2)/\langle w_{p^2}\rangle$, where w_p and w_{p^2} are the Atkin-Lehner involutions of the respective modular curve.

More recently, great interest has been generated in modular curves associated to different subgroups of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, in particular to normalizers of Cartan subgroups for $n = p$ prime. This is mainly due to the fact that rational points on these curves help classifying rational elliptic curves whose associated Galois representation modulo p is not surjective. This is directly linked to a question formulated by Serre (also known as *uniformity conjecture*) in the 1970s ([92]). After the works [72], on the Borel case, and [17], [18], on the *split* Cartan case, the only part of this problem left to understand nowadays is equivalent to asking whether, for almost every prime p, the modular curve $X_{\mathrm{ns}}^+(p)$ associated to the normalizer of a *non-split* Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ has other rational points besides the expected ones, namely the CM points of class number one. Such equivalence led to a certain amount of research driven towards computing equations and finding rational points of modular curves associated to non-split Cartan subgroups and their normalizers (see for example [12], [13], [10], [35], [36], [75]).

A curious connection between the problem of determining rational points and the one of determining automorphisms in a modular curve is given by the fact that in the case of the Borel modular curves $X_0(p)$ of genus at least 2, the sole occurrence of unexpected rational points ($p = 37$) in the setting of Serre's uniformity conjecture, happens in the presence of an unexpected automorphism of the corresponding modular curve. A further connection is made in [37], where is proven that, for almost every prime p, the absence of unexpected rational points of the curve $X_{\mathrm{ns}}^+(p)$ implies the absence of unexpected rational automorphisms of the modular curve $X_{\mathrm{ns}}(p)$ associated to a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

The first work centered on automorphisms of non-split Cartan modular curves has been [35], in which the existence of an unexpected automorphism of $X_{\mathrm{ns}}(11)$ is proven. Some partial results on the automorphisms of $X_{\mathrm{ns}}(p)$ and $X_{\mathrm{ns}}^+(p)$, for almost every prime p, were proven in [37], while in [48] the full determination of the automorphism group is obtained for low primes ($p \leq 31$).

In the present work we complete the results in [37] about the prime level case. Moreover, we extend the analysis to every composite level n, where we can define Cartan subgroups of mixed split/non-split type. The scope of our study concerns Cartan subgroups and also a specific subgroup of their normalizer in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ which we call *Cartan-plus* subgroup. However, in most cases, for example when n is odd, a Cartan-

plus subgroup actually coincides with the normalizer of the relative Cartan subgroup. We prove the following result:

Theorem 3.6.15. *Let $n \geq 10^{400}$ be an integer and let $H < \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ be either a Cartan or a Cartan-plus subgroup. Then every automorphism of X_H is modular, hence we have*

$$\mathrm{Aut}(X_H) \cong \begin{cases} N'/H' \times \mathbb{Z}/2\mathbb{Z}, & \text{if } n \equiv 2 \bmod 4 \text{ and } H \text{ is a Cartan-plus split at 2,} \\ N'/H', & \text{otherwise,} \end{cases}$$

where $N' < \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ is the normalizer of $H' := H \cap \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$.

It may be interesting to note that the modular curve associated to a Cartan-plus subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ which is split at every prime dividing n is isomorphic to the modular curve $X_0^*(n^2) := X_0(n^2)/W$, where W is the group generated by Atkin-Lehner involutions of the Borel curve $X_0(n^2)$.

In the case $n = p^e$, where p is a prime number, we can refine the techniques developed and obtain a more complete result:

Theorem 3.6.17. *Let p be a prime number and let e be a positive integer. If $p^e > 11$ and $p^e \notin \{3^3, 2^4, 2^5, 2^6\}$, then all the automorphisms of $X_{\mathrm{ns}}(p^e), X_{\mathrm{ns}}^+(p^e), X_{\mathrm{s}}(p^e)$ and $X_{\mathrm{s}}^+(p^e)$ are modular and*

$$\mathrm{Aut}(X_{\mathrm{ns}}(p^e)) \cong \mathbb{Z}/2\mathbb{Z}, \qquad \mathrm{Aut}(X_{\mathrm{ns}}^+(p^e)) \cong \{1\},$$

$$\mathrm{Aut}(X_{\mathrm{s}}(p^e)) \cong \begin{cases} (\mathbb{Z}/8\mathbb{Z})^2 \rtimes (\mathbb{Z}/2\mathbb{Z}), & \text{if } p = 2, \\ \mathbb{Z}/3\mathbb{Z} \times S_3, & \text{if } p = 3, \\ \mathbb{Z}/2\mathbb{Z}, & \text{if } p > 3, \end{cases} \quad \mathrm{Aut}(X_{\mathrm{s}}^+(p^e)) \cong \begin{cases} \mathbb{Z}/8\mathbb{Z}, & \text{if } p = 2, \\ \mathbb{Z}/3\mathbb{Z}, & \text{if } p = 3, \\ \{1\}, & \text{if } p > 3, \end{cases}$$

where the above semidirect product $(\mathbb{Z}/8\mathbb{Z})^2 \rtimes \mathbb{Z}/2\mathbb{Z}$ is described in Remark 3.6.16.

Corollary 3.6.18. *Let $p \geq 13$ be a prime number. Then the group of automorphisms of $X_{\mathrm{ns}}^+(p)$ is trivial and the group of automorphisms of $X_{\mathrm{ns}}(p)$ has order 2.*

The main technical novelty of our proofs is a thorough analysis of the action of Hecke operators on very general modular curves. This allows us to prove results about automorphisms without exploiting and worrying about the field of definition of the cusps and CM points which has been instead instrumental for determining automorphisms of modular curves throughout the literature in the past. We also give à la Chen results to describe jacobians of Cartan modular curves in terms of jacobians of Borel modular curves and we give an explicit upper bound on the dimension of the CM part of the jacobian of Borel modular curves. The structure of the paper is the following.

In Section 3.2 we define modular curves associated to general subgroups of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ and we give an equivalent condition to the fact that a point of a modular curves branches in the covering of the curve by $\mathbb{H}$.

In Section 3.3 we study the action of Hecke operators on modular curves. In particular we focus on the action on the cusps and the other points which could branch in the covering by $\mathbb{H}$. Such points are associated to elliptic curves with j-invariant equal to 0 or 1728.

In Section 3.4 we define Cartan and Cartan-plus subgroups of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ for every positive integer n. We also define the relative modular curves of composite level. Then we prove that the jacobian of a Cartan modular curve is a quotient of the jacobian of some Borel modular curve. When $n = p^e$, this is done applying the techniques of [26] and [39] to a previously unexplored case, and for n general we combine these results. We also extend the results of [26] to the case of even level.

In Section 3.5 we prove that all the automorphisms of Cartan modular curves must be defined on a compositum of quadratic fields when the level n is large enough. To do this, we use a geometrical criterion that we can apply by bounding the dimension of the CM part of the jacobian of Cartan modular curves. This last step is obtained using the isogenies of Section 3.4 and computing explicit bounds for the CM part of the jacobians of Borel modular curves. Furthermore, we refine the results in the case $n = p^e$, with p prime.

Finally, in Section 3.6 we prove the results stated above about automorphisms. The main idea is to show that each automorphism must preserve the cusps and the set of branching points of the covering by $\mathbb{H}$. This implies that there are no non-modular automorphisms. Thus, we compute the modular automorphisms to complete the analysis. We first concentrate on Cartan modular curves of general level n. Then we adapt the strategy to the case $n = p^e$, with p prime, giving the complete result for $X_{\mathrm{ns}}(p)$ and $X_{\mathrm{ns}}^+(p)$, and improving the result we obtained for the general level in the cases of $X_{\mathrm{s}}^+(p^e)$, $X_{\mathrm{ns}}(p^e)$ and $X_{\mathrm{ns}}^+(p^e)$. To treat some of the small level cases, we use the criterion of [48] which we verify through an algorithm implemented in MAGMA ([69]) which is available at [70].

As we did for the case of level $n = p^e$, with p prime, the result on Cartan modular curves of composite level can be sharpened, with our techniques, for levels with a specific type of factorization. However, certain cases remain out of the reach of the strategy described in this work, for example when we are not able to apply the criterion of [48] and either the curve has low gonality (e.g., $X_{\mathrm{ns}}(16)$, $X_{\mathrm{ns}}^+(16)$, $X_{\mathrm{ns}}^+(27)$) or its jacobian has a large CM part relative to its dimension (see Remark 3.5.11 for the example with the lowest level).

3.2 Modular curves

Let n be a positive integer. We denote by $Y(n)$ the (coarse if $n < 3$) moduli space that parametrizes pairs (E, ϕ) where E is an elliptic curve over a $\mathbb{Q}$-scheme S and $\phi\colon (\mathbb{Z}/n\mathbb{Z})^2_S \to E[n]$ is an isomorphism of S-group schemes. We denote by $X(n)$ the compactification of $Y(n)$ and we call $X(n)$ the *modular curve of full level n*.

Every matrix $\gamma \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ gives an automorphism of the constant group scheme $(\mathbb{Z}/n\mathbb{Z})^2_S$, hence γ acts on $Y(n)$ sending (E, ϕ) to $(E, \phi \circ \gamma)$. This defines an action of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ on $Y(n)$ that extends uniquely to $X(n)$. For each subgroup H of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, let X_H be the quotient $X(n)/H$. By [32, IV.6.7], X_H has good reduction over each prime that does not divide n and the smooth model of $Y_H = Y(n)/H$ over $\mathbb{Z}[1/n]$ is a coarse moduli space for *elliptic curves with H-structure*, i.e., the equivalence classes of pairs (E, ϕ) where E is an elliptic curve over a $\mathbb{Z}[1/n]$-scheme S and $\phi\colon (\mathbb{Z}/n\mathbb{Z})^2_S \to E[n]$ is an isomorphism of S-group schemes, and the equivalence relation is given by:

$$(3.2.1)\quad (E, \phi) \sim_H (E', \phi') \iff (\phi')^{-1} \circ \iota|_{E[n]} \circ \phi = h, \text{ for some } h \in H \text{ and } \iota\colon E \xrightarrow{\sim} E'.$$

In particular, for every algebraically closed field K of characteristic $p \nmid n$, we have a bijection between $Y_H(K)$ and the set of elliptic curves over K with H-structure.

Remark 3.2.2. Since -1 is an automorphism of every elliptic curve, then for every H, the curve X_H is isomorphic to $X_{\pm H}$, where $\pm H := \{\pm \mathrm{Id}\}\cdot H < \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Hence, the equivalence relation (3.2.1) can be written as follows

$$(E, \phi) \sim_H (E', \phi') \iff (\phi')^{-1} \circ \iota|_{E[n]} \circ \phi = h, \text{ for some } h \in \pm H \text{ and } \iota\colon E \xrightarrow{\sim} E'.$$

Let $\mathbb{H}$ be the complex upper half-plane $\{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}$, let $\mathbb{H}^{\pm} = \mathbb{C} - \mathbb{R}$ and moreover let $\overline{\mathbb{H}} = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ and $\overline{\mathbb{H}}^{\pm} = \mathbb{H}^{\pm} \cup \mathbb{P}^1(\mathbb{Q})$ be their "compactifications". The group $\mathrm{GL}_2(\mathbb{Z})$ acts on $\mathbb{H}$, $\mathbb{H}^{\pm}$, $\overline{\mathbb{H}}$ and $\overline{\mathbb{H}}^{\pm}$ by Möbius transformations. Moreover, every g in $\mathrm{GL}_2(\mathbb{Z})$ acts on pairs $(z, \gamma H) \in \mathbb{H}^{\pm} \times (\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})/H)$ as $(g(z), \bar{g}\gamma H)$, where $g(z)$ is the image of z under the Möbius transformation given by g and $\bar{g}$ is the reduction of g mod n. This action gives canonical isomorphisms of Riemann surfaces

$$\mathrm{GL}_2(\mathbb{Z})\backslash\big(\mathbb{H}^{\pm} \times (\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})/H)\big) \longrightarrow Y_H(\mathbb{C}), \tag{3.2.2.1}$$

$$\mathrm{GL}_2(\mathbb{Z})\backslash\big(\overline{\mathbb{H}}^{\pm} \times (\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})/H)\big) \longrightarrow X_H(\mathbb{C}). \tag{3.2.2.2}$$

The isomorphism (3.2.2.1) is equivalent to that one described in [32, IV.5.3] and is given by $\mathrm{GL}_2(\mathbb{Z})(\tau, \gamma H) \mapsto (E_\tau, \phi_\tau \circ \gamma)$, where E_τ is the elliptic curve $\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$ and $\phi_\tau\colon (\mathbb{Z}/n\mathbb{Z})^2_{\mathbb{C}} \to E_\tau[n]$ is the unique isomorphism such that

$$\phi_\tau \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{n}, \quad \phi_\tau \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{\tau}{n}.$$

The isomorphism (3.2.2.2) is just the extension of the previous one to the compactifications. For each subgroup H of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, we define

$$\Gamma_H := \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \pmod n \text{ lies in } H\}.$$

If $\det H \neq (\mathbb{Z}/n\mathbb{Z})^\times$, then $X_H(\mathbb{C})$ is not connected: the number of connected components is $[(\mathbb{Z}/n\mathbb{Z})^\times : \det(H)]$ and, for each connected component $X_H^{cc}(\mathbb{C})$, there are isomorphisms of Riemann surfaces

$$\Gamma_{gHg^{-1}}\backslash\overline{\mathbb{H}} \longrightarrow X_H^{cc}(\mathbb{C}), \quad \Gamma_{gHg^{-1}}\backslash\mathbb{H} \longrightarrow Y_H^{cc}(\mathbb{C}), \tag{3.2.3}$$

for some g in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. In particular, if $\det H = (\mathbb{Z}/n\mathbb{Z})^\times$, then Y_H and X_H are geometrically connected curves defined over $\mathbb{Q}$.

The following proposition about the morphisms (3.2.3) is used in Section 3.6. We say that an automorphism of an elliptic curve is *non-trivial* if it is different from $\pm\mathrm{Id}$.

Proposition 3.2.4. *Let n be a positive integer, let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, let g be in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ and consider the composition*

$$\mathbb{H} \longrightarrow \Gamma_{gHg^{-1}}\backslash\mathbb{H} \hookrightarrow Y_H(\mathbb{C}),$$

where the left map is the natural projection and the right map is in (3.2.3). Then a point $(E,\phi) \in Y_H(\mathbb{C})$ is a branch point for such composition if and only if there is a non-trivial automorphism u of E such that $\phi^{-1}\circ u|_{E[n]}\circ\phi \in \pm H$. If this happens, then each point $\tau \in \mathbb{H}$ projecting to (E,ϕ) has ramification index $\#\mathrm{Aut}(E)/2$.

Proof. By Remark 3.2.2 we can suppose that H contains $-\mathrm{Id}$. Instead of looking at a map $\mathbb{H} \to Y_H(\mathbb{C})$ parametrizing a single component of Y_H, we can work with the canonical map

$$\mathbb{H}^\pm \times \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \xrightarrow{\pi} Y(n)(\mathbb{C}) \xrightarrow{\pi_H} Y_H(\mathbb{C}).$$

Up to substituting n with $3n$ and H with its preimage under $\mathrm{GL}_2(\mathbb{Z}/3n\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, we can suppose that $n \geq 3$. This implies that π is an (unramified) covering map, hence the ramification index of the $\pi_H \circ \pi$ in a point (τ,γ) is equal to the ramification index of π_H in the point $\pi(\tau,\gamma)$. Hence, we only need to look at the ramification points of π_H. A point $(E,\phi) \in Y_H(\mathbb{C})$ is a branch point for π_H if and only if the fiber $\pi_H^{-1}(E,\phi)$ has

cardinality smaller than $\deg \pi_H = \#H/2$. The modular interpretation of Y_H and $Y(n)$ implies that

$$\pi_H^{-1}(E,\phi) = \big\{(E, u|_{E[n]}\circ\phi\circ h) : h \in H, u \in \mathrm{Aut}(E)\big\}/\mathrm{Aut}(E), \tag{3.2.5}$$

where $v \in \mathrm{Aut}(E)$ acts sending (E,ψ) to $(E, v|_{E[n]}\circ\psi)$. Since $n \geq 3$, the map that sends u to $\phi^{-1}\circ u|_{E[n]}\circ\phi$ gives an inclusion $\mathrm{Aut}(E) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, hence, by (3.2.5), we have

$$\#\pi_H^{-1}(E,\phi) = \#\Big((H\cdot\mathrm{Aut}(E))/\mathrm{Aut}(E)\Big) = \#\Big(H/(H\cap\mathrm{Aut}(E))\Big).$$

The group $\mathrm{Aut}(E)$ always contains the multiplication by -1 and is cyclic of order $2, 4$ or 6. Finally, there are two options for $\mathrm{Aut}(E)\cap H$:

- $\mathrm{Aut}(E)\cap H$ only contains $\pm\mathrm{Id}$ and (E,ϕ) is not a branch point;
- $\mathrm{Aut}(E)\cap H$ has order equal to $\#\mathrm{Aut}(E) > 2$, in this case (E,ϕ) is a branch point and, since the map π_H is Galois, every point in $\pi_H^{-1}(E,\phi)$ has ramification index equal to $\deg(\pi_H)/\#\pi_H^{-1}(E,\phi) = \#\mathrm{Aut}(E)/2$.

□

3.3 Hecke operators

Let n be a positive integer and let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. For every prime $\ell \nmid n$, there is a divisor $D_\ell \subset X_H \times X_H$ inducing the ℓ-th Hecke operator

$$T_\ell \colon \mathrm{Div}(X_H) \to \mathrm{Div}(X_H), \quad T_\ell \colon \mathrm{Jac}(X_H) \to \mathrm{Jac}(X_H).$$

On $Y_H(\mathbb{C})$, it is described by

$$T_\ell(E,\phi) = \sum_{0\lneq C\lneq E[\ell]} (E/C, \pi_C \circ \phi), \tag{3.3.1}$$

where $\pi_C \colon E \to E/C$ is the natural projection. Now we recall the definition of T_ℓ. Let H_ℓ be the subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\ell\mathbb{Z})$ containing the matrices whose reduction modulo n lies in H and whose reduction modulo ℓ is an upper triangular matrix. Given a $\mathbb{Z}[\frac{1}{n\ell}]$-scheme S and an elliptic curve E/S with H_ℓ-structure $\phi \colon (\mathbb{Z}/n\ell\mathbb{Z})^2 \to E[n\ell]$, we have two ways of constructing an elliptic curve over S with H-structure:

- The n-torsion subgroup of $(\mathbb{Z}/n\ell\mathbb{Z})^2$ is canonically isomorphic, via the Chinese Remainder Theorem, to $(\mathbb{Z}/n\mathbb{Z})^2$ and the restriction of ϕ to this subgroup gives an isomorphism $\phi|_{(\mathbb{Z}/n\mathbb{Z})^2} \colon (\mathbb{Z}/n\mathbb{Z})^2 \to E[n]$. One can check that the class of

$(E, \phi|_{(\mathbb{Z}/n\mathbb{Z})^2})$ modulo $\sim_H$ does not depend on the choice of the representative (E, ϕ) in the equivalence class defined by $\sim_{H_\ell}$, hence

$$\mathrm{pr}(E, \phi) := (E, \phi|_{(\mathbb{Z}/n\mathbb{Z})^2})$$

is a well defined elliptic curve over S with H-structure.

- The subgroup $C \subset E[\ell]$ generated by $\phi(\begin{smallmatrix} n \\ 0 \end{smallmatrix})$ is a subgroup of E of order ℓ and E/C is an elliptic curve over S. Denoting by $\pi_C \colon E \to E/C$ the natural projection, we have that

$$\mathrm{qt}(E, \phi) := (E/C, \pi_C \circ \phi|_{(\mathbb{Z}/n\mathbb{Z})^2})$$

is a well defined elliptic curve over S with H-structure.

These two constructions define natural transformations between the functor of elliptic curves with H_ℓ-structure and the functor of elliptic curves with H-structure restricted to schemes over $\mathbb{Z}[\frac{1}{n\ell}]$. We get induced morphisms between the coarse moduli spaces Y_{H_ℓ} and $(Y_H)_{\mathbb{Z}[\frac{1}{n\ell}]}$ that can be extended by smoothness to the compactifications:

$$\mathrm{pr}, \mathrm{qt} \colon X_{H_\ell} \longrightarrow (X_H)_{\mathbb{Z}[\frac{1}{n\ell}]}.$$

The image of X_{H_ℓ} under the map $(\mathrm{pr}, \mathrm{qt})$ defines a divisor inside $(X_H)_{\mathbb{Z}[\frac{1}{n\ell}]} \times (X_H)_{\mathbb{Z}[\frac{1}{n\ell}]}$. Since X_H is smooth over $\mathbb{Z}[\frac{1}{n}]$, this divisor extends uniquely to $D_\ell \subset X_H \times X_H$ whose irreducible components project surjectively on each factor X_H. This correspondence induces the operator $T_\ell = \mathrm{qt}_* \circ \mathrm{pr}^*$ and the definitions of qt and pr imply the equality (3.3.1).

The reduction of T_ℓ modulo ℓ is described by a celebrated theorem of Eichler and Shimura. To state this theorem in the full generality, we recall the definition of diamond operators. Let $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, then the matrix $(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix})$ normalizes H, hence

$$\langle a \rangle (E, \phi) := (E, \phi \circ (\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}))$$

defines an automorphism of the functor of elliptic curves with H-structure. So $\langle a \rangle$ induces an automorphism of the coarse moduli space Y_H and it extends to an automorphism of the compactification X_H. Eichler-Shimura Relation is nowadays a common knowledge, but in the literature is often stated in a different form than we need. The proof of [38, Theorem 8.7.2] can be directly adapted to our case, and another proof is in [94, Theorem 7.9 and Corollary 7.10]. We use the result in the following form.

Theorem (Eichler-Shimura Relation). *Let n be a positive integer, let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, let ℓ be a prime number not dividing n, let $\overline{X}_H$ be the reduction of X_H modulo ℓ, let $\overline{T}_\ell, \overline{\langle \ell \rangle} \colon \mathrm{Div}(\overline{X}_H) \to \mathrm{Div}(\overline{X}_H)$ be the reduction of the Hecke operator T_ℓ*

and of the diamond operator $\langle \ell \rangle$ *and let* $\mathrm{Frob}_\ell \colon \overline{X}_H \to \overline{X}_H$ *be the Frobenius morphism. Then*

$$\overline{T}_\ell = (\mathrm{Frob}_\ell)_* + \overline{\langle \ell \rangle}_* \circ (\mathrm{Frob}_\ell)^*.$$

Notice that in general X_H is not geometrically connected and if X' is a component of $\overline{X}_H$, the Frobenius morphism $\overline{X}_H \to \overline{X}_H$ may not restrict to a morphishm $X' \to X'$. Analogously, if x is a point on X', the divisor $T_\ell(x)$ may be not supported on X'. We are interested in Eichler-Shimura Relation because, as already pointed out in [60, Lemma 2.6], it implies that, in certain cases, Hecke operators commute with automorphisms of modular curves.

Proposition 3.3.2. *Let* n *be a positive integer, let* $H < \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ *be a subgroup containing the scalar matrices and such that* $\det H = (\mathbb{Z}/n\mathbb{Z})^\times$. *Let* ℓ *be a prime not dividing* n *and let* $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *be a Frobenius element at* ℓ. *Then, for any automorphism* u *of* X_H *defined over a compositum of quadratic fields, in* $\mathrm{End}(\mathrm{Jac}(X_H))$ *we have*

$$T_\ell \circ u = u^\sigma \circ T_\ell, \tag{3.3.3}$$

where we identify u *and* u^σ *with their pushforward on* $\mathrm{Jac}(X_H)$. *Moreover, if the gonality of* $X_H(\mathbb{C})$ *is greater than* $2(\ell+1)$, *then (3.3.3) holds at level of divisors.*

Proof. Let $J := \mathrm{Jac}(X_H)$, let $\mathrm{Frob}_\ell \colon \overline{X}_H \to \overline{X}_H$ be the Frobenius morphism and let ϕ_ℓ be the Frobenius generator of $\mathrm{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}_\ell)$. Let $D \in \mathrm{Div}(\overline{X}_H)$ and let $\bar{u}$ be the reduction of u modulo ℓ. Using Eichler-Shimura Relation, we have

$$\begin{aligned}\overline{T}_\ell \circ \bar{u}(D) =& ((\mathrm{Frob}_\ell)_* + (\mathrm{Frob}_\ell)^*) \circ \bar{u}(D) = (\mathrm{Frob}_\ell)_* \bar{u}(D) + (\mathrm{Frob}_\ell)^* \bar{u}(D) = \\ =& \bar{u}^{\phi_\ell} (\mathrm{Frob}_\ell)_*(D) + \bar{u}^{\phi_\ell^{-1}} (\mathrm{Frob}_\ell)^*(D) = \overline{u^\sigma} (\mathrm{Frob}_\ell)_*(D) + \overline{u^{\sigma^{-1}}} (\mathrm{Frob}_\ell)^*(D).\end{aligned}$$

Now, since u is defined over a compositum of quadratic fields, the Galois automorphisms σ and σ^{-1} act in the same way on u. This implies that the last term in the previous chain of equalities is equal to $\overline{u^\sigma} \circ \overline{T}_\ell(D)$ obtaining $\overline{T}_\ell \circ \bar{u} = \overline{u^\sigma} \circ \overline{T}_\ell$ in $\mathrm{End}(J_{\mathbb{F}_\ell})$.

Since J has good reduction at ℓ, the natural map $\mathrm{End}(J) \to \mathrm{End}(J_{\mathbb{F}_\ell})$ is injective, hence (3.3.3) holds in $\mathrm{End}(J)$. This means that, for any two points P and Q in $X_H(\mathbb{C})$, the divisor $D := (T_\ell u - u^\sigma T_\ell)(P - Q)$ is principal. Hence, either D is the zero divisor or is the divisor of a non-constant rational function on X_H of degree at most $2(\ell+1)$.

Now we suppose that the gonality of X_H exceeds $2(\ell+1)$. In this case, there are no non-constant rational functions on X_H of degree at most $2(\ell+1)$, hence D is the zero divisor. This gives the following equality of divisors:

$$T_\ell u(P) + u^\sigma T_\ell(Q) = u^\sigma T_\ell(P) + T_\ell u(Q).$$

For every point P, we can choose Q such that the supports of $T_\ell u(P)$ and $T_\ell u(Q)$ are disjoint, and, therefore, last equality implies $T_\ell u(P) = u^\sigma T_\ell(P)$ as divisors. Up to a base change to $\mathbb{C}$, each divisor on X_H is a sum of points with integer coefficients, hence we conclude that (3.3.3) holds at level of divisors. □

Multiple points in the image of Hecke operators

In the proofs of Section 3.6 we look at points $P \in X_H(\mathbb{C})$ and primes ℓ such that $T_\ell(P)$ is not a sum of distinct points. In this subsection we study this phenomenon. When P is a cusp, we have the following result.

Proposition 3.3.4. *Let n be a positive integer and let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Let ℓ be a prime number not dividing n, let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be a Frobenius element at ℓ and let $C \in X_H(\overline{\mathbb{Q}})$ be a cusp. Then*

$$T_\ell(C) = C^\sigma + \ell \langle \ell \rangle (C^{\sigma^{-1}}).$$

Proof. The divisor $T_\ell(C) = \mathrm{qt}_* \mathrm{pr}^*(C)$ is supported on the cusps because both the maps $\mathrm{pr}, \mathrm{qt} \colon X_{H_\ell} \to X_H$ send non-cuspidal points to non-cuspidal points and cusps to cusps. If we fix a prime ideal $\mathfrak{l}$ in the algebraic integers such that $\mathfrak{l} \mid \ell$, then, by [32, IV.3.4], each cusp in $X_H(\overline{\mathbb{Q}})$ reduces to a different point modulo $\mathfrak{l}$. Thus, it is enough to prove that $T_\ell(C)$ is congruent to $C^\sigma + \ell \langle \ell \rangle (C^{\sigma^{-1}})$ modulo $\mathfrak{l}$, and this is true by Eichler-Shimura Relation. □

We need a criterion to characterize the points $(E, \phi) \in Y_H(\mathbb{C})$ such that their image via T_ℓ contains a point with multiplicity at least 2. It is given by the following lemma.

Lemma 3.3.5. *Let n be a positive integer, let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ and let ℓ be a prime not dividing n. For all points $(E, \phi), (E, \phi') \in Y_H(\mathbb{C})$ and all positive integers $m \geq 2$, the following are equivalent:*

1. *$T_\ell(E, \phi)$ contains (E', ϕ') with multiplicity m;*
2. *there are m isogenies $\alpha_1, \ldots, \alpha_m \colon E \to E'$ of degree ℓ with distinct kernels such that $(\phi')^{-1} \circ \alpha_j|_{E[n]} \circ \phi$ lies in $\pm H$, for every $j = 1, \ldots, m$;*
3. *there are m endomorphisms $\beta_1 = \ell, \beta_2, \ldots, \beta_m$ of E' of degree ℓ^2 and an isogeny $\alpha \colon E' \to E$ of degree ℓ such that:*

P1 *$\beta_i \neq u \circ \beta_j$, for $i, j = 1, \ldots, m$, such that $i \neq j$ and for each $u \in \mathrm{Aut}(E')$;*

P2 *$\ker \alpha \subset \ker \beta_j$, for every j in $\{1, \ldots, m\}$;*

P3 *the matrices* $\ell^{-1}\phi^{-1}\circ\alpha|_{E'[n]}\circ\phi'$ *and* $\ell^{-1}(\phi')^{-1}\circ\beta_j|_{E'[n]}\circ\phi'$ *lie in* $\pm H$*, for every* j *in* $\{1,\dots,m\}$*, where* ℓ^{-1} *is the inverse of the scalar matrix* $\ell \bmod n$*.*

Proof. The equivalence between (1) and (2) follows by definition of Hecke operator. Now we prove the equivalence between (2) and (3). Let $\alpha_1,\dots,\alpha_m$ be isogenies of degree ℓ with distinct kernels, then it is enough to take α equal to the dual of α_1 and $\beta_j=\alpha_j\circ\alpha$, for $j=1,\dots,m$. Conversely, if $\beta_1,\dots,\beta_m$ respect the three properties above, then, for every $j=1,\dots,m$, we can take α_j to be the unique isogeny such that $\beta_j=\alpha_j\circ\alpha$. □

From now on we denote by $\rho=e^{\frac{2\pi i}{3}}$ the primitive third root of unity contained in $\mathbb{H}$. Moreover, for every $\tau\in\mathbb{H}$, we denote by E_τ the elliptic curve $\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$. The following result proves that if $T_\ell(E,\phi)$ shows certain multiplicities, then E has complex multiplication by $\mathbb{Q}(i)$ or $\mathbb{Q}(\rho)$.

Proposition 3.3.6. *Let* n *be a positive integer, let* H *be a subgroup of* $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$*, let* ℓ *be a prime not dividing* n *and let* (E,ϕ) *be a* $\mathbb{C}$*-point of* Y_H*. Then:*

1. *the points in the image* $T_\ell(E,\phi)$ *have multiplicity at most* 3*;*
2. *if* $T_\ell(E,\phi)$ *contains a point with multiplicity* 3*, then* $\mathrm{End}(E)$ *contains* $\mathbb{Z}[\ell^2\rho]$*;*
3. *if* $\ell\geq 5$ *and*

$$T_\ell(E,\phi)=2(P_1+\ldots+P_{\frac{\ell+1}{2}}) \quad \text{or} \quad T_\ell(E,\phi)=2(P_1+\ldots+P_{\frac{\ell-1}{2}})+P_{\frac{\ell+1}{2}}+P_{\frac{\ell+3}{2}},$$

for $P_1,\dots,P_{\frac{\ell+3}{2}}\in Y_H(\mathbb{C})$ *distinct points, then* $\mathrm{End}(E)$ *contains* $\mathbb{Z}[\ell^2 i]$*.*

Proof. Parts (1) and (2).

First we prove that if $T_\ell(E,\phi)$ contains a point with multiplicity at least 3, then $\mathrm{End}(E)$ contains $\mathbb{Z}[\ell^2\rho]$. Let $(E',\phi')\in Y_H(\mathbb{C})$ such that $T_\ell(E,\phi)\geq 3(E',\phi')$, then there are isogenies $\alpha\colon E'\to E$ and $\beta_1=\ell,\beta_2,\beta_3\colon E'\to E'$ as in Lemma 3.3.5 and, consequently, $\mathrm{End}(E')$ and $\mathrm{End}(E)$ are orders in a quadratic field K, with ring of integers $\mathcal{O}_K$. Since $\ker(\alpha)$ is non-trivial and it is contained in $\ker(\beta_j)$, for every $j=1,2,3$, the ideal of $\mathrm{End}(E')$ generated by β_1, β_2, β_3 is non-trivial. Using that $\mathrm{End}(E')\subset\mathcal{O}_K$ is a finite extension of rings, we deduce that the ideal of $\mathcal{O}_K$ generated by β_1, β_2, β_3 is non-trivial as well. The ideals $\beta_1\mathcal{O}_K$, $\beta_2\mathcal{O}_K$ and $\beta_3\mathcal{O}_K$ of $\mathcal{O}_K$ have norm ℓ^2 and if they are three distinct ideals, then there are two distinct primes $\mathfrak{l}_1,\mathfrak{l}_2\subset\ell\mathcal{O}_K$ such that, up to reordering, $\beta_1\mathcal{O}_K=\mathfrak{l}_1\mathfrak{l}_2$, $\beta_2\mathcal{O}_K=\mathfrak{l}_2^2$, $\beta_3\mathcal{O}_K=\mathfrak{l}_1^2$, implying that the ideal of $\mathcal{O}_K$ generated by β_1,β_2,β_3 is the whole $\mathcal{O}_K$, contradiction. Hence the ideals $\beta_1\mathcal{O}_K$, $\beta_2\mathcal{O}_K$ and $\beta_3\mathcal{O}_K$ cannot be distinct.

If $K\notin\{\mathbb{Q}(i),\mathbb{Q}(\rho)\}$, then $\mathcal{O}_K^\times=\{\pm 1\}$, hence $\beta_k\mathcal{O}_K=\beta_j\mathcal{O}_K$ implies $\beta_k=\pm\beta_j$, which is absurd by condition **P1** in Lemma 3.3.5. Hence either $K=\mathbb{Q}(i)$ or $K=\mathbb{Q}(\rho)$.

Then $\mathcal{O}_K = \mathbb{Z}[u]$ with $u \in \{i, \rho\}$ and $\mathrm{End}(E') = \mathbb{Z}[mu]$ for some positive integer $m > 0$. Condition **P1** in Lemma 3.3.5 implies that the ideals of $\mathrm{End}(E')$ generated by β_1, β_2 and β_3 are distinct and we have just proven that their extensions to $\mathbb{Z}[u]$ are not distinct. We know that ideal extension gives a bijection between ideals in $\mathbb{Z}[mu]$ with index coprime to m and ideals in $\mathbb{Z}[u]$ with index coprime to m, hence $\ell^2 = [\mathcal{O}_K : \beta_j \mathcal{O}_K]$ is not coprime to m. Therefore $\ell \mid m$ and $\mathrm{End}(E') \subset \mathbb{Z}[\ell u]$. Hence β_2 and β_3 are elements of $\mathbb{Z}[\ell u]$ having norm equal to ℓ^2 and the only elements of this kind are $\{\pm\ell, \pm\ell u, \pm\ell u^2\}$. If $K = \mathbb{Q}(i)$, then $\beta_1, \beta_2, \beta_3 \in \{\pm\ell, \pm\ell i\}$, contradicting $\beta_k \neq \pm\beta_j$, for $k \neq j$. If $K = \mathbb{Q}(\rho)$, the only possibility, up to reordering, is $\beta_2 = \pm\rho\ell$ and $\beta_3 = \pm\rho^2\ell$ and consequently $m = \ell$. Finally, since there is an isogeny $E' \to E$ of degree ℓ, we have $\mathbb{Z}[\ell^2\rho] \subset \mathrm{End}(E)$.

Finally, we suppose that $(E, \phi) \in Y_H(\mathbb{C})$ and (E', ϕ') appears in $T_\ell(E, \phi)$ with multiplicity at least 4. Then, by what we have just proven, $\mathrm{End}(E') = \mathbb{Z}[\ell\rho]$. Hence, there are exactly 3 elements in $\mathrm{End}(E')$, up to sign, with norm equal to ℓ^2 and we cannot find elements $\beta_1, \ldots, \beta_4$ satisfying the properties of Lemma 3.3.5. This contradiction concludes the proof of Parts (1) and (2).

Part (3).

Let τ be an element of $\mathbb{H}$ such that $E = E_\tau$. Then

$$T_\ell(E, \phi) = (E_{\frac{\tau}{\ell}}, \phi_0) + (E_{\frac{\tau+1}{\ell}}, \phi_1) + \ldots + (E_{\frac{\tau+\ell-1}{\ell}}, \phi_{\ell-1}) + (E_{\ell\tau}, \phi_\ell),$$

for suitable $\phi_0, \ldots, \phi_\ell$. The hypothesis on $T_\ell(E, \phi)$ implies that we can find three distinct integers $r_1, r_2, r_3 \in \{0, \ldots, \ell-1\}$, with corresponding

$$\tau_1 := (\tau + r_1)/\ell, \quad \tau_2 := (\tau + r_2)/\ell, \quad \tau_3 := (\tau + r_3)/\ell, \tag{3.3.7}$$

such that (E_{τ_1}, ϕ_{r_1}), (E_{τ_2}, ϕ_{r_2}) and (E_{τ_3}, ϕ_{r_3}) appear in $T_\ell(E, \phi)$ with multiplicity at least 2. In particular by Lemma 3.3.5 we see that $\mathrm{End}(E_{\tau_k})$ contains a non-trivial element of degree ℓ^2, for $k = 1, 2, 3$, hence E_{τ_k} and E have CM over some quadratic imaginary field $K \subset \mathbb{C}$. Therefore $\tau \in K$ and there are $a, b \in \mathbb{Q}$ such that

$$\tau^2 = a\tau + b. \tag{3.3.8}$$

Hence $\mathrm{End}(E_{\tau_1})$, $\mathrm{End}(E_{\tau_2})$ and $\mathrm{End}(E_{\tau_3})$ are naturally subrings of $\mathcal{O}_K$ the ring of integers of K. We denote by $\mathcal{I}$ their intersection.

Now, we prove that $\mathcal{I} \subset \mathbb{Z} + \ell\mathcal{O}_K$. Let $\lambda \in \mathcal{I}$. We know that λ defines an element in the endomorphism ring of E_{τ_1}, E_{τ_2} and E_{τ_3} if and only if the lattices

$$\mathbb{Z} + \mathbb{Z}\tau_1, \quad \mathbb{Z} + \mathbb{Z}\tau_2 \quad \text{and} \quad \mathbb{Z} + \mathbb{Z}\tau_3 \tag{3.3.9}$$

are stable under the multiplication by λ. In particular $\lambda = \lambda \cdot 1$ lies in all these lattices and in their intersection $\mathbb{Z}+\mathbb{Z}\tau$, hence $\lambda = x + y\tau$, for $x, y \in \mathbb{Z}$. Then, all the lattices in

(3.3.9) are stable also under the multiplication by $\mu := y\tau$ and consequently

$$\mu\tau_1 \in \mathbb{Z} + \mathbb{Z}\tau_1, \quad \mu\tau_2 \in \mathbb{Z} + \mathbb{Z}\tau_2, \quad \mu\tau_3 \in \mathbb{Z} + \mathbb{Z}\tau_3.$$

Then, using (3.3.7) and (3.3.8), we deduce that ay and by lie in $\mathbb{Z}$ and that the polynomial

$$p(t) := -yt^2 - yat + yb \in \mathbb{Z}[t]$$

has the property $p(r_1) \equiv p(r_2) \equiv p(r_3) \equiv 0 \bmod \ell$. Since r_1, r_2 and r_3 are pairwise distinct modulo ℓ, we deduce that y, ay and by are divisible by ℓ and consequently

$$\mu^2 = (y\tau)^2 = ay^2\tau + by^2 = ay\mu + by^2 \in ay\mathcal{O}_K + by\mathcal{O}_K \subset \ell\mathcal{O}_K.$$

If $y = 0$ or if the ideal $\ell\mathcal{O}_K$ is radical, we deduce that μ lies in $\ell\mathcal{O}_K$ and consequently $\lambda = x + \mu$ lies in $\mathbb{Z} + \ell\mathcal{O}_K$. If $y \neq 0$ and $\ell\mathcal{O}_K$ factors as $\mathfrak{l}^2$, for a prime ideal $\mathfrak{l} \mid \ell$, then the norm of μ is equal to by^2 which is a multiple of ℓ^2, hence μ lies in $\mathfrak{l}^2 = \ell\mathcal{O}_K$ and, as before, λ lies in $\mathbb{Z} + \ell\mathcal{O}_K$.

Let a_1, a_2, a_3 be positive integers such that $\mathrm{End}(E_{\tau_k}) = \mathbb{Z} + a_k\mathcal{O}_K$, for $k = 1, 2, 3$. Then $\mathbb{Z} + \mathrm{lcm}(a_1, a_2, a_3)\mathcal{O}_K = \mathcal{I} \subset \mathbb{Z} + \ell\mathcal{O}_K$. Hence $\ell \mid \mathrm{lcm}(a_1, a_2, a_3)$, i.e., we can suppose, up to renaming τ_1, τ_2, τ_3, that $\mathrm{End}(E_{\tau_1})$ is contained in $\mathbb{Z} + \ell\mathcal{O}_K$. Let $\beta_1 = \ell, \beta_2$ be endomorphisms of E_{τ_1} satisfying the properties of Lemma 3.3.5. We write $\mathcal{O}_K = \mathbb{Z}[\gamma]$, for a suitable γ, and $\beta_2 = z + w\gamma$. Since $\mathrm{End}(E_{\tau_1}) \subset \mathbb{Z} + \ell\mathcal{O}_K$, then w is multiple of ℓ and, since the norm of β_2 is ℓ^2, we deduce that z is multiple of ℓ as well. Hence $\beta_2 \in \ell\mathcal{O}_K$ and $\beta_2 = u\ell$ for some $u \in \mathcal{O}_K^\times$. Since $\beta_2 \neq \pm\beta_1 = \pm\ell$, we deduce that $\mathcal{O}_K$ has non-trivial units, hence either $K = \mathbb{Q}(i)$ or $K = \mathbb{Q}(\rho)$.

We suppose by contradiction that $K = \mathbb{Q}(\rho)$. Then we have that $u \in \{\pm\rho, \pm\rho^2\}$ and $\mathbb{Z}[\beta_2] = \mathbb{Z}[\ell\rho] \subset \mathrm{End}(E_{\tau_1})$. Since $\beta_2 \notin \ell\mathrm{End}(E_{\tau_1})^\times$ by property **P1** of Lemma 3.3.5, we deduce that $\mathrm{End}(E_{\tau_1}) \neq \mathbb{Z}[\rho]$, hence $\mathrm{End}(E_{\tau_1}) = \mathbb{Z}[\ell\rho]$. In particular $u^2\ell \in \mathrm{End}(E_{\tau_1})$ and the third condition in Lemma 3.3.5 is satisfied by (E, ϕ), (E_{τ_1}, ϕ_{r_1}), α, β_1, β_2 together with $\beta_3 := u^2\ell$. Hence the point (E_{τ_1}, ϕ_{r_1}) appears with multiplicity 3 in $T_\ell(E, \phi)$ which is impossible. Thus, $K = \mathbb{Q}(i)$ and $\beta_2 = \pm\ell i$. Hence $\mathrm{End}(E_{\tau_1})$ contains $\mathbb{Z}[\ell i]$ and, since there is an isogeny of degree ℓ between E and E_{τ_1}, then $\mathrm{End}(E)$ contains $\mathbb{Z}[\ell^2 i]$. □

The following proposition characterizes when $\phi^{-1}\circ\tau|_{E_\tau[n]}\circ\phi$ belongs to $\pm H$, for $\tau = \rho, i$, in terms of the multiplicities shown in the divisor $T_\ell(E_\tau, \phi)$.

Proposition 3.3.10. *Let n be a positive integer, let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ and let ℓ be a prime not dividing n.*

1. *Let $(E_\rho, \phi) \in Y_H(\mathbb{C})$. The matrix $\phi^{-1}\circ\rho|_{E_\rho[n]}\circ\phi$ lies in $\pm H$ if and only if the divisor $T_\ell(E_\rho, \phi)$ contains a point with multiplicity 3.*

2. *Let $(E_i, \phi) \in Y_H(\mathbb{C})$. If $\ell > 2$: The matrix $\phi^{-1} \circ i|_{E_i[n]} \circ \phi$ lies in $\pm H$ if and only if there are distinct points $P_1, \ldots, P_{\frac{\ell+3}{2}} \in Y_H(\mathbb{C})$ such that*

$$\begin{aligned} &T_\ell(E_i, \phi) = 2(P_1 + \ldots + P_{\frac{\ell+1}{2}}) \\ &\qquad \textit{or} \\ &T_\ell(E_i, \phi) = 2(P_1 + \ldots + P_{\frac{\ell-1}{2}}) + P_{\frac{\ell+1}{2}} + P_{\frac{\ell+3}{2}}. \end{aligned} \tag{3.3.11}$$

If $\ell = 2$: The matrix $\phi^{-1} \circ i|_{E_i[n]} \circ \phi$ lies in $\pm H$ if and only if there are two distinct points $P_1, P_2 \in Y_H(\mathbb{C})$ such that

$$T_2(E_i, \phi) = 2P_1 + P_2.$$

Proof. Part (1).

If $C \subset E_\rho[\ell]$ is a subgroup of order ℓ, then ρC and $\rho^2 C$ are subgroups of order ℓ as well and there are two unique isomorphisms u, v that make the following diagrams commutative:

$$\begin{array}{ccc} E_\rho & \xrightarrow{\rho} & E_\rho, \\ \downarrow{\scriptstyle \pi_C} & & \downarrow{\scriptstyle \pi_{\rho C}} \\ E_\rho/C & \xrightarrow{u} & E_\rho/\rho C, \end{array} \qquad \begin{array}{ccc} E_\rho & \xrightarrow{\rho^2} & E_\rho \\ \downarrow{\scriptstyle \pi_C} & & \downarrow{\scriptstyle \pi_{\rho^2 C}} \\ E_\rho/C & \xrightarrow{v} & E_\rho/\rho^2 C. \end{array}$$

We have that $\rho C = C$ if and only if ρ is an endomorphism of E_ρ/C, which is in turn equivalent to $\mathrm{Aut}(E_\rho/C) \neq \{\pm 1\}$ or $\mathrm{End}(E_\rho/C) = \mathbb{Z}[\rho]$ and, since the class number of $\mathbb{Z}[\rho]$ is equal to 1, this is equivalent to $E_\rho/C \cong E_\rho$. Hence, if $\rho C \neq C$, then $\mathrm{Aut}(E_\rho/C) = \{\pm 1\}$ and, using that π_C and $\pi_{\rho C}$ are bijections on the n-torsion subgroups, we have

$$\begin{aligned} (E_\rho/C, \pi_C \circ \phi) = (E_\rho/\rho C, \pi_{\rho C} \circ \phi) &\iff (\pi_{\rho C}|_{E_\rho[n]} \circ \phi)^{-1} \circ u|_{(E_\rho/C)[n]} \circ (\pi_C|_{E_\rho[n]} \circ \phi) \in \pm H \\ &\iff \phi^{-1} \circ \rho|_{E_\rho[n]} \circ \phi \in \pm H. \end{aligned} \tag{3.3.11.1}$$

Analogously, $\rho^2 C \neq C$ if and only if $\mathrm{Aut}(E_\rho/C) = \{\pm 1\}$ and when this happens

$$(E_\rho/C, \pi_C \circ \phi) = (E_\rho/\rho^2 C, \pi_{\rho^2 C} \circ \phi) \iff \phi^{-1} \circ \rho|_{E_\rho[n]} \circ \phi \in \pm H. \tag{3.3.12}$$

Since the endomorphism ρ does not act as a scalar on $E_\rho[\ell]$, there are at most two non-trivial subgroups of $E_\rho[\ell]$ that are ρ-stable. In particular we can take a non-trivial subgroup C_0 such that C_0, ρC_0 and $\rho^2 C_0$ are pairwise distinct.

If $\phi^{-1} \circ \rho|_{E_\rho[n]} \circ \phi$ lies in $\pm H$, then, by (3.3.11.1) and (3.3.12),

$$T_\ell(E_\rho, \phi) \geq (E_\rho/C_0, \pi_{C_0} \circ \phi) + (E_\rho/\rho C_0, \pi_{\rho C_0} \circ \phi) + (E_\rho/\rho^2 C_0, \pi_{\rho^2 C_0} \circ \phi) = 3(E_\rho/C_0, \pi_{C_0} \circ \phi).$$

Conversely, if $T_\ell(E_\rho, \phi)$ contains a point with multiplicity 3, there are three pairwise distinct subgroups $C_1, C_2, C_3 \subset E_\rho[\ell]$ of order ℓ such that

$$(E_\rho/C_1, \pi_{C_1}\circ\phi) = (E_\rho/C_2, \pi_{C_2}\circ\phi) = (E_\rho/C_3, \pi_{C_3}\circ\phi).$$

If one of the C_j is ρ-stable, then $E_\rho/C_1 \cong E_\rho/C_2 \cong E_\rho/C_3 \cong E_\rho$, and C_1, C_2, C_3 are all ρ-stable, contradicting that there are at most two non-trivial ρ-stable subgroups of $E_\rho[\ell]$. In particular $\mathbb{Z}[\rho] \supsetneq \mathrm{End}(E_\rho/C_1)$ and since E/C_1 is ℓ-isogenous to E_ρ we deduce that $\mathrm{End}(E_\rho/C_1) = \mathbb{Z}[\ell\rho]$. Hence, the only endomorphisms of E_ρ/C_1 having degree ℓ^2 are $\pm\ell, \pm\rho\ell, \pm\rho^2\ell$ and so there are at most three subgroups $C \subset E_\rho[\ell]$ of order ℓ such that E_ρ/C is isomorphic to E_ρ/C_1, namely: $C_1, \rho C_1$ and $\rho^2 C_1$. We deduce that, up to reordering, $C_2 = \rho C_1$ hence, by (3.3.11.1), $\phi^{-1}\circ\rho|_{E_\rho[n]}\circ\phi$ lies in $\pm H$.

Part (2).

If $C \subset E_i[\ell]$ is a subgroup of order ℓ, then iC is another subgroup of order ℓ and there is a unique isomorphism u that makes the following diagram commutative:

$$\begin{array}{ccc} E_i & \xrightarrow{\ i\ } & E_i \\ \downarrow{\scriptstyle \pi_C} & & \downarrow{\scriptstyle \pi_{iC}} \\ E_i/C & \xrightarrow{\ u\ } & E_i/iC. \end{array}$$

We have that $iC = C$ if and only if $\mathrm{End}(E_i/C) = \mathbb{Z}[i]$ if and only if $\mathrm{Aut}(E_i/C) \neq \{\pm 1\}$. Hence, if $iC \neq C$, then $\mathrm{Aut}(E_i/C) = \{\pm 1\}$ and, using that π_C and π_{iC} are bijections on the n-torsion subgroups, we have

(3.3.13)

$$\begin{aligned} (E_i/C, \pi_C\circ\phi) = (E_i/iC, \pi_{iC}\circ\phi) \quad &\iff \quad (\pi_{iC}\circ\phi)^{-1}\circ u|_{(E_i/C)[n]}\circ(\pi_C\circ\phi) \in \pm H \\ &\iff \quad \phi^{-1}\circ i|_{E_i[n]}\circ\phi \in \pm H. \end{aligned}$$

The endomorphism i does not act as multiplication by a scalar on $E_i[\ell]$. For each subgroup $C \subset E_i[\ell]$ of order ℓ, except at most two, we have $C \neq iC$. Hence, there are subgroups $C_1, \ldots, C_{\frac{\ell+3}{2}} \subset E_i$ of order ℓ such that $\{C_1, iC_1, \ldots, C_{\frac{\ell-1}{2}}, iC_{\frac{\ell-1}{2}}, C_{\frac{\ell+1}{2}}, C_{\frac{\ell+3}{2}}\}$ is the set of all the $\ell+1$ subgroups of order ℓ of E_i.

If $\phi^{-1}\circ i|_{E_i[n]}\circ\phi$ lies in $\pm H$, then, by (3.3.13), we have

$$T_\ell(E_i, \phi) = \sum_{k=1}^{\frac{\ell-1}{2}} 2(E_i/C_k, \pi_{C_k}\circ\phi) + (E_i/C_{\frac{\ell+1}{2}}, \pi_{C_{\frac{\ell+1}{2}}}\circ\phi) + (E_i/C_{\frac{\ell+3}{2}}, \pi_{C_{\frac{\ell+3}{2}}}\circ\phi),$$

and no point appears with multiplicity greater than 2 because of Proposition 3.3.6.

Now we assume that (3.3.11) holds. If $\ell = 3$, there are $C_1, C_2 \subset E_i$ subgroups of order 3 such that E_i/C_1 is not isomorphic to E_i/C_2 and C_1, iC_1, C_2, iC_2 are all the subgroups

of E_i of order 3. Hence Equation (3.3.11) implies that, up to renaming,

$$(E_i/C_1, \pi_{C_1} \circ \phi) = (E_i/iC_1, \pi_{iC_1} \circ \phi),$$

and by (3.3.13), we have that $\phi^{-1} \circ i|_{E_i[n]} \circ \phi$ lies in $\pm H$. The case $\ell = 2$ is similar to $\ell = 3$. We now suppose $\ell \geq 5$, so there are more repetitions in Equation (3.3.11). There are at most two possible subgroups C such that $iC = C$. Hence Equation (3.3.11) implies the existence of a subgroup $C_0 \subset E_i[\ell]$ such that $(E_i/C_0, \pi_{C_0} \circ \phi)$ has multiplicity 2 in $T_\ell(E_i, \phi)$ and $C_0 \neq iC_0$. It follows that E_i/C_0 is not isomorphic to E_i, thus $\mathrm{End}(E_i/C_0) = \mathbb{Z}[\ell i]$, and this implies that $\pm\ell$ and $\pm\ell i$ are the only elements of $\mathrm{End}(E_i/C_0)$ having degree ℓ^2. Hence, if C is a subgroup of $E_i[\ell]$ of order ℓ such that E_i/C is isomorphic to E_i/C_0, then $C \in \{C_0, iC_0\}$. Since $(E_i/C_0, \pi_{C_0} \circ \phi)$ has multiplicity 2, we have

$$(E_i/C_0, \pi_{C_0} \circ \phi) = (E_i/iC_0, \pi_{iC_0} \circ \phi),$$

and by (3.3.13), we have that $\phi^{-1} \circ i|_{E_i[n]} \circ \phi$ lies in $\pm H$. □

3.4 Cartan modular curves and their jacobians

We give the definition of Cartan modular curves following [93, Appendix A.5]. Let $n>1$ be an integer and let A be a free commutative étale $\mathbb{Z}/n\mathbb{Z}$-algebra of rank 2. For each prime $p \mid n$, we have that A/pA is isomorphic either to $\mathbb{F}_p \times \mathbb{F}_p$ or to $\mathbb{F}_{p^2}$: in the former case we say that A is *split* at p, in the latter we say that A is *non-split* at p. Moreover, for every assignment of each prime $p|n$ to split or non-split, there is a unique, up to isomorphism, algebra A which is split or non-split at every $p \mid n$ accordingly to the assignment.

We fix a $\mathbb{Z}/n\mathbb{Z}$-basis of A and, consequently, we identify the automorphism group of A, as $\mathbb{Z}/n\mathbb{Z}$-module, with $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. The group $A^\times$ of the units of A acts on A by multiplication, giving an embedding of $A^\times$ inside $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. A subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ which is the image of such an embedding is called a *Cartan subgroup*. The normalizer of $A^\times$ inside $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ contains all the matrices representing automorphisms of the ring A, hence $H := \langle A^\times, \mathrm{Aut}_{\mathrm{Ring}}(A)\rangle$ is a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ that contains $A^\times$ as normal subgroup. We call every such an H a *Cartan-plus subgroup* of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. The natural map $\mathrm{Aut}_{\mathrm{Ring}}(A) \to \prod_{p|n} \mathrm{Aut}_{\mathrm{Ring}}(A \otimes \mathbb{F}_p)$ is an isomorphism, hence $\mathrm{Aut}_{\mathrm{Ring}}(A)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{\omega(n)}$, where $\omega(n)$ is the number of prime divisors of n. In particular, given A, the Cartan subgroup has index $2^{\omega(n)}$ inside the Cartan-plus subgroup. Moreover, if n is odd, the Cartan-plus is equal to the normalizer of the Cartan subgroup inside $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. We call *Cartan modular curves* the modular curves associated to Cartan subgroups or to Cartan-plus subgroups of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$.

When $n = p^e$ is a prime power, we use the following notation:

- $X_{\mathrm{ns}}^{+}(p^e) := X_H$, if H is a Cartan-plus subgroup non-split at p;
- $X_{\mathrm{ns}}(p^e) := X_H$, if H is a Cartan subgroup non-split at p;
- $X_{\mathrm{s}}^{+}(p^e) := X_H$, if H is a Cartan-plus subgroup split at p;
- $X_{\mathrm{s}}(p^e) := X_H$, if H is a Cartan subgroup split at p.

Remark 3.4.1. If H_1 and H_2 are two conjugate subgroups of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, then the corresponding modular curves X_{H_1} and X_{H_2} are isomorphic. Moreover, given two Cartan or two Cartan-plus subgroups C_1 and C_2 of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ with the same assignment of each prime $p \mid n$ to split or non-split, then C_1 and C_2 are conjugate, so $X_{C_1} \cong X_{C_2}$. This implies that the above definitions are unambiguous.

We want to understand the structure, up to isogeny, of the jacobian of the Cartan modular curves. This is achieved using Chen's isogenies (see [25], [39],[26]). Let p be a prime and let e be a positive integer. We give an analogue of [26, Theorem 1.1] involving the jacobian of $X_{\mathrm{ns}}(p^e)$ for every p, and, to do this, we extend the analysis in [26] to the case $p = 2$. In order to state our result, we choose a non-square element $\xi \in (\mathbb{Z}/p^e\mathbb{Z})^\times$ when p is odd and define the following subgroups of $\mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z})$ for every prime p:

$$C_{\mathrm{s}}(p^e) := \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}, a, d \in (\mathbb{Z}/p^e\mathbb{Z})^\times \right\};$$

$$C_{\mathrm{s}}^{+}(p^e) := C_{\mathrm{s}} \cup \left\{ \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}, b, c \in (\mathbb{Z}/p^e\mathbb{Z})^\times \right\};$$

$$C_{\mathrm{ns}}(2^e) := \left\{ \begin{pmatrix} a & b \\ b & a+b \end{pmatrix}, a, b \in \mathbb{Z}/2^e\mathbb{Z}, (a,b) \not\equiv (0,0) \bmod 2 \right\};$$

$$C_{\mathrm{ns}}^{+}(2^e) := C_{\mathrm{ns}}(2^e) \cup \left\{ \begin{pmatrix} a & a-b \\ b & -a \end{pmatrix}, a, b \in \mathbb{Z}/2^e\mathbb{Z}, (a,b) \not\equiv (0,0) \bmod 2 \right\};$$

$$C_{\mathrm{ns}}(p^e) := \left\{ \begin{pmatrix} a & b\xi \\ b & a \end{pmatrix}, a, b \in \mathbb{Z}/p^e\mathbb{Z}, (a,b) \not\equiv (0,0) \bmod p \right\}, \quad \text{if } p \text{ is odd};$$

$$C_{\mathrm{ns}}^{+}(p^e) := C_{\mathrm{ns}}(p^e) \cup \left\{ \begin{pmatrix} a & b\xi \\ -b & -a \end{pmatrix}, a, b \in \mathbb{Z}/p^e\mathbb{Z}, (a,b) \not\equiv (0,0) \bmod p \right\}, \quad \text{if } p \text{ is odd};$$

$$B_r(p^e) := \left\{ \begin{pmatrix} a & bp^r \\ cp^{r+1} & d \end{pmatrix}, a, b, c, d \in \mathbb{Z}/p^e\mathbb{Z}, \quad ad \not\equiv 0 \bmod p \right\}, \text{ for } r = 0, 1, \ldots, e-1;$$

$$T_r(p^e) := \left\{ \begin{pmatrix} a & bp^r \\ cp^r & d \end{pmatrix}, a, b, c, d \in \mathbb{Z}/p^e\mathbb{Z}, ad - bcp^{2r} \in (\mathbb{Z}/p^e\mathbb{Z})^\times \right\}, \text{ for } r = 0, 1, \ldots, e.$$

We remark that $T_e(p^e) = C_{\mathrm{s}}(p^e)$ and that $C_{\mathrm{s}}(p^e), C_{\mathrm{ns}}(p^e)$ are respectively a split and a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z})$ and $C_{\mathrm{s}}^+(p^e), C_{\mathrm{ns}}^+(p^e)$ are the corresponding Cartan-plus subgroups.

Proposition 3.4.2. *Let p be a prime, let e be a positive integer and let $G = \mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z})$. We have the following isomorphism of $\mathbb{Q}$-representations of G:*

$$\mathbb{Q}[G/C_{\mathrm{ns}}(p^e)] \oplus \bigoplus_{r=0}^{e-1} 2\mathbb{Q}[G/B_r(p^e)] \cong \mathbb{Q}[G/C_{\mathrm{s}}(p^e)] \oplus \bigoplus_{r=0}^{e-1} 2\mathbb{Q}[G/T_r(p^e)]. \tag{3.4.3}$$

Proof. We follow the same strategy as in [26]. It is enough to prove that the representation on the right hand side has the same character as the representation on the left hand side. For every subgroup $H \subset G$, let χ_H be the character of the representation $\mathbb{Q}[G/H]$. If $p = 2$, the character χ_H for the groups appearing in the statement is computed in the Appendix of this article. If p is odd and H has the form B_r, T_r or C_{s}, the character χ_H is given in [26, Tables 3 and 4]; if p is odd and $H = C_{\mathrm{ns}}(p^e)$, then

$$\chi_H(g) = \begin{cases} (p-1)p^{2e-1}, & \text{if } g \text{ is a scalar matrix (type } I \text{ in [26, Tables 3, 4])}, \\ 2p^{2\mu}, & \text{if } g \text{ is a conjugate of } \left(\begin{smallmatrix} \alpha & \xi\beta p^\mu \\ \beta p^\mu & \alpha \end{smallmatrix}\right), \text{ with } \beta \in (\mathbb{Z}/p^e\mathbb{Z})^\times \\ & \text{and } 0 \le \mu < e-1 \text{ (types } RI'_\mu \text{ and } T' \text{ in [26, Tables 3, 4])}, \\ 0, & \text{otherwise.} \end{cases}$$

The characters of the representations in Equation (3.4.3) are sums of the previous characters. A straightforward computation proves the proposition. □

As explained in [39, Théorème 2 and the discussion below it], the representation theoretic result in Proposition 3.4.2, together with the isomorphisms of modular curves $X_{B_r(p^e)} \cong X_0(p^{2r+1})$ and $X_{T_r(p^e)} \cong X_{C_{\mathrm{s}}}(p^r) \cong X_0(p^{2r})$, implies the following proposition on jacobians of modular curves.

Proposition 3.4.4. *Let p be a prime, let e be a positive integer and let $J_{\mathrm{ns}}(p^e)$ be the jacobian of $X_{\mathrm{ns}}(p^e)$. We have the following isogenies over $\mathbb{Q}$:*

$$J_{\mathrm{ns}}(p^e) \times \prod_{r=0}^{e-1} J_0(p^{2r+1})^2 \sim J_0(p^{2e}) \times \prod_{r=0}^{e-1} J_0(p^{2r})^2, \qquad J_{\mathrm{ns}}(p^e) \sim \prod_{r=1}^{e} J_0^{\mathrm{new}}(p^{2r}).$$

For jacobians of Cartan curves of composite level we have the following theorem.

Theorem 3.4.5. *Let $n > 1$ be an integer and let $H < \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ be a Cartan or a Cartan-plus subgroup. Then the jacobian of X_H is a quotient of $J_0(n^2)$.*

Proof. Since all the Cartan-plus subgroups contain a Cartan subgroup, we can suppose that H is a Cartan subgroup. Let a, b be positive integers such that $n = ab$ and such that H is split at all primes dividing a and non-split at all the primes dividing b. If $b = 1$, then $X_H(n) \cong X_0(n^2)$. Thus, we suppose that $b > 1$. Let $b = p_1^{e_1} \cdots p_k^{e_k}$ be the prime factorization of b and for each $j = 1, \dots, k$, we set $G_j := \mathrm{GL}_2(\mathbb{Z}/p_j^{e_j}\mathbb{Z})$ and $H_j := C_{\mathrm{ns}}(p_j^{e_j}) < G_j$. Moreover we set $G := \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ and $G_{\mathrm{s}} := \mathrm{GL}_2(\mathbb{Z}/a\mathbb{Z})$, and we choose a totally split Cartan subgroup $H_{\mathrm{s}} < G_{\mathrm{s}}$. Chinese Remainder Theorem gives an identification between G and $G_{\mathrm{s}} \times \prod_{j=1}^k G_j$ sending H to a conjugate of $H_s \times \prod_{j=1}^k H_j$.

Instead of working with G-representations up to isomorphism, it is easier to work inside the representation ring of G, namely the Grothendieck ring of the category of finite-dimensional G-representations, where we can take differences of representations. By Proposition 3.4.2 we have the following equality in the representation ring of G_j over $\mathbb{Q}$:

$$\mathbb{Q}\big[G_j/H_j\big] = \mathbb{Q}\big[G_j/K_j(p_j^{2e_j})\big] + 2\sum_{i=0}^{2e_j-1}(-1)^i\mathbb{Q}\big[G_j/K_j(p_j^i)\big],$$

where $K_j(p_j^{2r}) := T_r(p_j^{e_j})$ for $r = 0, \dots, e_j$, and $K_j(p_j^{2r+1}) := B_r(p_j^{e_j})$ for $r = 0, \dots, e_j - 1$. Interpreting G_j-representations as G-representations via the reduction modulo $p_j^{e_j}$ map, the above equality also holds in the representation ring of G over $\mathbb{Q}$. We now get information about the representation $\mathbb{Q}[G/H]$ by taking the tensor product of the above identities, for $j = 1, \dots, k$, and using that, for all the groups $\mathcal{G}_1, \mathcal{G}_2$ and all the subgroups $\mathcal{H}_i < \mathcal{G}_i$, we have the isomorphisms of $(\mathcal{G}_1 \times \mathcal{G}_2)$-representations

$$\mathbb{Q}[\mathcal{G}_1/\mathcal{H}_1] \otimes \mathbb{Q}[\mathcal{G}_2/\mathcal{H}_2] \cong \mathbb{Q}[(\mathcal{G}_1 \times \mathcal{G}_2)/(\mathcal{H}_1 \times \mathcal{H}_2)].$$

Denoting by $\otimes$ the product in the representation ring of G over $\mathbb{Q}$, we have

$$\begin{aligned}
\mathbb{Q}\big[G/H\big] &= \mathbb{Q}\big[G_{\mathrm{s}}/H_s\big] \otimes \bigotimes_{j=1}^k \mathbb{Q}\big[G_j/H_j\big] \\
&= \mathbb{Q}\big[G_{\mathrm{s}}/H_s\big] \otimes \bigotimes_{j=1}^k \left(\mathbb{Q}\big[G_j/K_j(p_j^{2e_j})\big] + 2\sum_{i=0}^{2e_j-1}(-1)^i\mathbb{Q}\big[G_j/K_j(p_j^i)\big]\right) \\
&= \sum_{d \mid b^2} \varepsilon(d) m(d) \mathbb{Q}\big[G/K(d)\big],
\end{aligned} \tag{3.4.6}$$

where, for every $d = p_1^{f_1} \cdots p_k^{f_k}$ dividing b^2, we have

$$\varepsilon(d) := (-1)^{f_1 + \dots + f_k}, \quad m(d) := 2^{\#\{j : f_j \neq 2e_j\}}, \quad K(d) := H_s \times \prod_{j=1}^k K_j(p_j^{f_j}) < G.$$

As explained in [39], Equation (3.4.6) implies the following equality in the Grothendieck group of the category of abelian varieties over $\mathbb{Q}$ up to isogeny:

$$\mathrm{Jac}(X_H) \sim \prod_{d|b^2} \mathrm{Jac}(X_{K(d)})^{\varepsilon(d)m(d)}.$$

Denoting by $U(m)$ the Borel subgroup $\{\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)\} < \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, we notice that a $K_j(p_j^i)$-structure on an elliptic curve E is equivalent to a $U(p_j^i)$-structure on E and a H_s-structure is equivalent to a $U(a^2)$-structure. Therefore, a $K(d)$-structure on an elliptic curve E is equivalent to a $U(a^2d)$-structure on E. Hence the modular curve $X_{K(d)}$ is isomorphic to $X_0(a^2d)$ and consequently

$$\mathrm{Jac}(X_H) \sim \prod_{d|b^2} J_0(a^2d)^{\varepsilon(d)m(d)}.$$

Using $J_0(a^2d) \sim \prod_{m|a^2d} J_0^{\mathrm{new}}(m)^{\sigma_0\left(\frac{a^2d}{m}\right)}$, where $\sigma_0(n)$ is the number of divisors of n, one can compute that

$$\mathrm{Jac}(X_H) \sim \prod_{d|b^2} J_0(a^2d)^{\varepsilon(d)m(d)} \sim \prod_{\substack{c|a^2 \\ d|b}} J_0^{\mathrm{new}}(cd^2)^{\sigma_0\left(\frac{a^2}{c}\right)}. \tag{3.4.7}$$

Hence, in the Grothendieck group of the category of abelian varieties over $\mathbb{Q}$ up to isogeny, $\mathrm{Jac}(X_H)$ is equal to an abelian subvariety of $J_0(n^2)$. This proves the theorem. □

Remark 3.4.8. In [26], Chen deals with Cartan curves and Cartan subroups whose level is an odd prime power. Using the computations in our Appendix, Theorem 1.1 in [26] (and therefore all the results contained in the paper), can be extended to the cases of level 2^e, for e a positive integer. Notice that $C_{\mathrm{s}}^+(2^e)$ is different from the normalizer of $C_{\mathrm{s}}(2^e)$ and that, substituting $C_{\mathrm{s}}^+(p^e)$ with the normalizer of $C_{\mathrm{s}}(p^e)$, Theorem 1.1 in [26] wouldn't extend to the case of level 2^e.

Now we give a lower bound for the genus of Cartan modular curves: we show that for every $\varepsilon > 0$ the genus of a Cartan modular curve of level n big enough is larger than $n^{2-\varepsilon}$.

Proposition 3.4.9. *Let $n \geq 10^5$ be an integer and let $H < \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ be either a Cartan or a Cartan-plus subgroup. Denoting by $g(\Gamma_H)$ the genus of X_H we have*

$$g(\Gamma_H) > 0.01 \frac{n^{2-\frac{0.96}{\log\log n}}}{\log\log n}.$$

Proof. Since $\det(H) = (\mathbb{Z}/n\mathbb{Z})^\times$, then $X_H = \Gamma_H \backslash \overline{\mathbb{H}}$. Given a congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ containing $-\mathrm{Id}$, we denote by $d(\Gamma)$ the index $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$. Moreover, we denote

by $\varepsilon_\infty(\Gamma)$ the number of cusps of $\Gamma\backslash\overline{\mathbb{H}}$ and by $\varepsilon_2(\Gamma)$, respectively $\varepsilon_3(\Gamma)$, the number of elliptic points of period 2, respectively 3, of $\Gamma\backslash\overline{\mathbb{H}}$. Then, by [38, Theorem 3.1.1], the genus of $\Gamma\backslash\overline{\mathbb{H}}$ is

$$g(\Gamma) = 1 + \frac{d(\Gamma)}{12} - \frac{\varepsilon_2(\Gamma)}{4} - \frac{\varepsilon_3(\Gamma)}{3} - \frac{\varepsilon_\infty(\Gamma)}{2}. \tag{3.4.10}$$

The numbers $d(\Gamma), \varepsilon_\infty(\Gamma), \varepsilon_2(\Gamma)$ and $\varepsilon_3(\Gamma)$ are multiplicative with the following meaning: Given two coprime integers n_1, n_2 and two congruence subgroups $\Gamma_1, \Gamma_2 < \mathrm{SL}_2(\mathbb{Z})$ of level n_1 and n_2 respectively, both containing $-\mathrm{Id}$, then

$$\begin{aligned} &d(\Gamma_1 \cap \Gamma_2) = d(\Gamma_1)d(\Gamma_2), && \varepsilon_\infty(\Gamma_1 \cap \Gamma_2) = \varepsilon_\infty(\Gamma_1)\varepsilon_\infty(\Gamma_2), \\ &\varepsilon_2(\Gamma_1 \cap \Gamma_2) = \varepsilon_2(\Gamma_1)\varepsilon_2(\Gamma_2), && \varepsilon_3(\Gamma_1 \cap \Gamma_2) = \varepsilon_3(\Gamma_1)\varepsilon_3(\Gamma_2). \end{aligned} \tag{3.4.11}$$

Let $n = p_1^{e_1} \cdots p_k^{e_k}$ the prime factorization of n and we denote by H_j the reduction of H modulo $p_j^{e_j}$. Then each H_j is either a Cartan or a Cartan-plus subgroup and, under the isomorphism $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \cong \prod_{j=1}^k \mathrm{GL}_2(\mathbb{Z}/p_j^{e_j}\mathbb{Z})$, we have $H \cong \prod_{j=1}^k H_j$ and therefore $\Gamma_H = \bigcap_{j=1}^k \Gamma_{H_j}$. Last equation, together with the multiplicativity and (3.4.10), implies that we can estimate the genus of X_H estimating the quantities $d(\Gamma_H), \varepsilon_\infty(\Gamma_H), \varepsilon_2(\Gamma_H)$ and $\varepsilon_3(\Gamma_H)$ for $n = p^e$. We write these values in Table 3.1 (see [38] and [36] for the split case and [11] for the non-split case).

Table 3.1: Degree, elliptic points and cusps for prime power levels.

H	$d(\Gamma_H)$	$\varepsilon_2(\Gamma_H)$	$\varepsilon_3(\Gamma_H)$	$\varepsilon_\infty(\Gamma_H)$
$C_{\mathrm{s}}(p^e)$	$p^{2e-1}(p+1)$	2 if $p \equiv 1\,(4)$ 0 if $p \not\equiv 1\,(4)$	2 if $p \equiv 1\,(3)$ 0 if $p \not\equiv 1\,(3)$	$p^{e-1}(p+1)$
$C_{\mathrm{s}}^+(p^e)$	$\frac{p^{2e-1}(p+1)}{2}$	2^{e-1} if $p = 2$ $1+\frac{p^{e-1}(p-1)}{2}$ if $p \equiv 1\,(4)$ $\frac{p^{e-1}(p+1)}{2}$ if $p \equiv 3\,(4)$	1 if $p \equiv 1\,(3)$ 0 if $p \not\equiv 1\,(3)$	2 if $p^e = 2$ $\frac{p^{e-1}(p+1)}{2}$
$C_{\mathrm{ns}}(p^e)$	$p^{2e-1}(p-1)$	0 if $p \not\equiv 3\,(4)$ 2 if $p \equiv 3\,(4)$	0 if $p \not\equiv 2\,(3)$ 2 if $p \equiv 2\,(3)$	$p^{e-1}(p-1)$
$C_{\mathrm{ns}}^+(p^e)$	$\frac{p^{2e-1}(p-1)}{2}$	2^{e-1} if $p = 2$ $\frac{p^{e-1}(p-1)}{2}$ if $p \equiv 1\,(4)$ $1+\frac{p^{e-1}(p+1)}{2}$ if $p \equiv 3\,(4)$	0 if $p \not\equiv 2\,(3)$ 1 if $p \equiv 2\,(3)$	1 if $p^e = 2$ $\frac{p^{e-1}(p-1)}{2}$

The table implies that for every prime p_j dividing n with exponent e_j we have

$$d(\Gamma_{H_j}) \geq \tfrac{1}{2}p_j^{2e_j}(1-\tfrac{1}{p_j}), \quad \varepsilon_2(\Gamma_{H_j}) \leq p_j^{e_j}, \quad \varepsilon_3(\Gamma_{H_j}) \leq 2, \quad \varepsilon_\infty(\Gamma_{H_j}) \leq p_j^{e_j}(1+\tfrac{1}{p_j}).$$

These inequalities and the multiplicativity (3.4.11) imply the following estimates for $n \geq 15$:

$$d(\Gamma_H) \geq \frac{n\phi(n)}{2^{\omega(n)}} > \frac{n^2}{4.4\,\log\log(n)2^{\omega(n)}} \geq \frac{n^2}{4.4\,\log\log(n)2^{1.3841\frac{\log n}{\log\log n}}} > \frac{n^{2-\frac{0.96}{\log\log n}}}{4.4\,\log\log n},$$

$$\varepsilon_2(\Gamma_H) \leq n, \quad \varepsilon_3(\Gamma_H) \leq 2^{\omega(n)} \leq n, \quad \varepsilon_\infty(\Gamma_H) \leq n\prod_{j=1}^{k}(1+\tfrac{1}{p_j}) \leq \sigma_1(n) \leq 2.59n\log\log n,$$

where $\phi(n)$ is Euler's totient function which is estimated using [89, Theorem 15], $\omega(n)=k$ is the number of prime divisors of n which is estimated as in [87, Théorème 11], and $\sigma_1(n)$ is the sum of positive divisors of n which is estimated as in [55, Theorem 1]. For $n \geq 10^5$, substituting in (3.4.10), we get

$$g(\Gamma_H) > 1 + \frac{n^{2-\frac{0.96}{\log\log n}}}{52.8\,\log\log n} - \frac{n}{3} - \frac{n}{4} - 1.3n\log\log n \geq 0.01\frac{n^{2-\frac{0.96}{\log\log n}}}{\log\log n}.$$

□

3.5 Field of definition of automorphisms

In this section we prove that, when the level is large enough, every automorphism of the modular curve X_H associated to a subgroup H of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ is defined over the compositum of some quadratic fields, and in some cases we find explicitly this field.

Whenever K is a field, X is a variety over K, and F is an extension of K, we write $\mathrm{Aut}_F(X)$ for the set of automorphisms of X defined over F; analogously we use the notations $\mathrm{End}_F(X)$ and $\mathrm{Hom}_F(X,Y)$ for X and Y being abelian varieties over K. Whenever we omit the dependency on the field, we mean automorphisms (or endomorphisms) defined over the algebraic closure of K; in particular when X is a modular curve the "group of the automorphisms of X" is $\mathrm{Aut}_{\overline{\mathbb{Q}}}(X)$ or equivalently $\mathrm{Aut}_{\mathbb{C}}(X)$. We start with a straightforward generalization of [60, Lemma 1.4].

Lemma 3.5.1. *Let K be a perfect field with algebraic closure $\overline{K}$, let X be a smooth projective and geometrically connected curve defined over K of genus $g(X)$ and let $\mathrm{Jac}(X)$ be its jacobian variety. We suppose that there are two abelian varieties A_1 and A_2 over K such that $\mathrm{Hom}_{\overline{K}}(A_1,A_2)=0$ and such that $\mathrm{Jac}(X)$ is isogenous to $A_1\times_K A_2$. If*

$$g(X) > 2\dim(A_2)+1,$$

and if $F \subset \overline{K}$ is an extension of K such that $\mathrm{End}_{\overline{K}}(A_1) = \mathrm{End}_F(A_1)$, then every automorphism of X over $\overline{K}$ can be defined over F.

Proof. We fix isogenies $\varphi\colon \mathrm{Jac}(X) \to A_1 \times_K A_2$ and $\tilde{\varphi}\colon A_1 \times_K A_2 \to \mathrm{Jac}(X)$ whose compositions are multiplications by an integer. Let $u \in \mathrm{Aut}_{\overline{K}}(X)$ and $\sigma \in \mathrm{Gal}(\overline{K}/F)$ and consider the automorphism $v := u^\sigma \circ u^{-1}$. Let Y be the quotient of X by the subgroup of automorphisms generated by v (which is finite since $g(X) \geq 2$) and let $\mathrm{Jac}(Y)$ be the jacobian of Y. Using φ and the equality $\mathrm{Hom}_{\overline{K}}(A_1, A_2) = 0$, we can identify $u_*, u_*^\sigma \in \mathrm{Aut}_{\overline{K}}(\mathrm{Jac}(X))$ respectively with

$$(u_1, u_2), (u_1^\sigma, u_2^\sigma) \in \left(\mathrm{End}_{\overline{K}}(A_1 \times_K A_2) \otimes \mathbb{Q}\right)^\times \cong \left(\mathrm{End}_{\overline{K}}(A_1) \otimes \mathbb{Q}\right)^\times \times \left(\mathrm{End}_{\overline{K}}(A_2) \otimes \mathbb{Q}\right)^\times.$$

Since $\mathrm{End}_{\overline{K}}(A_1) = \mathrm{End}_F(A_1)$, then $u_1 = u_1^\sigma$, and $v_* = (\mathrm{id}, v_2)$. This implies that there is a morphism of abelian varieties $A_1 \to \mathrm{Jac}(Y)$ with finite kernel, namely the composition of the natural inclusion $A_1 \to A_1 \times_K A_2$, the isogeny $\tilde{\varphi}$ and the map $\mathrm{Jac}(X) \to \mathrm{Jac}(Y)$. In particular, denoting by $g(Y)$ the genus of Y, we have

$$g(X) - \dim(A_2) = \dim(A_1) \leq g(Y).$$

Hence, by the Riemann-Hurwitz formula applied to the projection $X \to Y$, we have

$$\dim(A_1) + \dim(A_2) - 1 \geq d(g(Y) - 1) \geq d\dim(A_1) - d,$$

where d is the order of v. If $d > 1$, we get $\dim(A_1) \leq \dim(A_2) + 1$, which is impossible by hypothesis. Hence $d = 1$ and v is the identity. This implies that $u^\sigma = u$, for every $\sigma \in \mathrm{Gal}(\overline{K}/F)$, i.e., since K is perfect, $u \in \mathrm{Aut}_F(X)$. □

Every abelian variety A over a number field K, is isogenous over $\mathbb{C}$ to a product of geometrically simple abelian varieties. We denote by A^{C} the CM part of A that is the product, with multiplicities, of the simple abelian varieties in the decomposition of A with complex multiplication and we denote by A^{N} the non-CM part of A defined analogously. The CM part and the non-CM part of A are unique only up to isogeny and are defined over K. We want to apply Lemma 3.5.1 to the case $A_1 = \mathrm{Jac}(X)^{\mathrm{N}}$ and $A_2 = \mathrm{Jac}(X)^{\mathrm{C}}$. Hence, we are interested in an upper bound on the dimension of the CM part of the jacobian of Cartan modular curves. By Theorem 3.4.5, it is enough to know an upper bound in the case $X = X_0(n)$.

Proposition 3.5.2. *For every integer $n > 1$, the dimension $g_0^{\mathrm{C}}(n)$ of the CM part of $J_0(n)$ satisfies*

$$g_0^{\mathrm{C}}(n) \leq 9\log(n)^2 n^{\frac{1}{2} + \frac{2.816}{\log\log n}}.$$

Proof. For every positive integer k, let $J_0^{\mathrm{new}}(k)$ be the new part of $J_0(k)$ and let $\sigma_0(k)$ be the number of positive divisors of k. Then we have a canonical isogeny

$$J_0(n) \sim \prod_{d|n} J_0^{\mathrm{new}}(d)^{\sigma_0(n/d)}.$$

Denoting by $g_0^{\mathrm{new,C}}(d)$ the dimension of the CM part of $J_0^{\mathrm{new}}(d)$, we also have

$$g_0^{\mathrm{C}}(n) = \sum_{d|n} \sigma_0(n/d) g_0^{\mathrm{new,C}}(d). \tag{3.5.3}$$

We know that $J_0^{\mathrm{new}}(d)$ is isogenous over $\mathbb{Q}$ to $\prod_{[f]} A_f$, where $[f]$ is the Galois orbit of the newform f (see [38, Chapter 6]). By [95, Proposition 1.6], A_f has non-trivial CM part if and only if A_f is isogenous over $\mathbb{C}$ to the product of finitely many copies of an elliptic curve with CM by an imaginary quadratic field K, which is in turn equivalent to the existence of an ideal $\mathfrak{m}$ of $\mathcal{O}_K$ and a primitive Grössencharacter λ of K defined modulo $\mathfrak{m}$ such that $f = f_\lambda$ (see [96, Section 4] for the definition of Grössencharacter and the definition of the modular form associated to a Grössencharacter), the nebentypus ε_λ is trivial (see [96, Lemma 3]) and $d = |\Delta_K||\mathfrak{m}|$, where Δ_K is the discriminant of K and $|\mathfrak{m}|$ is the norm of the ideal $\mathfrak{m}$. This implies that $g_0^{\mathrm{new,C}}(d)$ is equal to the number of such triples $(K, \mathfrak{m}, \lambda)$. For every choice of K and $\mathfrak{m}$, the set of primitive Grössencharacters of K defined modulo $\mathfrak{m}$ is a subset of the set of Grössencharacters of K defined modulo $\mathfrak{m}$. If this set is not empty, then there is at least one Grössencharacter λ_0 and all other Grössencharacters are given by $\lambda_0\chi$, for χ a character of the group

$$\widetilde{\mathrm{Cl}}_{\mathfrak{m}}(K) := \frac{\{\text{fractional ideals of } \mathcal{O}_K \text{ coprime to } \mathfrak{m}\}}{\{(\alpha) : \exists a \in \mathbb{Z} \text{ coprime to } \mathfrak{m} \text{ such that } \alpha \equiv a \bmod \mathfrak{m}\}}.$$

Thus, for given K and $\mathfrak{m}$, the cardinality of $\widetilde{\mathrm{Cl}}_{\mathfrak{m}}(K)$ is larger than the number of triples $(K, \mathfrak{m}, \lambda)$ we are interested in, hence

$$g_0^{\mathrm{new,C}}(d) \leq \sum_{|\Delta_K||\mathfrak{m}|=d} \#\widetilde{\mathrm{Cl}}_{\mathfrak{m}}(K)\,. \tag{3.5.4}$$

To give a bound on $\widetilde{\mathrm{Cl}}_{\mathfrak{m}}(K)$ we look at the following short exact sequence

$$1 \longrightarrow \frac{(\mathcal{O}_K/\mathfrak{m})^\times}{\mathcal{O}_K^\times \cdot (\mathbb{Z}/(\mathbb{Z}\cap\mathfrak{m}))^\times} \longrightarrow \widetilde{\mathrm{Cl}}_{\mathfrak{m}}(K) \longrightarrow \mathrm{Cl}(K) \longrightarrow 0,$$

where $\mathrm{Cl}(K)$ is the class group of K and we write $\mathcal{O}_K^\times$ and $(\mathbb{Z}/(\mathbb{Z}\cap\mathfrak{m}))^\times$ in place of their natural image inside $(\mathcal{O}_K/\mathfrak{m})^\times$. We write $\mathfrak{m} = \prod_p \mathfrak{m}_p$ for p varying in the set of rational primes and $\mathfrak{m}_p$ being a product of primes of $\mathcal{O}_K$ dividing p. Thus the above short exact

sequence gives

$$\#\widetilde{\mathrm{Cl}}_{\mathfrak{m}}(K) \leq \#\mathrm{Cl}(K)\cdot\#\left(\frac{(\mathcal{O}_K/\mathfrak{m})^\times}{(\mathbb{Z}/(\mathbb{Z}\cap\mathfrak{m}))^\times}\right) = \#\mathrm{Cl}(K)\prod_{p\,|\,|\mathfrak{m}|}\#\left(\frac{(\mathcal{O}_K/\mathfrak{m}_p)^\times}{(\mathbb{Z}/(\mathbb{Z}\cap\mathfrak{m}_p))^\times}\right) \leq$$
$$\leq 3\log(|\Delta_K|)\sqrt{|\Delta_K|}\prod_{p\,|\,|\mathfrak{m}|}\left((1+\tfrac{1}{p})|\mathfrak{m}_p|^{1/2}\right) = 3\log(|\Delta_K|)\sqrt{|\Delta_K||\mathfrak{m}|}\prod_{p\,|\,|\mathfrak{m}|}(1+\tfrac{1}{p}),$$

where the class number of K is estimated using [81, Theorem 8.10 and Lemma 8.16] and the bound on the cardinality of $(\mathcal{O}_K/\mathfrak{m}_p)^\times/(\mathbb{Z}/(\mathbb{Z}\cap\mathfrak{m}_p))^\times$ is trivial after factoring $\mathfrak{m}_p$. Substituting in (3.5.4), we have

$$g_0^{\mathrm{new,C}}(d) \leq \sum_{|\Delta_K||\mathfrak{m}|=d}\left(3\sqrt{d}\log(|\Delta_K|)\prod_{p|\,|\mathfrak{m}|}(1+\tfrac{1}{p})\right).$$

Let $M_d := \#\Big\{(K,\mathfrak{m}) : |\Delta_K||\mathfrak{m}| = d\Big\}$ and for $m \in \mathbb{Z}_{\geq 1}$, we denote by $\sigma_1(m)$ the sum of the positive divisors of m. We have $\sigma_1(m) < 3m\log m$, for each $m \geq 2$ (see [55, Theorem 1] if $m \geq 7$, it is trivial in the remaining cases). Then

$$g_0^{\mathrm{new,C}}(d) \leq 3M_d\sqrt{d}\log(d)\prod_{p|d}(1+\tfrac{1}{p}) \leq 3M_d\sqrt{d}\log(d)\tfrac{\sigma_1(d)}{d} \leq 9M_d\sqrt{d}\log(d)^2.$$

Substituting in (3.5.3), we get

$$\begin{aligned} g_0^{\mathrm{C}}(n) &\leq 9\sum_{d|n}\sigma_0(n/d)M_d\sqrt{d}\log(d)^2 \leq 9\sqrt{n}\log(n)^2\sum_{d|n}M_d\sigma_0(n/d) \leq \\ &\leq 9\sqrt{n}\log(n)^2\#\Big\{(K,\mathfrak{m},d) : |\Delta_K||\mathfrak{m}|d \text{ divides } n\Big\}. \end{aligned} \tag{3.5.5}$$

Writing the prime factorization $n = \prod_{i=1}^r p_i^{e_i}$, we know that an imaginary quadratic field K with discriminant dividing n must be $K = \mathbb{Q}(\sqrt{-\prod_{i=1}^r p_i^{\varepsilon_i}})$, with $\varepsilon \in \{0,1\}^r$. Hence

$$\#\Big\{(K,\mathfrak{m},d) : |\Delta_K||\mathfrak{m}|d \text{ divides } n\Big\} \leq \sum_{\varepsilon\in\{0,1\}^r}\#\Big\{(\mathfrak{m},d) : |\Delta_K||\mathfrak{m}|d \text{ divides } n\Big\} \leq$$
$$\leq \sum_{\substack{\varepsilon\in\{0,1\}^r\\ m\in\mathbb{Z}_{>0}}}\#\Big\{\mathfrak{m}\subset\mathcal{O}_K : |\mathfrak{m}| = m\Big\}\cdot\#\Big\{d\in\mathbb{Z}_{>0} : dm\prod_{i=1}^r p_i^{\varepsilon_i} \text{ divides } n\Big\}.$$

We have the factorizations $m = \prod_{i=1}^r p_i^{f_i}$ and $d = \prod_{i=1}^r p_i^{c_i}$, where $f_i, c_i \in \{0,1,\ldots,e_i\}$, for $i = 1,\ldots,r$, and we denote by f the r-tuple whose components are the f_i's and similarly we define c. Then the number of ideals $\mathfrak{m}$ in $\mathcal{O}_K$ having norm m is less than $\prod_{i=1}^r(f_i+1)$ which is equal to the number of pairs (a,b) of elements of $\mathbb{Z}_{\geq 0}^r$ such that

$a+b=f$. Hence we get

$$\#\Big\{(K,\mathfrak{m},d):|\Delta_K||\mathfrak{m}|d \text{ divides } n\Big\}\leq\#\Big\{(\varepsilon,a,b,c)\in\{0,1\}^r\times(\mathbb{Z}^r_{\geq 0})^3\colon \varepsilon_i+a_i+b_i+c_i\leq e_i\Big\}\leq$$
$$\leq\prod_{i=1}^r\Big(\#\Big\{(a_i,b_i,c_i)\in\mathbb{Z}^3_{\geq 0}: a_i+b_i+c_i\leq e_i\Big\}+\#\Big\{(a_i,b_i,c_i)\in\mathbb{Z}^3_{\geq 0}: a_i+b_i+c_i\leq e_i-1\Big\}\Big)\leq$$
$$\leq\prod_{i=1}^r\Big(\binom{e_i+3}{3}+\binom{e_i+2}{3}\Big)\leq\prod_{i=1}^r\frac{(e_i+2)(e_i+1)^2}{2}.$$

Notice that $\sigma_0(n)=\prod_{i=1}^r(e_i+1)$ is the number of positive divisors of n and that the product $\prod_{i=1}^r\frac{(e_i+2)(e_i+1)}{2}$ is the number of triples (d_1,d_2,d_3) of positive integers such that $d_1d_2d_3=n$. Using the upper bounds, contained in [82] and [88], for these two quantities, we get

$$\#\Big\{(K,\mathfrak{m},d):|\Delta_K||\mathfrak{m}|d \text{ divides } n\Big\}\leq n^{\frac{1.538\log 2}{\log\log n}}n^{\frac{1.592\log 3}{\log\log n}}\leq n^{\frac{2.816}{\log\log n}}.$$

Substituting in (3.5.5) we find

$$g_0^{\mathrm{C}}(n)\leq 9\sqrt{n}\log(n)^2n^{\frac{2.816}{\log\log n}}=9\log(n)^2n^{\frac{1}{2}+\frac{2.816}{\log\log n}}.$$

□

When the level is a prime power, the previous upper bound is easier and smaller.

Proposition 3.5.6. *For every prime p and positive integer e, the dimension $g_0^{\mathrm{C}}(p^e)$ of the CM part of $J_0(p^e)$ satisfies*

$$g_0^{\mathrm{C}}(p^e)\leq\begin{cases}13\sqrt{2^e} & \text{if } p=2,\\ 0 & \text{if } p\equiv 1 \bmod 4,\\ 5.5\sqrt{p^e}\log p & \text{if } p\equiv 3 \bmod 4.\end{cases}$$

The proof follows the same steps of the previous proposition and is simplified by the fact that there are few quadratic imaginary fields K whose discriminant divides p^e. More precisely: there are two fields when $p=2$, there are no fields if $p\equiv 1 \bmod 4$ and there is only one field if $p\equiv 3 \bmod 4$. We now give an upper bound for the field of definition of the automorphisms of a Cartan modular curve of large enough level.

Proposition 3.5.7. *Let $n\geq 10^{400}$ be an integer and let $H<\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ be either a Cartan or a Cartan-plus subgroup. Then every automorphism of X_H is defined over the compositum of all the quadratic fields whose discriminant divides n.*

Proof. Let J_H be the jacobian of X_H and let J_H^{C} and J_H^{N} be the CM part and the non-CM part of J_H respectively. By Lemma 3.5.1, it is enough to prove that $2\dim(J_H^{\mathrm{C}})+1$ is smaller than the genus of X_H and that every endomorphism of J_H^{N} is defined over the compositum of all the quadratic fields whose discriminant divides n. The latter is true because, by Theorem 3.4.5, J_H^{N} is a quotient of $J_0(n^2)^{\mathrm{N}}$ and by [60, Proposition 1.3] every endomorphism of $J_0(n^2)^{\mathrm{N}}$ is defined over the compositum of all the quadratic fields whose discriminant divides n. By Theorem 3.4.5 J_H^{C} is a quotient of $J_0(n^2)^{\mathrm{C}}$ hence we can use Proposition 3.5.2 to bound the $\dim(J_H^{\mathrm{C}})$; this, together with the bound for the genus $g(X_H)$ of X_H given in Proposition 3.4.9, implies the inequality we need when $n \geq 10^{400}$:

$$2\dim(J_H^{\mathrm{C}}) + 1 \leq 2\dim(J_0(n^2)^{\mathrm{C}}) + 1 \leq 73\log(n)^2 n^{1+\frac{5.632}{\log\log n}} < \frac{n^{2-\frac{0.96}{\log\log n}}}{100\log\log n} < g(X_H).$$

□

Proposition 3.5.7 can be made sharper when n is a prime power.

Proposition 3.5.8. *Let p be a prime and e a positive integer and let X be a curve associated to a Cartan or a Cartan-plus subgroup of level p^e. If the genus of X is at least 2, then every automorphism of X is defined over the field*

$$K_p = \begin{cases} \mathbb{Q}(i, \sqrt{2}), & \text{if } p = 2, \\ \mathbb{Q}\left(\sqrt{p}\right), & \text{if } p \equiv 1 \bmod 4, \\ \mathbb{Q}\left(\sqrt{-p}\right), & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

A strategy of proof is the same of Proposition 3.5.7:

(I) give an upper bound for $\dim(\mathrm{Jac}(X)^{\mathrm{C}})$;

(II) give a lower bound for the genus;

(III) apply [60, Proposition 1.3] and Theorem 3.4.5 to deduce that the endomorphisms of $\mathrm{Jac}(X)^{\mathrm{N}}$ are defined over K_p;

(IV) apply Lemma 3.5.1.

In particular in the case of $X_{\mathrm{ns}}(p^e)$ and $X_{\mathrm{ns}}^+(p^e)$, when $p^e > 600$, the propositions 3.4.4 and 3.5.6 and Table 3.1 give bounds in ((I)) and ((II)) that are sharp enough for ((IV)). If $p^e \leq 600$, the bounds in Proposition 3.5.6 are sometimes not sharp enough. In these cases we can compute explicitly the CM part and notice that only a factor of it of low dimension has endomorphisms defined over a field bigger than K_p: whenever a CM factor

is a rational elliptic curve, we know by CM theory that its endomorphisms are defined over K_p and it can be discarded from the count. This is done in the MAGMA script available at [70]. The case $X_{\mathrm{s}}(p^e) \cong X_0(p^{2e})$ follows from [60, Corollary 1.14] and the case $X_{\mathrm{s}}^+(p^e) \cong X_0(p^{2e})$ follows from the following proposition.

Proposition 3.5.9. *Let p be a prime and e a positive integer. If the genus of $X_0^*(p^e)$ is at least 2, then every automorphism of $X_0^*(p^e)$ is defined over the field*

$$K_p = \begin{cases} \mathbb{Q}(i, \sqrt{2}), & \text{if } p = 2, \\ \mathbb{Q}\left(\sqrt{p}\right), & \text{if } p \equiv 1 \bmod 4, \\ \mathbb{Q}\left(\sqrt{-p}\right), & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

Again, one can apply the same strategy used for Propositions 3.5.7 and 3.5.8, together with the MAGMA script available at [70]. In particular we need a lower bound for the genus of $X_0^*(p^e)$. Since we do not know an explicit reference giving a formula for this genus, we write it in the following remark.

Remark 3.5.10. Given a positive integer n, let $X_0^+(n)$ be the quotient of $X_0(n)$ by the n-th Atkin-Lehner operator. This curve is equal to $X_0^*(n)$ when n is the power of a prime.

In [84, Equation 9] there is a formula for the genus $g_0^+(n)$ of $X_0^+(n)$ when n is prime. When $n = p^{2e}$ with p prime, we can compute $g_0^+(n)$ using Table 3.1 since $X_0^+(n)$ is isomorphic to a split Cartan curve. For general n, [84, Equation 9] can be easily generalized applying Riemann-Hurwitz formula to the natural map $X_0(n) \to X_0^+(n)$ and counting the number of fixed points of the n-th Atkin-Lehner operator. This gives

$$g_0^+(n) = \begin{cases} 0, & \text{if } n \in \{1, 2, 3, 4\}, \\ \frac{1+g_0(n)}{2} - \frac{h(-n)+h(-4n)}{4}, & \text{if } n \geq 5 \text{ is odd}, \\ \frac{1+g_0(n)}{2} - \frac{h(-4n)}{4}, & \text{if } n \geq 5 \text{ is even}, \end{cases}$$

where $g_0(n)$ is the genus of $X_0(n)$ and $h(D)$ is the class number of the quadratic order with discriminant D, with the convention $h(D) = 0$ if D is a square or if $D \equiv 2, 3 \bmod 4$.

Remark 3.5.11. We are not always able to prove that every automorphism of a Cartan modular curve is defined over a compositum of quadratic fields. For example, an analogue of Section 3.4.7 for Cartan-plus curves, proved using Chen's isogeny in [26], implies that the jacobian of the totally non-split Cartan-plus curve X of level 48 contains $J_0^{\mathrm{new},*}(48^2)$. Since there are two CM (weight 2) newforms of level 48^2 of degree 2 and invariant under the action of both the Atkin-Lehner operators w_9 and w_{256}, then the jacobian $J_0^{\mathrm{new},*}(48^2)$ has a CM part of dimension at least 4 whose endomorphisms could be defined over a field bigger than the compositum of quadratic fields. This prevents us from applying Lemma 3.5.1 in ((IV)) of the strategy above, because the genus of X is 9 (see Table 3.1).

3.6 Automorphisms

In this section we treat our main problem, namely to determine the automorphisms of certain modular curves X_H over $\mathbb{C}$ for a subgroup H of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. We restrict our attention to X_H geometrically connected, i.e., $\det(H) = (\mathbb{Z}/n\mathbb{Z})^\times$. Every automorphism we are interested in induces an automorphism of the Riemann surface $X_H(\mathbb{C}) = \Gamma_H\backslash\overline{\mathbb{H}}$ and, since it is compact, each of these automorphisms comes from an automorphism of the algebraic curve $(X_H)_{\mathbb{C}}$. Let $\mathbb{P}\colon \mathrm{GL}_2^+(\mathbb{Q}) \to \mathrm{PGL}_2^+(\mathbb{Q})$ be the natural map. Each matrix $m \in \mathrm{PGL}_2^+(\mathbb{Q})$ defines a Möbius transformation $m\colon \overline{\mathbb{H}} \to \overline{\mathbb{H}}$ and such an automorphism of the Riemann surface $\overline{\mathbb{H}}$ pushes down to an automorphism of $\Gamma_H\backslash\overline{\mathbb{H}}$ if and only if m normalizes $\mathbb{P}(\Gamma_H)$.

Definition 3.6.1. Let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ such that $\det(H) = (\mathbb{Z}/n\mathbb{Z})^\times$. An automorphism of X_H defined over $\mathbb{C}$ is *modular* if its action on $X_H(\mathbb{C}) = \Gamma_H\backslash\overline{\mathbb{H}}$ is described by a Möbius transformation associated to a matrix $m \in \mathrm{PGL}_2^+(\mathbb{Q})$ normalizing $\mathbb{P}(\Gamma_H)$.

When H has surjective determinant, $\mathrm{Aut}(X_H)$ contains the subgroup of modular automorphisms which is isomorphic to $\mathcal{N}/\mathbb{P}(\Gamma_H)$, where $\mathcal{N}$ is the normalizer of $\mathbb{P}(\Gamma_H)$ inside $\mathrm{PGL}_2^+(\mathbb{Q})$.

Remark 3.6.2. Notice that we can define modular automorphisms of Y_H looking at $\mathrm{PGL}_2^+(\mathbb{R})$, instead of $\mathrm{PGL}_2^+(\mathbb{Q})$, as follows: an automorphism ι of $Y_H(\mathbb{C}) = \Gamma_H\backslash\mathbb{H}$ is *modular* if there is a matrix $m \in \mathrm{PGL}_2^+(\mathbb{R})$ that normalizes the image of Γ_H in $\mathrm{PGL}_2^+(\mathbb{R})$ and hence defines a Möbius transformation $m\colon \mathbb{H} \to \mathbb{H}$ that pushes down to ι. This is equivalent to the previous definition. Indeed if $\tilde{m} \in \mathrm{GL}_2^+(\mathbb{R})$ is a lift of m, then $\tilde{m}$ normalizes $\Gamma_{\pm H} = (\mathbb{R}^\times\Gamma_H) \cap \mathrm{SL}_2(\mathbb{R})$, hence conjugation by $\tilde{m}$ preserves the set of $\mathbb{Q}$-linear combinations of matrices in $\Gamma_{\pm H}$, which is equal to the set of matrices with entries in $\mathbb{Q}$. Looking at the conjugates by $\tilde{m}$ of the matrices $\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right)$, we easily deduce that $\tilde{m}$ is a real multiple of a matrix in $\mathrm{GL}_2(\mathbb{Q})$, and consequently m lies in $\mathrm{PGL}_2^+(\mathbb{Q})$.

In other words: every modular automorphism of $Y_H(\mathbb{C})$ extends to a modular automorphism of X_H and, conversely, every modular automorphism of X_H preserves the set of cusps, hence restricts to a modular automorphism of $Y_H(\mathbb{C})$.

If an automorphism is modular, then it preserves the set of cusps and also the set of branch points for the map $\mathbb{H} \to \Gamma_H\backslash\mathbb{H}$. The converse is also true.

Lemma 3.6.3. *Let n be a positive integer and let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ such that $\det(H) = (\mathbb{Z}/n\mathbb{Z})^\times$. An automorphism of X_H defined over $\mathbb{C}$ is modular if and only if it preserves the set of cusps and the set of branch points for the map $\mathbb{H} \to \Gamma_H\backslash\mathbb{H} = Y_H(\mathbb{C})$.*

Proof. We prove that an automorphism u of X_H is modular if it preserves the set of cusps and the set of branch points for the map $\mathbb{H} \to \Gamma_H \backslash \mathbb{H} = Y_H(\mathbb{C})$. Since u preserves the set of the cusps, then it restricts to an automorphism of $Y_H(\mathbb{C})$. Moreover, since u preserves $\mathcal{B}$, then it induces an automorphism $\tilde{u}$ of $Y_H(\mathbb{C}) - \mathcal{B}$. Since $\det(H) = (\mathbb{Z}/n\mathbb{Z})^\times$, the map

$$\tilde{\pi} \colon \mathbb{H} - \pi^{-1}(\mathcal{B}) \longrightarrow Y_H(\mathbb{C}) - \mathcal{B}$$

is a covering map and the pushforward $\tilde{\pi}_*$ sends the fundamental group $\pi_1(\mathbb{H} - \pi^{-1}(\mathcal{B}))$ to the subgroup of $\pi_1(Y_H(\mathbb{C}) - \mathcal{B})$ generated by the loops running around a point in $\mathcal{B}$. Since $\tilde{u}$ extends to $u \colon Y_H(\mathbb{C}) \to Y_H(\mathbb{C})$, the image, under $\tilde{u}$, of a loop running around a point in $\mathcal{B}$ is still a loop running around a point in $\mathcal{B}$. Hence, $\tilde{u}_*$ sends $\tilde{\pi}_*(\pi_1(\mathbb{H} - \pi^{-1}(\mathcal{B})))$ into itself and consequently $\tilde{u}$ lifts to an automorphism $\tilde{v}$ of $\mathbb{H} - \pi^{-1}(\mathcal{B})$. Again, since $\tilde{u}$ extends to $u \colon Y_H(\mathbb{C}) \to Y_H(\mathbb{C})$, then $\tilde{v}$ extends to an automorphism $v \colon \mathbb{H} \to \mathbb{H}$ as well.

We know that $\mathrm{Aut}(\mathbb{H}) = \mathrm{PGL}_2^+(\mathbb{R})$, hence v is a Möbius transformation given by a matrix $m \in \mathrm{PGL}_2^+(\mathbb{R})$ and, since it passes to the quotient, m belongs to the normalizer of the image of Γ_H in $\mathrm{PGL}_2^+(\mathbb{R})$. Hence the restriction of u to Y_H is modular and, by Remark 3.6.2, u itself is modular. □

In the following two propositions, we give sufficient conditions for an automorphism to preserve the set of cusps and the set of branch points.

Proposition 3.6.4. *Let n be a positive integer and let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ containing the scalar matrices and such that $\det(H) = (\mathbb{Z}/n\mathbb{Z})^\times$. Let $\mathrm{gon}(X_H)$ be the gonality of X_H. If there is a prime ℓ not dividing n such that $5 \leq \ell < \frac{1}{2}\mathrm{gon}(X_H) - 1$, then every automorphism of X_H defined over a compositum of quadratic fields preserves the set of cusps.*

Proof. Let u be an automorphism of X_H defined over the compositum L of some quadratic fields and let $C \in X_H(\mathbb{C})$ be a cusp. Then the propositions 3.3.2 and 3.3.4 imply

$$T_\ell u(C) = u^\sigma T_\ell(C) = \ell u^\sigma \langle \ell \rangle (C^{\sigma^{-1}}) + u^\sigma(C^\sigma),$$

where $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ is a Frobenius element at ℓ. Since $\ell \geq 5$, then $T_\ell u(C)$ contains a point of multiplicity at least 4 and, by Part (1) of Proposition 3.3.6, this implies that $u(C)$ must be a cusp. □

Proposition 3.6.5. *Let n be a positive integer and let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ containing the scalar matrices and such that $\det(H) = (\mathbb{Z}/n\mathbb{Z})^\times$. Let $\mathrm{gon}(X_H)$ be the gonality of X_H. If there are two prime numbers $\ell_1 < \ell_2$ not dividing n and such that $5 \leq \ell_2 < \frac{1}{2}\mathrm{gon}(X_H) - 1$, then every automorphism of X_H defined over a compositum of quadratic fields preserves the set of branch points of the map $\mathbb{H} \to \Gamma_H \backslash \mathbb{H} = Y_H(\mathbb{C})$.*

Proof. Let L be a compositum of quadratic fields and let $\sigma_1, \sigma_2 \in \mathrm{Gal}(L/\mathbb{Q})$ be Frobenius elements at the primes ℓ_1 and ℓ_2 respectively. Let u be an automorphism of X_H defined over L and let $P = (E, \phi) \in Y_H(\mathbb{C})$ be a branch point for the map $\mathbb{H} \to \Gamma_H \backslash \mathbb{H} = Y_H(\mathbb{C})$. Applying Proposition 3.6.4 with $\ell = \ell_2 \geq 5$, we deduce that u sends non-cuspidal points to non-cuspidal points, hence we can write $u(P) = (E', \phi')$ for some elliptic curve $E'/\mathbb{C}$. Proposition 3.3.2 implies that

$$T_{\ell_1} u(P) = u^{\sigma_1} T_{\ell_1}(P) \quad \text{and} \quad T_{\ell_2} u(P) = u^{\sigma_2} T_{\ell_2}(P). \tag{3.6.6}$$

Since, up to isomorphism, the only elliptic curves over $\mathbb{C}$ with non-trivial automorphisms are E_i and E_ρ, Proposition 3.2.4 implies that there are only two possibilities: $E = E_i$ or $E = E_\rho$.

Firstly we treat the case $P = (E_\rho, \phi)$. Since P is a branch point, by Proposition 3.2.4, we know that $\phi^{-1} \circ \rho|_{E_\rho[n]} \circ \phi \in H$. Hence, we can apply Part (1) of Proposition 3.3.10, for each $k \in \{1, 2\}$, which gives

$$T_{\ell_k}(E', \phi') = T_{\ell_k} u(P) = u^{\sigma_k} T_{\ell_k}(P) \geq 3P_1, \tag{3.6.7}$$

for some point $P_1 \in Y_H(\mathbb{C})$. Because of last inequality, we can apply Proposition 3.3.6 Part (2) to obtain that $\mathbb{Z}[\ell_1^2 \rho]$ and $\mathbb{Z}[\ell_2^2 \rho]$ are both contained in $\mathrm{End}(E')$ which implies $\mathrm{End}(E') = \mathbb{Z}[\rho]$. Since the class group of $\mathbb{Z}[\rho]$ is trivial, we have $E' \cong E_\rho$. Again by Inequality (3.6.7), Proposition 3.3.10 Part (1) implies that $\phi'^{-1} \circ \rho|_{E_\rho[n]} \circ \phi' \in H$. By Proposition 3.2.4, we conclude that $u(P)$ is a branch point associated to the elliptic curve E_ρ.

Now, we consider $P = (E_i, \phi)$. Since P is a branch point, by Proposition 3.2.4, we know that $\phi^{-1} \circ i|_{E_i[n]} \circ \phi \in H$. Hence, by Proposition 3.3.10 Part (2), one of the following two possibilities happens

$$\begin{aligned} &T_{\ell_2} u(P) = u^{\sigma_2} T_{\ell_2}(P) = 2(P_1 + \ldots + P_{\frac{\ell_2+1}{2}}) \quad \text{or} \\ &T_{\ell_2} u(P) = u^{\sigma_2} T_{\ell_2}(P) = 2(P_1 + \ldots + P_{\frac{\ell_2-1}{2}}) + P_{\frac{\ell_2+1}{2}} + P_{\frac{\ell_2+3}{2}}, \end{aligned} \tag{3.6.8}$$

with $P_1, \ldots, P_{\frac{\ell_2+3}{2}}$ being distinct points in $Y_H(\mathbb{C})$. This equation implies that the hypotheses of Proposition 3.3.6 Part (3) are satisfied, hence $\mathbb{Z}[\ell_2^2 i]$ is contained in $\mathrm{End}(E')$. We now prove, distinguishing three cases, that $\mathbb{Z}[\ell_1^2 i]$ is contained in $\mathrm{End}(E')$. If $\ell_1 \geq 5$, we can apply the same argument used for ℓ_2. If $\ell_1 = 2$ or $\ell_1 = 3$, by Proposition 3.3.10 Part (2) and Equation (3.6.6), there is a point $(E'', \phi'') \in Y_H(\mathbb{C})$ such that

$$T_{\ell_1}(E', \phi') = T_{\ell_1} u(P) = u^{\sigma_1} T_{\ell_1}(P) \geq 2(E'', \phi''). \tag{3.6.9}$$

If $\ell_1 = 3$, Lemma 3.3.5 implies that E'' has an endomorphism $\beta \neq \pm 3$ having degree 9. Since E'' is isogenous to E', we know that $\mathrm{End}(E'') \subset \mathbb{Z}[i]$, hence $\beta = \pm 3i$. Using that

E' and E'' are 3-isogenous, we see that

$$\mathrm{End}(E') \supset \mathbb{Z} + 3\mathrm{End}(E'') \supset \mathbb{Z} + 3\mathbb{Z}[\beta] = \mathbb{Z}[9i].$$

If $\ell_1 = 2$, Inequality (3.6.9) and Lemma 3.3.5 imply that E'' has an endomorphism $\beta \neq \pm 2$ having degree 4. Since E'' is isogenous to E', we know that $\mathrm{End}(E'') \subset \mathbb{Z}[i]$, hence $\beta = \pm 2i$ or $\beta = \pm 1 \pm i$. Using that E' and E'' are 2-isogenous, we see that

$$\mathrm{End}(E') \supset \mathbb{Z} + 2\mathrm{End}(E'') \supset \mathbb{Z} + 2\mathbb{Z}[\beta] \supset \mathbb{Z}[4i].$$

We proved that both $\mathbb{Z}[\ell_1^2 i]$ and $\mathbb{Z}[\ell_2^2 i]$ are contained in $\mathrm{End}(E')$, hence $\mathrm{End}(E') = \mathbb{Z}[i]$ and, since the class group of $\mathbb{Z}[i]$ is trivial, we deduce that $E' \cong E_i$. By Equation (3.6.8), the hypotheses of Proposition 3.3.10 Part (2) are satisfied, hence $\phi'^{-1} \circ i|_{E_i[n]} \circ \phi' \in H$ and, by Proposition 3.2.4, we conclude that $u(P)$ is a branch point. □

Propositions 3.6.4 and 3.6.5, together with Lemma 3.6.3, imply the following Corollary, which gives a concise sufficient condition to exclude the presence of non-modular automorphisms.

Corollary 3.6.10. *Let n be a positive integer let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ containing the scalar matrices and such that $\det(H) = (\mathbb{Z}/n\mathbb{Z})^\times$ and let $\mathrm{gon}(X_H)$ be the gonality of X_H. If there are two primes $\ell_1 < \ell_2$ not dividing n such that $5 \leq \ell_2 < \frac{1}{2}\mathrm{gon}(X_H) - 1$, then every automorphism of X_H defined over a compositum of quadratic fields is modular.*

We still need to determine which are the modular automorphisms of a modular curve X_H for Cartan and Cartan-plus subgroups H of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Since in these cases we have $\det(H) = (\mathbb{Z}/n\mathbb{Z})^\times$, then Y_H also parametrizes pairs $[E, \phi]$ such that the Weil pairing of $(\phi\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right), \phi\left(\begin{smallmatrix}0\\1\end{smallmatrix}\right))$ is fixed, up to the action of $H \cap \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$. With this interpretation, every matrix $\gamma \in \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ that normalizes $H \cap \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ defines an automorphism of Y_H sending $[E, \phi] \mapsto [E, \phi \circ \gamma]$: such an automorphism is modular, induced by a lift of γ in $\mathrm{SL}_2(\mathbb{Z})$. Next proposition implies that these are all the modular automorphisms except when $n \equiv 2 \bmod 4$ and H is a Cartan-plus which is split at 2. We now suppose we are in this last case and we construct another modular automorphism. Letting $n = 2n'$, we have

$$H = H_2 \times H_{n'} \subset \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/n'\mathbb{Z}) = \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}),$$

where H_2 and $H_{n'}$ are the images of H in $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ and $\mathrm{GL}_2(\mathbb{Z}/n'\mathbb{Z})$ respectively. Since we are assuming that H_2 is a split Cartan-plus subgroup, there are three possibilities for H_2 (all conjugated) and, depending on them, we define

$$\gamma_0 := \begin{cases} \left(\begin{smallmatrix}3&1\\1&1\end{smallmatrix}\right), & \text{if } H_2 = \{\mathrm{Id}, \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)\}, \\ \left(\begin{smallmatrix}2&1\\2&2\end{smallmatrix}\right), & \text{if } H_2 = \{\mathrm{Id}, \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)\}, \\ \left(\begin{smallmatrix}2&2\\1&2\end{smallmatrix}\right), & \text{if } H_2 = \{\mathrm{Id}, \left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)\}. \end{cases} \tag{3.6.11}$$

Since the projection $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/2n\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}/n'\mathbb{Z})$ is surjective and since $\det(H_{n'}) = (\mathbb{Z}/n'\mathbb{Z})^\times$, there exists

$$\text{(3.6.12)} \quad \gamma_1 \in \mathrm{SL}_2(\mathbb{Z}) \quad \text{such that} \quad \gamma_1 \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \pmod 4 \quad \text{and} \quad \gamma_0\gamma_1 \pmod{\tfrac{n}{2}} \in H_{\frac{n}{2}}.$$

The matrix $\mathbb{P}(\gamma_0\gamma_1)$ lies in the normalizer $\mathcal{N}$ of $\mathbb{P}(\Gamma_H)$ inside $\mathrm{PGL}_2^+(\mathbb{Q})$ and we have that $\mathbb{P}(\gamma_0\gamma_1)^2 \in \mathbb{P}(\Gamma_H)$, hence $\mathbb{P}(\gamma_0\gamma_1)$ induces an involution on X_H. Since $\mathbb{P}(\gamma_0\gamma_1)$ is not in $\mathbb{P}(\mathrm{SL}_2(\mathbb{Z}))$, the modular automorphism defined by $\gamma_0\gamma_1$ is not of the form $[E, \phi] \mapsto [E, \phi \circ \gamma]$ with $\gamma \in \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$.

Proposition 3.6.13. *Let n be a positive integer and let $H < \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ be either a Cartan subgroup or a Cartan-plus subgroup. Let $N' < \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ be the normalizer of the group $H' := H \cap \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ and let $\mathcal{N}$ be the normalizer of $\mathbb{P}(\Gamma_H)$ in $\mathrm{PGL}_2^+(\mathbb{Q})$. If $n \equiv 2 \bmod 4$ and H is a Cartan-plus split at 2, then, for every choice of γ_0 and γ_1 as in (3.6.11) and (3.6.12), $\mathcal{N}$ is generated by $\mathbb{P}(\Gamma_{N'})$ and $\mathbb{P}(\gamma_0\gamma_1)$. Otherwise $\mathcal{N}$ is $\mathbb{P}(\Gamma_{N'})$.*

Proof. Let $\tilde{\mathcal{N}} < \mathrm{GL}_2^+(\mathbb{Q})$ be the normalizer of $\mathbb{Q}^\times\Gamma_H$, or, equivalently, the normalizer of Γ_H (each matrix normalizing $\mathbb{Q}^\times\Gamma_H$ also normalizes $(\mathbb{Q}^\times\Gamma_H) \cap \mathrm{SL}_2(\mathbb{Q}) = \Gamma_H$, and since scalar matrices commute with everything, each matrix normalizing Γ_H also normalizes $\mathbb{Q}^\times\Gamma_H$). The statement of the proposition is equivalent to

$$\tilde{\mathcal{N}} = \mathbb{Q}^\times\Gamma_{N'} \quad \text{or} \quad \tilde{\mathcal{N}} = \mathbb{Q}^\times\langle\gamma_0\gamma_1, \Gamma_{N'}\rangle,$$

depending on the case. The inclusions $\supseteq$ are trivial, hence we prove the other inclusions. Since the normalizer of Γ_H inside $\mathrm{SL}_2(\mathbb{Z})$ is $\Gamma_{N'}$, it is enough to show that

$$\tilde{\mathcal{N}} \subseteq \mathbb{Q}^\times\mathrm{SL}_2(\mathbb{Z}) \quad \text{or} \quad \tilde{\mathcal{N}} \subseteq \mathbb{Q}^\times\mathrm{SL}_2(\mathbb{Z}) \cup \gamma_0\gamma_1\mathbb{Q}^\times\mathrm{SL}_2(\mathbb{Z}),$$

depending on the case. We suppose that $\tilde{\mathcal{N}}$ contains a matrix $m = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ not lying in $\mathbb{Q}^\times\mathrm{SL}_2(\mathbb{Z})$: it is enough to prove, with this assumption, that $n \equiv 2 \bmod 4$ and H is a Cartan-plus subgroup split at 2 and $m \in \gamma_0\gamma_1\mathbb{Q}^\times\mathrm{SL}_2(\mathbb{Z})$.

Up to multiplication by a scalar matrix, we can suppose that $a, b, c, d \in \mathbb{Z}$ and that $\gcd(a, b, c, d) = 1$. Since $m \notin \mathbb{Q}^\times\mathrm{SL}_2(\mathbb{Z})$, then $\det(m) \neq 1$. Let p be a prime dividing $\det(m)$, let $\lambda_1 = \left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right), \lambda_2 = \left(\begin{smallmatrix} b \\ d \end{smallmatrix}\right) \in \mathbb{Z}^2$ and let $\Lambda \subset \mathbb{Z}^2$ be the lattice generated by λ_1, λ_2. By definition of $\tilde{\mathcal{N}}$, for every $\gamma \in \Gamma_H$ there is $\gamma' = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \in \Gamma_H$ such that $\gamma m = m\gamma'$. Hence, looking at the columns of γm, we get $\gamma\lambda_1 = x\lambda_1 + z\lambda_2$ and $\gamma\lambda_2 = y\lambda_1 + w\lambda_2$. Since γ is arbitrary and $\gamma' \in \mathrm{SL}_2(\mathbb{Z})$, we have

$$\Gamma_H\Lambda = \Lambda.$$

Let $\overline{\Lambda}$ be the image of Λ under the quotient map $\mathbb{Z}^2 \to \mathbb{F}_p^2$. Since at least one of a, b, c, d is not multiple of p, we know that $\overline{\Lambda} \neq \{0\}$ and since $\det(m)$ is multiple of p, we know

that $\overline{\Lambda} \neq \mathbb{F}_p^2$. Hence $\overline{\Lambda}$ is a line inside $\mathbb{F}_p^2$ which is left invariant by every matrix in the image $\overline{\Gamma}_H$ of Γ_H in $\mathrm{GL}_2(\mathbb{F}_p)$. This implies that $\overline{\Gamma}_H$ is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$, thus p divides the level n and $\overline{\Gamma}_H = \overline{H} \cap \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, where $\overline{H}$ is the image of H in $\mathrm{GL}_2(\mathbb{F}_p)$. We deduce that either H is a Cartan group split at p or $p = 2$ and H is a Cartan-plus group split at p.

First we suppose that H is a Cartan group split at p. Let p^e be the maximum power of p dividing n. Up to conjugacy, the image of H in $\mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z})$ is $\{\left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right)\}$, hence, for every $\gamma \in \Gamma_H$, we have

$$m^{-1}\gamma m = \tfrac{1}{\det(m)} \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right) \gamma \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right) \pmod{p^e}.$$

Applying this to $\gamma = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$ and $\gamma = \left(\begin{smallmatrix} 1 & 0 \\ n & 1 \end{smallmatrix}\right)$, we see that since $\det(m)$ is multiple of p, then a, b, c, d are all multiples of p, which is a contradiction.

This contradiction implies that the only prime dividing $\det(m)$ is 2 and H is a Cartan-plus group split at 2. Let 2^e be the maximum power of 2 dividing n. Up to conjugacy, the image of H in $\mathrm{GL}_2(\mathbb{Z}/2^e\mathbb{Z})$ is $\{\left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & * \\ * & 0 \end{smallmatrix}\right)\}$. In particular the image of H in $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ is $\{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)\}$, hence $\overline{\Lambda} = \langle \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right) \rangle$ is the only $\overline{\Gamma}_H$-invariant line. In other words the columns $\left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right), \left(\begin{smallmatrix} b \\ d \end{smallmatrix}\right)$ of m span $\langle \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right) \rangle$ in $\mathbb{F}_2^2$ and with a similar argument we see that the rows $(a\,b), (c\,d)$ of m span $\langle (1\,1) \rangle$ in $\mathbb{F}_2^2$. Hence $m \equiv \left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right) \pmod 2$. For every $\gamma \in \Gamma_H$, we have

$$m^{-1}\gamma m \pmod{2^e} \in \left\{\left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & * \\ * & 0 \end{smallmatrix}\right)\right\}. \tag{3.6.14}$$

When $\gamma = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$, we see that $m^{-1}\gamma m \equiv \left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right) \pmod{2^e}$ is not possible because both c and d are odd, hence $m^{-1}\gamma m \equiv \left(\begin{smallmatrix} 0 & * \\ * & 0 \end{smallmatrix}\right) \pmod{2^e}$ and, by explicit computations, we deduce that $\det(m) = 2$ and $n \equiv 2 \bmod 4$. Finally, since $m \equiv \left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right) \pmod 2$ and $\det(m) = 2$, we see that $(\gamma_0\gamma_1)^{-1}m \in \mathrm{SL}_2(\mathbb{Z})$. □

We now prove the main results of this paper.

Theorem 3.6.15. *Let $n \geq 10^{400}$ be an integer and let $H < \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ be either a Cartan or a Cartan-plus subgroup. Then every automorphism of X_H is modular, hence we have*

$$\mathrm{Aut}(X_H) \cong \begin{cases} N'/H' \times \mathbb{Z}/2\mathbb{Z}, & \text{if } n \equiv 2 \bmod 4 \text{ and } H \text{ is a Cartan-plus split at 2,} \\ N'/H', & \text{otherwise,} \end{cases}$$

where $N' < \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ is the normalizer of $H' := H \cap \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$.

Proof. Let $\mathcal{N}$ be the normalizer of $\mathbb{P}(\Gamma_H)$ inside $\mathrm{PGL}_2^+(\mathbb{Q})$. By Proposition 3.6.13 we

have

$$\mathcal{N}/\mathbb{P}(\Gamma_H) \cong \begin{cases} \mathbb{P}(\Gamma_{N'})/\mathbb{P}(\Gamma_H) \times \mathbb{Z}/2\mathbb{Z}, & \text{if } n \equiv 2 \bmod 4 \text{ and } H \text{ is a Cartan-plus split at 2,} \\ \mathbb{P}(\Gamma_{N'})/\mathbb{P}(\Gamma_H), & \text{otherwise,} \end{cases}$$

where the first case is true because $\mathbb{P}(\gamma_0\gamma_1\Gamma_H)$ has order 2 in $\mathcal{N}/\mathbb{P}(\Gamma_H)$ and commutes with every element in $\mathbb{P}(\Gamma_{N'})/\mathbb{P}(\Gamma_H)$. Since $\mathbb{P}(\Gamma_{N'})/\mathbb{P}(\Gamma_H) \cong \mathbb{P}(\Gamma_{N'})/\mathbb{P}(\Gamma_{H'}) \cong N'/H'$, it is enough to prove that every automorphism of X_H is modular. For $n \geq 10^{400}$ every automorphism is defined over the compositum of some quadratic fields by Proposition 3.5.7. We can bound the gonality $\mathrm{gon}(X_H)$ of X_H using [1] and, with the same estimates used in the proof of Proposition 3.4.9, we have

$$\mathrm{gon}(X_H) \geq \frac{7}{800}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_H] \geq \frac{7n^2}{800(\omega(n)+1)2^{\omega(n)}} > 10n.$$

So, there are at least two primes $\ell_1 < \ell_2$ not dividing n with $5 \leq \ell_2 < \frac{1}{2}\mathrm{gon}(X_H) - 1$. By Corollary 3.6.10, we can conclude that every automorphism is modular. □

Remark 3.6.16. One can determine the groups N'/H' in all cases. Indeed, let $n = \prod_{i=1}^{r} p_i^{e_i}$ be any positive integer with its prime factorization, let $H < \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ be either a Cartan or a Cartan-plus subgroup and let $N' < \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ be the normalizer of the group $H' := H \cap \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$. By Chinese Remainder Theorem we have

$$H' \cong \prod_{i=1}^{r} H_i' \quad \text{and} \quad N' \cong \prod_{i=1}^{r} N_i' \quad \text{inside} \quad \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \cong \prod_{i=1}^{r} \mathrm{SL}_2(\mathbb{Z}/p^{e_i}\mathbb{Z}),$$

where H_i' is the image of H' in $\mathrm{SL}_2(\mathbb{Z}/p^{e_i}\mathbb{Z})$ and $N_i' < \mathrm{SL}_2(\mathbb{Z}/p^{e_i}\mathbb{Z})$ is the normalizer of H_i'. Hence the knowledge of N'/H' for $H \in \{C_{\mathrm{ns}}(p^e), C_{\mathrm{ns}}(p^e), C_{\mathrm{s}}(p^e), C_{\mathrm{s}}^+(p^e)\}$ allows to compute the group N'/H' for every Cartan or Cartan-plus subgroup H of level n not necessarily a prime power. Explicit computations give the following:

- if $H = C_{\mathrm{ns}}(p^e)$, then $N'/H' \cong \mathbb{Z}/2\mathbb{Z}$, since $N' = C_{\mathrm{ns}}^+(p^e) \cap \mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z})$;
- if $p^e \neq 3$ and $H = C_{\mathrm{ns}}^+(p^e)$, then $N'/H' \cong \{1\}$;
- if $H = C_{\mathrm{ns}}^+(3)$, then $N'/H' \cong \langle \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \rangle \cong \mathbb{Z}/3\mathbb{Z}$;
- if $p \neq 2, 3$ and $H = C_{\mathrm{s}}(p^e)$, then $N'/H' \cong \langle \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \rangle \cong \mathbb{Z}/2\mathbb{Z}$;
- if $e \geq 2$ and $H = C_{\mathrm{s}}(3^e)$, then

  $$N'/H' \cong \left\langle \begin{pmatrix} 1 & 3^{e-1} \\ -3^{e-1} & 1 \end{pmatrix} \right\rangle \times \left\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 3^{e-1} \\ 3^{e-1} & 1 \end{pmatrix} \right\rangle \cong \mathbb{Z}/3\mathbb{Z} \times S_3,$$

  where S_3 is the symmetric group acting on three elements;

- if $e \geq 5$ and $H = C_{\mathrm{s}}(2^e)$, then
$$N'/H' \cong \left\langle \left(\begin{smallmatrix} 1 & 2^{e-3} \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ -2^{e-3} & 1 \end{smallmatrix}\right) \right\rangle \rtimes \left\langle \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \right\rangle \cong (\mathbb{Z}/8\mathbb{Z})^2 \rtimes_{\varphi} (\mathbb{Z}/2\mathbb{Z}),$$
where $(\varphi(1))(x, y) = (y, x)$; this group is labeled as $(128, 67)$ in MAGMA, [50];
- if $p^e \in \{3, 2, 2^2, 2^3\}$ and $H = C_{\mathrm{s}}(p^e)$, then $N'/H' \cong \mathrm{PSL}_2(\mathbb{Z}/p^e\mathbb{Z})$, since we have $N' = \mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z})$;
- if $H = C_{\mathrm{s}}(2^4)$, then $N'/H' \cong \left\langle \left(\begin{smallmatrix} -1 & 6 \\ 6 & -5 \end{smallmatrix}\right), \left(\begin{smallmatrix} 4 & 9 \\ 7 & -4 \end{smallmatrix}\right) \right\rangle \rtimes \left\langle \left(\begin{smallmatrix} 1 & -2 \\ 0 & 1 \end{smallmatrix}\right) \right\rangle \cong D_8 \rtimes_{\varphi} (\mathbb{Z}/8\mathbb{Z})$, where $D_8 \cong \mathbb{Z}/8\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ is the dihedral group of order 16 and $(\varphi(1))(1, 0) = (5, 0)$ and $(\varphi(1))(0, 1) = (3, 1)$; moreover N'/H' is labeled as $(128, 68)$ in MAGMA, [50];
- if $p \neq 2, 3$ and $p^e \neq 5$ and $H = C_{\mathrm{s}}^+(p^e)$ then $N'/H' \cong \{1\}$;
- if $H = C_{\mathrm{s}}^+(5)$, then $N'/H' \cong \langle \left(\begin{smallmatrix} 1 & 2 \\ 1 & 3 \end{smallmatrix}\right) \rangle \cong \mathbb{Z}/3\mathbb{Z}$;
- if $e \geq 2$ and $H = C_{\mathrm{s}}^+(3^e)$, then $N'/H' \cong \left\langle \begin{pmatrix} 1 & -3^{e-1} \\ 3^{e-1} & 1 \end{pmatrix} \right\rangle \cong \mathbb{Z}/3\mathbb{Z}$;
- if $H = C_{\mathrm{s}}^+(3)$, then $N'/H' \cong \langle \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right) \rangle \cong \mathbb{Z}/2\mathbb{Z}$;
- if $e \geq 6$ and $H = C_{\mathrm{s}}^+(2^e)$, then $N'/H' \cong \left\langle \begin{pmatrix} 1 & -2^{e-3} \\ 2^{e-3} & 1 \end{pmatrix} \right\rangle \cong \mathbb{Z}/8\mathbb{Z}$;
- if $H = C_{\mathrm{s}}^+(2)$, then $N'/H' \cong \{1\}$;
- if $H = C_{\mathrm{s}}^+(2^2)$, then $N'/H' \cong \langle \left(\begin{smallmatrix} 1 & 2 \\ 2 & 1 \end{smallmatrix}\right) \rangle \cong \mathbb{Z}/2\mathbb{Z}$;
- if $H = C_{\mathrm{s}}^+(2^3)$, then $N'/H' \cong \left\langle \left(\begin{smallmatrix} 1 & -2 \\ 2 & -3 \end{smallmatrix}\right) \right\rangle \cong \mathbb{Z}/4\mathbb{Z}$;
- if $H = C_{\mathrm{s}}^+(2^4)$, then $N'/H' \cong \left\langle \left(\begin{smallmatrix} 1 & 6 \\ 2 & -3 \end{smallmatrix}\right) \right\rangle \cong \mathbb{Z}/8\mathbb{Z}$;
- if $H = C_{\mathrm{s}}^+(2^5)$, then $N'/H' \cong \left\langle \left(\begin{smallmatrix} 1 & -4 \\ 4 & -15 \end{smallmatrix}\right) \right\rangle \cong \mathbb{Z}/8\mathbb{Z}$.

Recall that the groups N'/H' computed for $H = C_{\mathrm{s}}(p^e)$ are the same determined in [4], [2], [14], in the setting of Borel modular curves.

For Cartan modular curves of prime power level we make Theorem 3.6.15 more precise.

Theorem 3.6.17. *Let p be a prime number and let e be a positive integer. If $p^e > 11$ and $p^e \notin \{3^3, 2^4, 2^5, 2^6\}$, then all the automorphisms of $X_{\mathrm{ns}}(p^e), X_{\mathrm{ns}}^+(p^e), X_{\mathrm{s}}(p^e)$ and $X_{\mathrm{s}}^+(p^e)$ are modular and*

$$\mathrm{Aut}(X_{\mathrm{ns}}(p^e)) \cong \mathbb{Z}/2\mathbb{Z}, \qquad \mathrm{Aut}(X_{\mathrm{ns}}^+(p^e)) \cong \{1\},$$

$$\mathrm{Aut}(X_{\mathrm{s}}(p^e)) \cong \begin{cases} (\mathbb{Z}/8\mathbb{Z})^2 \rtimes (\mathbb{Z}/2\mathbb{Z}), & \text{if } p = 2, \\ \mathbb{Z}/3\mathbb{Z} \times S_3, & \text{if } p = 3, \\ \mathbb{Z}/2\mathbb{Z}, & \text{if } p > 3, \end{cases} \quad \mathrm{Aut}(X_{\mathrm{s}}^+(p^e)) \cong \begin{cases} \mathbb{Z}/8\mathbb{Z}, & \text{if } p = 2, \\ \mathbb{Z}/3\mathbb{Z}, & \text{if } p = 3, \\ \{1\}, & \text{if } p > 3, \end{cases}$$

where the above semidirect product $(\mathbb{Z}/8\mathbb{Z})^2 \rtimes \mathbb{Z}/2\mathbb{Z}$ is described in Remark 3.6.16.

Proof. We first treat the case $p^e > 49$ with $p^e \neq 2^6 = 64$. Up to conjugacy we can assume that $H \in \{C_{\mathrm{s}}(p^e), C_{\mathrm{s}}^+(p^e), C_{\mathrm{ns}}(p^e), C_{\mathrm{ns}}^+(p^e)\}$ where these groups are the subgroups of $\mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z})$ defined in Chapter 3.4 and $X_H \in \{X_{\mathrm{ns}}(p^e), X_{\mathrm{ns}}^+(p^e), X_{\mathrm{s}}(p^e), X_{\mathrm{s}}^+(p^e)\}$ is the corresponding associated modular curve. By [1, Theorem 0.1] and Table 3.1, for $p^e > 87$, we have the following lower bounds for the gonality of X_H:

$$\mathrm{gon}(X_H) \geq \frac{7}{800}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_H] \geq \frac{7}{800}\frac{p^{2e}(1-\frac{1}{p})}{2} > \frac{7 \cdot 87^2}{3200} > 16.$$

Hence there are two primes $\ell_1 < \ell_2$, different from p, such that $5 \leq \ell_2 < \frac{1}{2}\mathrm{gon}(X_H) - 1$: we can take $\ell_1 = 3$, $\ell_2 = 7$ if $p \in \{2, 5\}$ and $\ell_1 = 2$, $\ell_2 = 5$ otherwise. With a similar computation one can show that $\mathrm{gon}(X_H) > 12$, for $49 < p^e \leq 87$, if $p^e \neq 64$ and we can take $\ell_1 \in \{2, 3\}$, $\ell_2 = 5$. Applying Corollary 3.6.10 we deduce that all the automorphisms of X_H defined over a compositum of quadratic fields are modular, hence, by Proposition 3.5.8, all the automorphisms of X_H are modular. Finally, we can use Proposition 3.6.13 and Remark 3.6.16 to obtain the group of modular automorphisms.

We now assume $11 < p^e \leq 49$. All the cases $X_{\mathrm{s}}(p^e) \cong X_0(p^{2e})$ are treated in [60], all the cases $X_{\mathrm{s}}^+(p)$ are treated in [47] and the cases $X_{\mathrm{ns}}(p)$, $X_{\mathrm{ns}}^+(p)$, for $13 \leq p \leq 31$, are treated in [48]. The remaining cases $X_{\mathrm{s}}^+(25)$, $X_{\mathrm{s}}^+(49)$ and $X_{\mathrm{ns}}(p^e)$, $X_{\mathrm{ns}}^+(p^e)$, for $p^e = 25, 37, 41, 43, 47, 49$, are treated in the MAGMA script available at [70]. □

Last theorem can be specialized to the prime level case, obtaining new results for non-split Cartan curves. The split cases are treated in [47] and [60].

Corollary 3.6.18. *Let $p \geq 13$ be a prime number. Then the group of automorphisms of $X_{\mathrm{ns}}^+(p)$ is trivial and the group of automorphisms of $X_{\mathrm{ns}}(p)$ has order 2.*

Remark 3.6.19. Theorem 3.6.17 implies that, for p^{2e} big enough, all the automorphisms of $X_0^*(p^{2e}) \cong X_{\mathrm{s}}^+(p^e)$ are modular, extending [5] and [47] that treat the cases $X_0^*(p)$ and $X_0^*(p^2)$. Our techniques (in particular Lemma 3.6.5) cannot be generalized to the case $X_0^*(p^e)$ with e odd, because some of the branch points of the natural map $\mathbb{H} \to Y_0^+(p^e)$ have the form $\{(E, C), (E/C, E[p^e]/C)\}$ with $E \neq E_i, E_\rho$. Anyway, the techniques used in [47, Lemmas 4, 5, 6], together with Proposition 3.5.9, can be used to prove the modularity of all elements in $\mathrm{Aut}(X_0^*(p^e))$, without restrictions on e, for all but finitely many cases.

3.7 Appendix

Let $G := \mathrm{GL}_2(\mathbb{Z}/2^e\mathbb{Z})$. For each $H < G$, let $\chi_H \colon G \to \mathbb{Q}$ be the character of the representation $\mathbb{Q}[G/H]$. The entry (γ, H) of the table below is $\chi_H(\gamma)$. Every element of G is conjugated to a unique element appearing in the first column, hence the table determines

the characters χ_H for H appearing in Proposition 3.4.2 or in [26, Theorem 1.1]. In the first column we have $\lambda, a \in (\mathbb{Z}/2^e\mathbb{Z})^\times$, $b \in (\mathbb{Z}/2^e\mathbb{Z})$, $k \in \{1, \dots, e-1\}$, and $u \in (\mathbb{Z}/2^{e-k}\mathbb{Z})^\times$.

Proving that the first column contains every conjugacy class of $\mathrm{GL}_2(\mathbb{Z}/2^e\mathbb{Z})$ exactly once is rather easy, yet cumbersome, using the following lemma.

Lemma 3.7.1. *Let $M \in \mathrm{M}_{2\times 2}(\mathbb{Z}/2^e\mathbb{Z})$. If $M \equiv \left(\begin{smallmatrix} 0 & * \\ 1 & * \end{smallmatrix}\right) \bmod 2$ or $M \equiv \left(\begin{smallmatrix} * & 1 \\ * & 0 \end{smallmatrix}\right) \bmod 2$, then there are unique elements $a, b \in \mathbb{Z}/2^e\mathbb{Z}$ such that M is conjugated to $\left(\begin{smallmatrix} 0 & a \\ 1 & b \end{smallmatrix}\right)$. If $M \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \bmod 2$ or $M \equiv \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) \bmod 2$, then there are unique elements $\lambda_1, \lambda_2 \in \mathbb{Z}/2^e\mathbb{Z}$, the first odd and the second even, such that M is conjugated to $\left(\begin{smallmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{smallmatrix}\right)$*

Proof. The cases $M \equiv \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) \bmod 2$ and $M \equiv \left(\begin{smallmatrix} * & 1 \\ * & 0 \end{smallmatrix}\right) \bmod 2$ can be reduced to the remaining cases by considering $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)^{-1} M \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Let V be the module made of column vectors in $(\mathbb{Z}/2^e\mathbb{Z})^2$ with standard basis e_1, e_2 and let $F_M \colon V \to V$ be the multiplication by M.

If $M \equiv \left(\begin{smallmatrix} 0 & * \\ 1 & * \end{smallmatrix}\right) \bmod 2$ we notice that $e_1, F_M(e_1)$ are a basis of V when we reduce modulo 2, hence they are a basis of V. In the basis $B = (e_1, F_M(e_1))$ we have

$$M \sim F_M^B = \left(\begin{smallmatrix} 0 & a \\ 1 & b \end{smallmatrix}\right)$$

for some a, b, that are unique since $a = -\det(M)$ and $b = \mathrm{tr}(M)$.

Finally the case $M \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \bmod 2$. The uniqueness result is motivated by the fact that λ_1, λ_2 are the only roots of $\det(M - \lambda\mathrm{Id})$. The existence part is a Hensel argument. Let $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and let us lift for example e_1 to an eigenvector:

$$\begin{aligned} &F_M(e_1 + \lambda) = (a + \lambda b)e_1 + (c + \lambda d)e_2 \quad \in \langle e_1 + \lambda e_2 \rangle \quad \iff \\ &\lambda(a + \lambda b) = c + \lambda d \quad \iff b\lambda^2 + (a - d)\lambda - c = 0 \end{aligned}$$

and last equation has a unique zero because the polynomial $p(\lambda) = b\lambda^2 + (a-d)\lambda - c$ satisfies $p(0) \equiv 0, p'(0) \not\equiv 0$ modulo 2. With the same argument we can lift e_2 to an eigenvector. □

In order to fill Table 3.2 we use that

$$\mathbb{Q}[G/H] = \bigoplus gH \cdot \mathbb{Q} \quad \text{and} \quad \forall \gamma \in G: \quad \rho_H(\gamma)(gH) = \gamma gH$$

hence, in basis $\{gH\}$ the matrix $\rho_H(\gamma)$ is a permutation matrix and consequently

$$\chi_H(\gamma) = \mathrm{tr}(\rho_H(\gamma)) = \#\{gH : \gamma gH = gH\} = \frac{\#\{g : \gamma g \in gH\}}{\#H} = \frac{\#\{g : g^{-1}\gamma g \in H\}}{\#H}.$$

Table 3.2: Character table.

	$B_r, r \geq 0$	T_0	$T_r, r > 0$	C_s	C_s^+	C_{ns}	C_{ns}^+
λId	$3{\cdot}2^{2r}$	1	$3{\cdot}2^{2r-1}$	$3{\cdot}2^{2e-1}$	$3{\cdot}2^{2e-2}$	2^{2e-1}	2^{2e-2}
$\left(\begin{smallmatrix}0 & a\\ 1 & b\end{smallmatrix}\right)$ b odd	0	1	0	0	0	2	1
$\left(\begin{smallmatrix}0 & a\\ 1 & b\end{smallmatrix}\right)$ b even	1 if $r{=}0$ 0 if $r{>}0$	1	0	0	2^{e-1} if $b{=}0$ 0 if $b{\neq}0$	0	2^{e-1} if $b{=}0$ 0 if $b{\neq}0$
$\left(\begin{smallmatrix}\lambda & 0\\ 0 & \lambda+2^k u\end{smallmatrix}\right)$	$3{\cdot}2^{2r}$ if $r{<}k$ 2^{2k+1} if $r{\geq}k$	1	$3{\cdot}2^{2r-1}$ if $r{\leq}k$ 2^{2k+1} if $r{>}k$	2^{2k+1}	2^{2k}	0	0
$\left(\begin{smallmatrix}\lambda & 2^k u\\ 2^k & \lambda\end{smallmatrix}\right)$	$3{\cdot}2^{2r}$ if $r{<}k$ 2^{2r} if $r{=}k$ 0 if $r{>}k$	1	$3{\cdot}2^{2r-1}$ if $r{\leq}k$ 0 if $r{>}k$	0	0	0	0
$\left(\begin{smallmatrix}\lambda & 2^k u\\ 2^k & \lambda+2^k\end{smallmatrix}\right)$	$3{\cdot}2^{2r}$ if $r{<}k$ 0 if $r{\geq}k$	1	$3{\cdot}2^{2r-1}$ if $r{\leq}k$ 0 if $r{>}k$	0	0	2^{2k+1}	2^{2k}
$\left(\begin{smallmatrix}\lambda & 2^k u\\ 2^k & \lambda+2^{k+1}\end{smallmatrix}\right)$	$3{\cdot}2^{2r}$ if $r{<}k$ 2^{2r} if $r{=}k$ 0 if $r{>}k$	1	$3{\cdot}2^{2r-1}$ if $r{\leq}k$ 0 if $r{>}k$	0	0	0	0

Chapter 4

Discrete logarithms in small characteristic

Solving the discrete logarithm problem means the following: given a group G, a generator $g \in G$ and another element $h \in G$, find an integer z such that $g^z = h$. The hardness of this problem, which depends on the choice of G, has had implications in cryptography since the very beginning [33] of public-key cryptography. We are concerned with the cases where G is the multiplicative group of a finite field of *small characteristic*, which, for us, means a field of characteristic p and cardinality p^n for some integer $n > p$. Our main result is the following.

Theorem 4.0.1. *There exists a probabilistic algorithm, described in Section 4.4, that solves the discrete logarithm problem in $K^\times$ for all finite fields K of small characteristic in expected time*

$$(\log \#K)^{O(\log \log \#K)}.$$

An algorithm whose complexity is as above is called *quasi-polynomial*. In 2013 Barbulescu, Gaudry, Joux and Thomé presented in [19] the first heuristic quasi-polynomial algorithm solving the discrete logarithm in finite fields of small characteristic. One of their main ideas, originally in [56], was looking for a "simple" description of the Frobenius automorphism $\phi\colon K \to K$ and, if one can find such a simple description, using it in an index calculus algorithm to find relations among the elements of the factor base more easily.

In [49] a new algorithm was then presented, based on similar ideas, that was proven to terminate in quasi-polynomial expected time when it is possible to find a "simple" description of the Frobenius automorphism $\phi\colon K \to K$. In particular, we could deduce Theorem 4.0.1 if we knew that all finite fields of small characteristic K can be embedded in a slightly larger field K' admitting a presentation as in [49]. Unfortunately, the author

is not aware of any proof of this fact, even though computations like [56, Table 1] support it.

Our algorithm is based on the same approach as [49], adapted to fields admitting a different kind of presentation in terms of elliptic curves. Since over a finite field $\mathbb{F}_q$ there are many non-isomorphic elliptic curves, it is easy to prove that all finite fields of small characteristic can be embedded in a slightly larger field admitting such an elliptic presentation.

Elliptic presentations were firstly introduced in [30], as we have learnt after our first (incomplete) attempt to prove Theorem 4.0.1 using elliptic presentations (see the author's master's thesis [67]). In [65] Kleinjung and Wesolowski have independently proved Theorem 4.0.1, also using elliptic presentations of finite fields. One of the main differences between the present approach and the one in [65] is the proof of the correctness of the algorithms. In both cases it is a matter of showing the irreducibility of certain curves: the approach in [65] is based on the ideas in [64], while we mostly rely on a little bit of Galois theory over function fields; both approaches use some cumbersome computations and in our case these computations are mostly contained in Proposition 4.6.3 and in the Claims 4.8.2.3, 4.8.2.6, 4.8.3.2. The practical feasibility of algorithms using elliptic presentations has been studied by Joux and Pierrot in [57].

In Section 4.1 we define elliptic presentations and we prove that all finite fields of small characteristic can be embedded in a slightly larger field admitting an elliptic presentation. Section 4.2 has technical importance: given an elliptic presentation, we define a finite and small set of points on the associated elliptic curve that we call "traps" since they interfere with our algorithm. In Section 4.3 we describe the general setup of our algorithm and we explain how to pass from a factor base made of irreducible polynomials in $\mathbb{F}_q[x]$ to a factor base made of irreducible divisors on an elliptic curve $E/\mathbb{F}_q$. In Section 4.4 we give our algorithm, stated in terms of a descent procedure that is described in Section 4.5. A more precise statement about the complexity of the main algorithm is given in Theorem 4.4.4. Our descent procedure consists of two steps, presented and analysed in Section 4.5 under an assumption on the number of points of certain varieties that are used in these steps. These assumptions are proven in Section 4.8 for the first step and in Section 4.7 for the second and easier step. In Section 4.6 we prove a lemma, mainly using some Galois theory over function fields, that is useful in Sections 4.7 and 4.8.

Acknowledgements I thank René Schoof for introducing me to this research problem in 2016 and for the useful ideas that lead to substantial simplifications.

4.1 Elliptic presentations

One of the main ideas in [56] and in the original quasi-polynomial algorithm [19], is to present a field K using two subfields $\mathbb{F}_q \subsetneq \mathbb{F}_Q \subseteq K$ of order q, Q (both "small" compared to $\#K$) and an element $x_1 \in K$ generating the extension $\mathbb{F}_Q \subset K$ such that the q-th Frobenius acts on x_1 in a simple way, namely $x_1^q = f(x_1)$ for some $f \in \mathbb{F}_q(x)$ of degree at most 2. We now define a presentation based on a similar idea: describing K as $\mathbb{F}_q(x_1, y_1)$ where $\mathbb{F}_q$ is a finite field of order q "small" compared to $\#K$ and x_1, y_1 are two elements of K on which the q-th Frobenius acts in a "simple" way.

Let q be a prime power, let n be a positive integer and let K be a field of cardinality q^n. Let $\mathbb{F}_q$ be a finite field of cardinality q and let $\overline{\mathbb{F}_q}$ be its algebraic closure. Suppose there exists an elliptic curve $E/\mathbb{F}_q$ defined by a Weierstrass equation and a point $P_0 \in E(\mathbb{F}_q)$ of order n. Denoting by ϕ be the q-th Frobenius on the elliptic curve E, the map $E \to E$ given by $P \mapsto \phi(P) - P$ is surjective. Therefore there is a point $P_1 = (x_1, y_1) \in E(\overline{\mathbb{F}_q})$ such that $\phi(P_1) = P_1 + P_0$. Hence

$$(x_1^{q^i}, y_1^{q^i}) = \phi^i(P_1) = P_1 + i \cdot P_0 \quad \text{for every } i \in \mathbb{Z}\,, \tag{4.1.1}$$

implying that the field extension $\mathbb{F}_q \subset \mathbb{F}_q(x_1, y_1)$ has degree n. Hence $\mathbb{F}_q(x_1, y_1)$ is isomorphic to K. Moreover, using the addition formulas on E, we see that the q-th Frobenius acts on the pair (x_1, y_1) in a "simple" way: there are polynomials $f_1, f_2, f_3 \in \mathbb{F}_q(x, y)$ of small degree such that

$$x_1^q = f_1(x_1, y_1)/f_3(x_1, y_1)\,, \quad y_1^q = f_2(x_1, y_1)/f_3(x_1, y_1)\,.$$

With this heuristic in mind, we give the following definition.

Definition 4.1.2. Let $E/\mathbb{F}_q$ be an elliptic curve defined by a Weierstrass polynomial in $\mathbb{F}_q[x, y]$ and let P_0 be a $\mathbb{F}_q$-point on E. An $(E/\mathbb{F}_q, P_0)$-*presentation* of a finite field K is an ideal $\mathfrak{m} \subset \mathbb{F}_q[x, y]$ such that

(i) K is isomorphic to $\mathbb{F}_q[x, y]/\mathfrak{m}$ with a chosen isomorphism;

(ii) denoting $\phi\colon E \to E$ the q-th Frobenius, there exists a point $P_1 = (x_1, y_1)$ in $E(\overline{\mathbb{F}_q})$ such that $\phi(P_1) = P_1 + P_0$ and $\mathfrak{m} = \{f \in \mathbb{F}_q[x, y] : f(x_1, y_1) = 0\}$;

(iii) $q > 2$ and, under the isomorphism (i), we have $[K : \mathbb{F}_q] > 2$.

Sometimes we omit the dependence on $(E/\mathbb{F}_q, P_0)$ and we simply write "elliptic presentation". The technical hypothesis $q > 2$ is used in the proof of Claim 4.8.2.3.

Remark 4.1.3. Any elliptic presentation $\mathfrak{m}$ is a maximal ideal, since $\mathbb{F}_q[x, y]/\mathfrak{m}$ is a field.

Remark 4.1.4. If $\mathfrak{m}$ is an elliptic presentation, then the inclusion $\mathbb{F}_q[x] \to \mathbb{F}_q[x,y]$ induces an isomorphism $\mathbb{F}_q[x]/\mu \cong \mathbb{F}_q[x,y]/\mathfrak{m}$ for a certain $\mu \in \mathbb{F}_q[x]$.

Proving this is equivalent to proving that x generates the extension $\mathbb{F}_q \subset \mathbb{F}_q[x,y]/\mathfrak{m}$. Using the notation in Definition 4.1.2, this is equivalent to proving that $\mathbb{F}_q(x_1)$ is equal to $\mathbb{F}_q(x_1,y_1)$. If, for the sake of contradiction, this is not the case, then the Weierstrass equation satisfied by x_1 and y_1 implies that the extension $\mathbb{F}_q(x_1) \subset \mathbb{F}_q(x_1,y_1)$ has degree 2, hence $[\mathbb{F}_q(x_1) : \mathbb{F}_q] = \frac{n}{2}$, where $n := [\mathbb{F}_q(x_1,y_1) : \mathbb{F}_q] = [K : \mathbb{F}_q]$. Using Equation 4.1.1, we deduce that

$$x(P_1) = x_1 = x_1^{q^{n/2}} = x(\phi^{n/2}P_1) = x(P_1 + \tfrac{n}{2}P_0) \quad \Longrightarrow \quad P_1 + \tfrac{n}{2}P_0 = \pm P_1\,.$$

Since, by Equation 4.1.1, the order of P_0 is equal to n, we have $P_1 + \frac{n}{2}P_0 = -P_1$, implying that $2P_1$ lies $E(\mathbb{F}_q)$. Therefore P_0 has order 2, contradicting $n = [K : \mathbb{F}_q] > 2$ in (iii).

We now show that any finite field K of small characteristic can be embedded in a "slightly larger" field admitting an elliptic presentation with q "small" compared to $\#K$.

Proposition 4.1.5. *For any finite field K of small characteristic there exists an extension $K \subset K'$ having a elliptic presentation $\mathfrak{m} \subset \mathbb{F}_q[x,y]$ of K' such that*

$$\log(\#K') \leq 13\log(\#K)\log\log(\#K) \quad \textit{and} \quad q \leq \log(\#K')^4\,.$$

Moreover such K' and its presentation can be computed in polynomial time in $\log(\#K)$.

Proof. Let $\#K = p^n$ for a prime p and an integer $n > p$. Put $k_0 := \lceil \log_p n \rceil$ and $q := p^{2k_0}$, so that n has a multiple n_1 in the interval $[q - \sqrt{q} + 1, q + 1]$. If $n_1 \equiv 1 \bmod p$ we define $n_2 := n_1 + n$, otherwise we define $n_2 := n_1$. Since n_2 in an integer contained in the Hasse interval $[q - 2\sqrt{q} + 1; q + 2\sqrt{q} + 1]$ that is not congruent to 1 modulo p, by [90, Theorems 1a, 3] we can choose an elliptic curve $E/\mathbb{F}_q$ whose group of rational points $E(\mathbb{F}_q)$ is cyclic of order n_2. Since n divides n_2, we can choose a point $P_0 \in E(\mathbb{F}_q)$ of order n.

We can assume E is defined by a Weierstrass polynomial. Since the map $P \mapsto \phi(P) - P$ is surjective, we can choose a point $(x_1,y_1) = P_1 \in E(\overline{\mathbb{F}_q})$ such that $\phi(P_1) = P_1 + P_0$. We define

$$\mathfrak{m} := \{f \in \mathbb{F}_q[x,y] : f(x_1,y_1) = 0\}\,, \quad K' := \mathbb{F}_q(x_1,y_1) \subset \overline{\mathbb{F}_q}\,.$$

The map $\mathbb{F}_q[x,y] \to K$ sending $x \mapsto x_1, y \mapsto y_1$ induces an isomorphism $\mathbb{F}_q[x,y]/\mathfrak{m} \cong K'$. To prove that $\mathfrak{m}$ is an elliptic presentation of K' it remains to show that both q and $[K' : \mathbb{F}_q]$ are larger than 2: in the first case it is true because $k_0 > 1$, in the second case it is true because, by (4.1.1), the degree of $\mathbb{F}_q \subset K'$ is equal to the order n of P_0, and $n > p \geq 2$.

Since $[K' : \mathbb{F}_q] = n$ divides $[K' : \mathbb{F}_p]$, the field K' has a subfield with p^n elements. In other words K can be embedded in K'. Moreover we have

$$\log(\#K') = n \log q < 2n \log(p)(\log_p(n)+1) \leq 4 \log(p) \log(n) \leq 13 \log(\#K) \log\log(\#K),$$
$$2 < p^2 \leq q = p^{2\lceil \log_p n \rceil} < p^{2+2\log_p n} = (pn)^2 \leq n^4 < \log(q^n)^4 = \log(\#K')^4 .$$

We now prove that it is possible to compute such K' and $\mathfrak{m}$ in polynomial time in $\log(\#K)$. We describe a procedure following the abstract part of the proof. Computing k_0, q, n_1 is easy. We can construct a field $\mathbb{F}_q$ by testing the primality of all polynomials of degree $2k_0$ over $\mathbb{F}_p$ until an irreducible ν is found and define $\mathbb{F}_q = \mathbb{F}_p[T]/\nu$; since there are less than n^2 polynomials of this type, this takes polynomial time. Similarly we can find an elliptic curve E with an $\mathbb{F}_q$-point P_0 of order n in polynomial time, by listing all possible Weierstrass equations (there are less than q^6), testing if they define an elliptic curve and, when they do, enumerate all their $\mathbb{F}_q$-points. Then, using the addition formula on E, we write down the ideal $I \subset \mathbb{F}_q[x, y]$ whose vanishing locus inside $\mathbb{A}^2$ is the set of points $P = (x, y) \in E(\overline{\mathbb{F}_q})$ such that $\phi(P) = P + P_0$. As we showed before, the set of such points is non-empty, hence I is a proper ideal and we can find a maximal ideal $\mathfrak{m}$ containing I. We don't need general algorithms for primary decomposition since we can take $\mathfrak{m} = (\mu(x), \lambda(x, y))$, with (μ) being an irreducible factor of the generator of the ideal $J \cap \mathbb{F}_q[x]$ and $\lambda(x, y)$ being an irreducible factor of the image of the Weierstrass equation of E inside $(\mathbb{F}_q[x]/\mu)[y]$. Since the Weiestrass polynomial is monic in y, we can assume that λ is monic in y too. Hence there is a point $P_1 = (x_1, y_1)$ in the vanishing locus of $(\mu(x), \lambda(x, y)) = \mathfrak{m}$. Since $\mathfrak{m}$ contains I, the point P_1 lies on E and satisfies $\phi(P_1) = P_1 + P_0$. The maximality of $\mathfrak{m}$ implies that $\mathbb{F}_q[x, y](\mathfrak{m}) = \mathbb{F}_q(x_1, y_1) = K'$. Hence $\mathfrak{m}$ is the elliptic presentation we want. □

Notation 4.1.6. For the rest of the article $\mathbb{F}_q$ is a finite field with q elements, $\overline{\mathbb{F}_q}$ is its algebraic closure, K is a finite extension of $\mathbb{F}_q$, the ideal $\mathfrak{m} \subset \mathbb{F}_q[x, y]$ is a $(E/\mathbb{F}_q, P_0)$-presentation of K, the map $\phi\colon E \to E$ is the q-th Frobenius and $P_1 = (x_1, y_1) \in E(\overline{\mathbb{F}_q})$ is a point such that $\mathfrak{m} = \{f \in \mathbb{F}_q[x, y] : f(x_1, y_1) = 0\}$. By O_E we denote the neutral element of $E(\mathbb{F}_q)$.

4.2 Traps

As first pointed out in [27], there are certain polynomials, called "traps" for which the descent procedure in [19] does not work. In [19] such traps are dealt with differently than the other polynomials. In [49] the notion of "trap" is extended: it includes not only polynomials for which the descent procedure is proven not to work, but also polynomials

for which the authors do not give proof of the descent's correctness. In [49] traps are avoided by the algorithm.

We describe a descent procedure stated in terms of points and divisors on E and there are certain points in $E(\overline{\mathbb{F}_q})$ that play the role of "traps", as in [49]. The definition of this subset of $E(\overline{\mathbb{F}_q})$ is rather cumbersome, but it is easy to deduce that we have less than $15q^4$ traps. In particular, in contrast to [49], we can include them in the factor base.

Definition 4.2.1. A point $P \in E(\overline{\mathbb{F}_q})$ is a *trap* if it satisfies one of the following conditions:

$$2P = 0\,, \quad \text{or} \quad (2\phi - \mathrm{Id})(\phi^2 - \phi + \mathrm{Id})(P) = P_0\,, \quad \text{or} \quad (2\phi - \mathrm{Id})(\phi + \mathrm{Id})(P) = 2P_0$$
$$\text{or } (\phi^4 - \mathrm{Id})(P) = 4P_0\,, \quad \text{or } 2(\phi^3 - \mathrm{Id})(P) = 6P_0\,, \quad \text{or} \quad (2\phi + \mathrm{Id})(\phi - \mathrm{Id})(P) = 2P_0\,.$$

We explain why these points interfere with our strategy of proof in (4.7.2.2) and at the beginning of the proof of Claim 4.8.2.3.

4.3 Divisors and discrete logarithm

For us a divisor on E is a formal sum

$$D = \sum_{P \in E(\overline{\mathbb{F}_q})} n_P P\,,$$

where the n_P's are integers and $n_P = 0$ for all but a finite number of P's. The Galois group of $\mathbb{F}_q$ acts on the group of divisors by the formula

$$\sigma\left(\sum_{P \in E(\overline{\mathbb{F}_q})} n_P P\right) = \sum_{P \in E(\overline{\mathbb{F}_q})} n_P\, \sigma(P)\,.$$

For any algebraic extension $\mathbb{F}_q \subset k$ we define the set of divisors *defined over* k, denoted $\mathrm{Div}_k(E)$, to be the set of divisors D such that $\sigma D = D$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}_q}/k)$. We say that a divisor is *irreducible over* k if it is the sum, with multiplicity 1, of all the $\mathrm{Gal}(\overline{\mathbb{F}_q}/k)$-conjugates of some point $P \in E(\overline{\mathbb{F}_q})$. Every divisor defined over k is a $\mathbb{Z}$-combination of irreducible divisors over k. We refer to [97, Chapter 2] for the definitions of principal divisor and support of a divisor.

We need two quantities to describe the "complexity" of a divisor. The first one is the *absolute degree* of a divisor, defined as as

$$\mathrm{absdeg}\left(\sum_{P \in E(\overline{\mathbb{F}_q})} n_P(P)\right) := \sum_{P \in E(\overline{\mathbb{F}_q})} |n_P|\,.$$

The second quantity is analogous to the degree of the splitting field of a polynomial, but we decide to "ignore" trap points. We say that a point is *good* if it is not a trap point, we say that a divisor on E is *good* if it is supported outside the set of traps. Given an algebraic extension $\mathbb{F}_q \subset k$ and a divisor $D \in \mathrm{Div}_k(E)$, there is a unique good divisor D^{good}, defined over k, such that $D - D^{\mathrm{good}}$ is supported on the set of trap points. We define the *essential degree of D over k* to be the least common multiple of the degrees of the irreducible divisors appearing in the support of D^{good}. In other words, if we denote as $k(D^{\mathrm{good}})$ the minimal algebraic extension $\widetilde{k} \supset k$ such that the support of D is contained in $E(\widetilde{k})$, then

$$\mathrm{essdeg}_k(D) := [k(D^{\mathrm{good}}) : k] .$$

If $D^{\mathrm{good}} = 0$ we take $\mathrm{essdeg}_k(D) = 1$.

Now consider the discrete logarithm problem in a field having an elliptic presentation $\mathfrak{m}$. First of all, if q is small compared to $\#K$, for example $q \leq (\log K)^4$ as in Proposition 4.1.5, and if we are able to compute discrete logarithms in $K^\times/\mathbb{F}_q^\times$ in quasi-polynomial time, then we can also compute discrete logarithms in $K^\times$ in quasi-polynomial time. Hence in the rest of the article we are concerned with computing discrete logarithms in $K^\times/\mathbb{F}_q^\times$.

Denoting $\mathbb{F}_q[x,y]_{\mathfrak{m}}$ the localization of $\mathbb{F}_q[x,y]$ at the maximal ideal $\mathfrak{m}$, we have

$$K \cong \mathbb{F}_q[x,y]/\mathfrak{m} \cong \mathbb{F}_q[x,y]_{\mathfrak{m}}/\mathfrak{m}_{\mathfrak{m}} .$$

An element f of $(\mathbb{F}_q[x,y]_{\mathfrak{m}})^\times$ defines a rational function on E which is defined over $\mathbb{F}_q$ and regular and non-vanishing in P_1. We represent elements in $K^\times/\mathbb{F}_q^\times$ with elements of $\mathbb{F}_q(E)$ that are regular and non-vanishing on P_1.

Let g, h be elements of $\mathbb{F}_q(E)$ both regular and non-vanishing on P_1 and let us suppose that g generates the group $K^\times/\mathbb{F}_q^\times$. Then the logarithm of h in base g is a well defined integer modulo $\frac{\#K-1}{q-1}$ that we denote $\log_{\mathfrak{m},g}(h)$ or simply $\log h$. Since we are working modulo $\mathbb{F}_q^\times$, the logarithm of h only depends on the divisor of zeroes and poles of h: if $h' \in \mathbb{F}_q(E)$ satisfies $\mathrm{div}(h) = \mathrm{div}(h')$, then $h/h' \in \mathbb{F}_q^\times$ and consequently $\log(h) = \log(h')$. Hence, putting

$$\log(\mathrm{div}(h)) := \log(h) ,$$

we define the discrete logarithm as homomorphism whose domain is the subgroup of $\mathrm{Div}_{\mathbb{F}_q}(E)$ made of principal divisors, supported outside P_1 and whose image is $\mathbb{Z}/(\frac{\#K-1}{q-1})\mathbb{Z}$. The kernel of this morphism is a subgroup of $\mathrm{Div}_{\mathbb{F}_q}(E)$, hence it defines the following equivalence relation on $\mathrm{Div}_{\mathbb{F}_q}(E)$

$$\begin{aligned} D_1 \sim D_2 &\iff D_1 - D_2 \in \mathrm{Ker}(\log) \\ &\iff \exists f \in \mathbb{F}_q(E) \text{ such that } f(P_1) = 1 \text{ and } \mathrm{div}(f) = D_1 - D_2 . \end{aligned} \tag{4.3.1}$$

We notice that this equivalence relation does not depend on g and that, given rational functions $h_1, h_2 \in \mathbb{F}_q(E)$ regular and non-vanishing on P_1, we have $\log h_1 = \log h_2$ if and only if $\mathrm{div}(h_1) \sim \mathrm{div}(h_2)$. Motivated by this, for all divisors $D_1, D_2 \in \mathrm{Div}_{\mathbb{F}_q}(E)$ we use the notation

$$\log_{\mathfrak{m}} D_1 = \log_{\mathfrak{m}} D_2 \iff D_1 \sim D_2 \,.$$

Notice that we do not define the expression $\log_{\mathfrak{m}}(D)$ or $\log_{\mathfrak{m},g}(D)$ for any D in $\mathrm{Div}_{\mathbb{F}_q}(E)$, since the function log might not extend to a morphism $\mathrm{Div}_{\mathbb{F}_q}(E) \to \mathbb{Z}/(\frac{\#K-1}{q-1})\mathbb{Z}$. In our algorithm we use the equivalence relation (4.3.1) to recover equalities of the form $\log h_1 = \log h_2$.

4.4 The main algorithm

As in [49] our algorithm is based on a descent procedure, stated in terms of divisors on E.

Theorem 4.4.1. *There exists an algorithm, described in the proof, that takes as input an $(E/\mathbb{F}_q, P_0)$-presentation $\mathfrak{m}$ and a divisor $D \in \mathrm{Div}_{\mathbb{F}_q}(E)$ such that $\mathrm{essdeg}_{\mathbb{F}_q}(D) = 2^m$ for some integer $m \geq 7$ and computes a divisor $D' \in \mathrm{Div}_{\mathbb{F}_q}(E)$ such that*

$$\log_{\mathfrak{m}} D = \log_{\mathfrak{m}} D' \,, \quad (\mathrm{essdeg}_{\mathbb{F}_q} D') \mid 2^{m-1} \,, \quad \mathrm{absdeg}(D') \leq 4q^2 \mathrm{absdeg} D \,.$$

This algorithm is probabilistic and runs in expected polynomial time in $q\mathrm{absdeg}(D)$.

Applying repeatedly the algorithm of the above theorem we deduce the following result.

Corollary 4.4.2. *There exists an algorithm, described in the proof, that takes as input an $(E/\mathbb{F}_q, P_0)$-presentation and a divisor $D \in \mathrm{Div}_{\mathbb{F}_q}(E)$ such that $\mathrm{essdeg}_{\mathbb{F}_q} D = 2^m$ for some integer m and computes a divisor $D' \in \mathrm{Div}_{\mathbb{F}_q}(E)$ such that*

$$\log_{\mathfrak{m}} D = \log_{\mathfrak{m}} D' \,, \quad \mathrm{essdeg}_{\mathbb{F}_q} D' \mid 64 \,, \quad \mathrm{absdeg}(D') \leq (2q)^{2m} \mathrm{absdeg}(D) \,.$$

This algorithm is probabilistic and runs in expected polynomial time in $q^m\mathrm{absdeg}(D)$.

The algorithm in [49] is based on the descent procedure [49, Theorem 3]. Using the same ideas we use the descent procedure of the last corollary to describe our main algorithm, which computes discrete logarithms in finite fields with an elliptic presentation.

The idea is setting up an index calculus with factor base the irreducible divisors whose essential degree divides 64. To collect relations we use a "zig-zag descent": for every $f = g^a h^b$, we first use the polynomial μ determined in Remark 4.1.4 to find

$f' \equiv f \bmod \mathfrak{m}$ such that the essential degree of $\mathrm{div}(f')$ is a power of 2, and we then apply the descent procedure to express $\log(f) = \log(f')$ as the logarithm of sums of elements in the factor base.

Main Algorithm Input: an $(E/\mathbb{F}_q, P_0)$-epresentation $\mathfrak{m} \subset \mathbb{F}_q[x,y]$ of a field K and two polynomials $g, h \in \mathbb{F}_q[x,y] \setminus \mathfrak{m}$ such that g generates the group $(\mathbb{F}_q[x,y]/\mathfrak{m})^\times / \mathbb{F}_q^\times$.

Output: an integer z such that

$$g^z \equiv \gamma \cdot h \pmod{\mathfrak{m}} \quad \text{for some } \gamma \in \mathbb{F}_q^\times ,$$

which is equivalent to $g^z = h$ in the group $K^\times/\mathbb{F}_q^\times$.

1. *Preparation:* Compute the monic polynomial $\mu \in \mathbb{F}_q[x]$ generating the ideal $\mathfrak{m} \cap \mathbb{F}_q[x]$. Compute polynomials $\tilde{g}, \tilde{h} \in \mathbb{F}_q[x]$ such that $\tilde{g} \equiv g$ and $\tilde{h} \equiv h$ modulo $\mathfrak{m}$. Put $c := \#E(\mathbb{F}_q)$, $n := \deg \mu$ and $m := \lceil \log n \rceil + 3$.

2. *Factor base:* List the irreducible divisors $D_1, \ldots, D_t \in \mathrm{Div}_{\mathbb{F}_q}(E)$ that do not contain P_1 and either have degree dividing 64 or are supported on the trap points.

3. *Collecting relations*: For $j = 1, \ldots, t+1$ do the following:

   Pick random integers $\alpha_j, \beta_j \in \{1, \ldots, \frac{q^n-1}{q-1}\}$ and compute $\tilde{g}^{\alpha_j}\tilde{h}^{\beta_j}$. Pick random polynomials $f(x)$ of degree 2^m such that $f \equiv \tilde{g}^{\alpha_j}\tilde{h}^{\beta_j} \pmod{\mu}$ until f is irreducible. Apply the descent procedure in Corollary 4.4.2 to find $v_j = (v_{j,1}, \ldots, v_{j,t}) \in \mathbb{Z}^t$ such that

   $$\log_{\mathfrak{m}}(\mathrm{div}(f)) = \log_{\mathfrak{m}}(v_{j,1}D_1 + \ldots + v_{j,t}D_t) .$$

4. *Linear algebra*: Compute $d_1, \ldots, d_{t+1} \in \mathbb{Z}$ such that $\gcd(d_1, \ldots, d_{t+1}) = 1$ and

   $$d_1 v_1 + \ldots + d_{t+1} v_{t+1} \equiv (0, \ldots, 0) \pmod{\tfrac{q^n-1}{q-1}c} .$$

   Put $a := d_1\alpha_1 + \ldots + d_{t+1}\alpha_{t+1}$ and $b := d_1\beta_1 + \ldots + d_{t+1}\beta_{t+1}$.

5. *Finished?*: If b is not invertible modulo $\frac{q^n-1}{q-1}$ go back to step 3, otherwise output

   $$z := -ab^{-1} \left(\bmod \tfrac{q^n-1}{q-1}\right)$$

Analysis of the main algorithm We first prove, assuming Theorem 4.4.1, that the algorithm, when it terminates, gives correct output. First of all we notice that, as explained in Remark 4.1.4, the polynomials $\mu, \tilde{g}$ and $\tilde{h}$ exist and that $\tilde{g}$ and $\tilde{h}$ define the same element as g, respectively h, in $K \cong \mathbb{F}_q[x,y]/\mathfrak{m}$. Let d_j, α_j, β_j and v_j be the

integers and vectors of integers stored at the beginning of the fourth step the last time it is executed. By definition of d_j, we have

$$\sum_{j=1}^{t+1}\sum_{i=1}^{t} d_j v_{j,i} D_i = \tfrac{q^n-1}{q-1} c \cdot D\,,$$

for a certain $D \in \mathrm{Div}_{\mathbb{F}_q}(E)$. The divisor cD is principal because $c = \#\mathrm{Pic}^0(E/\mathbb{F}_q)$ and, since for all j the divisor $\sum_i v_{j,i} D_i$ is principal, D has degree 0. Choosing λ in $\mathbb{F}_q(E)$ such that $\mathrm{div}(\lambda) = cD$, we have

$$\sum_{j=1}^{t+1}\sum_{i=1}^{t} d_j v_{j,i} D_i = \mathrm{div}(\lambda^{\frac{q^n-1}{q-1}})\,. \tag{4.4.3}$$

Writing log for $\log_{\mathfrak{m},g}$, by definition of v_j we have

$$\log(g^{\alpha_j} h^{\beta_j}) = \log\left(\sum_{i=1}^{t} v_{j,i} D_i\right)\,.$$

This, together with Equation (4.4.3), imply the following equalities in $\mathbb{Z}/\frac{q^n-1}{q-1}\mathbb{Z}$

$$\begin{aligned} a + b\log(h) &= \sum_{j=1}^{t+1} d_j(\alpha_j + \beta_j \log(h)) = \sum_{j=1}^{t+1} d_j \log(g^{\alpha_j} h^{\beta_j}) = \sum_{j=1}^{t+1} d_j \log\left(\sum_{i=1}^{t} v_{j,i} D_i\right) \\ &= \log\left(\sum_{j=1}^{t+1}\sum_{i=1}^{t} d_j v_{j,i} D_i\right) = \log\left(\mathrm{div}(\lambda^{\frac{q^n-1}{q-1}})\right) = \tfrac{q^n-1}{q-1}\log(\lambda) = 0\,, \end{aligned}$$

implying that the output z of the algorithm is correct.

We now estimate the running time step by step. The first step can be performed with easy Groebner basis computations. Now the second step. We represent irreducible divisors D not supported on O_E in the following way: either D is the vanishing locus of a prime ideal $(a(x), W(x,y))$ with a monic and irreducible and W the Weierstrass polynomial defining E, or D is the vanishing locus of a prime ideal $(a(x), y - b(x))$ for some polynomials $a, b \in \mathbb{F}_q[x]$ and a monic irreducible; in the first case $\deg D = 2\deg a$, in the second case $\deg D = \deg a$. We can list all the irreducible divisors with degree dividing 64 by listing all monic irreducible polynomials $\mu_1, \ldots, \mu_r \in \mathbb{F}_q[x]$ of degree dividing 64 and, for each i compute the prime ideals containing (μ_i, W), which amounts to factoring W as a polynomial in y, considered over the field $\mathbb{F}_q[x]/\mu_i$. Listing all the divisors supported on the trap points can be done case by case. For example we can list the irreducible divisors supported on the set $S := \{P \in E(\overline{\mathbb{F}_q}) : \phi^4(P) - P = 4P_0\}$ by writing down, with the addition formula on E, an ideal $J \subset \mathbb{F}_q[x,y]$ whose vanishing

locus is $S \subset \mathbb{A}^2(\overline{\mathbb{F}}_q)$ and computing all the prime ideals containing J. The divisor O_E appears among $D_1, \ldots, D_s$ because O_E is a trap point. Since there are q^{64} monic polynomials of degree 64 and at most $15q^4$ trap points and since, using [15], factoring a polynomial of degree d in $\mathbb{F}_q[x]$ takes on average $O(\log(q)d^3)$ operations, the second step takes polynomial time in q. Moreover, we have $t \leq 2q^{64}$.

Now the third step. By [100, Theorem 5.1], if $f(x)$ is a random polynomial of degree 2^m congruent to $\tilde{g}^{\alpha_j}\tilde{h}^{\beta_j}$ modulo μ, then the probability of f being irreducible is at least 2^{-m-1}. Therefore finding a good f requires on average $O(2^m) = O(n)$ primality tests, hence $O(n^4 \log q)$ operations. By assumption finding the vector v_j requires polynomial time in $q^m 2^{m+1}$. We deduce that the third step has probabilistic complexity $tq^{O(\log n)} = q^{O(\log n)}$.

The fourth step can be can be performed by computing a Hermite normal form of the matrix having the v_j's as columns. Since $c \leq q+2\sqrt{q}+1$, the entries of the v_j are at most as big as $4q^{n+1}$. Therefore the fourth step is polynomial in $t\log(q^n)$, hence polynomial in n.

The last step only requires arithmetic modulo $(q^n-1)/(q-1)$.

To understand how many times each step is repeated on average, we need to estimate the probability that, in the last step, b is invertible modulo $(q^n-1)/(q-1)$ and to do so we look at the quantities in the algorithms as if they were random variables. The vector $(d_1, \ldots, d_{t+1})$ only depends on the elements $h^{\alpha_j}g^{\beta_j}$'s and on the randomness contained in the descent procedure and in step 2. Since the α_j's and β_j's are independent variables and since g is a generator, we deduce that the vector $(\beta_1, \ldots, \beta_{t+1})$ is independent of $(g^{\alpha_1}h^{\beta_1}, \ldots, g^{\alpha_{t+1}}h^{\beta_{t*1}})$, hence also independent of the vector $(d_1, \ldots, d_{t+1})$. Since $(\beta_1, \ldots, \beta_{t+1})$ takes on all values in $\{0, \ldots, q^n - 1\}^{t+1}$ with the same probability and $\gcd(d_1, \ldots, d_{t+1}) = 1$, then

$$b = d_1\beta_1 + \ldots d_{t+1}\beta_{t+1}$$

takes all values in $\mathbb{Z}/(q^n - 1)\mathbb{Z}$ with the same probability. Hence

$$\left(\text{probability that } b \text{ is coprime to } \tfrac{q^n-1}{q-1}\right) = \phi\left(\tfrac{q^n-1}{q-1}\right) / \tfrac{q^n-1}{q-1} \gg \frac{1}{\log\log q^n}$$

When running the algorithm, the first and the second step get executed once and the other steps get executed the same number of times, say r, whose expected value is the inverse of the above probability. Since r is $O(\log\log(q^n))$ on average and each step has average complexity at most $q^{O(\log n)}$, the average complexity of the algorithm is $O(q^{O(\log n)})$. Hence, assuming Theorem 4.4.1 we have proved the following theorem.

Theorem 4.4.4. *The above Main Algorithm solves the discrete logarithm problem in the group $K^\times/\mathbb{F}_q^\times$ for all finite fields K having an elliptic presentation $\mathfrak{m} \subset \mathbb{F}_q[x, y]$. It runs in expected time $q^{O(\log[K:\mathbb{F}_q])}$.*

Theorem 4.0.1 follows from Theorem 4.4.4 and Proposition 4.1.5: the latter states that any finite field of small characteristic K can be embedded in a slightly larger field K' having an elliptic presentation $\mathfrak{m} \subset \mathbb{F}_q[x,y]$ such that $q \leq \log(\#K')^4$ and Theorem 4.0.1 implies that the discrete logarithm problem is at most quasi-polynomial for such a K'. Moreover, by Proposition 4.1.5, such a K', together with its elliptic presentation, can be found in polynomial time in $\log(\#K)$, by [66] we can compute an embedding $K \hookrightarrow K'$ in polynomial time in $\log(\#K)$ and by [89, Theorem 15] a random element $g' \in K'$ has probability $\phi(\#K')/\#K' \gg 1/\log\log \#K'$ of being a generator of K': hence, given elements $g, h \in K$, we can compute $\log_g(h)$ by embedding K inside K' and trying to compute the pair $(\log_{g'} g, \log_{g'} h)$ for different random values of $g' \in K'$.

Proposition 4.1.5 is proven, while Theorem 4.4.4 relies on the the existence of a descent procedure as described in Theorem 4.4.1. In the rest of the article, we describe this descent procedure.

4.5 Strategy of proof of Theorem 4.4.1: the descent procedure

Since the descent is trivial for divisors supported on the trap points, it is enough to prove Theorem 4.4.1 and describe the descent procedure for divisors D that are good and irreducible over $\mathbb{F}_q$. In other words, if we write $2^m = 4l$, we can suppose that

$$D = Q + \sigma Q + \ldots + \sigma^{4l-1} Q\,,$$

where Q is a good point on E such that $[\mathbb{F}_q(Q) : \mathbb{F}_q] = 4l = 2^m$ and σ is a generator of $\mathrm{Gal}(\mathbb{F}_q(Q)/\mathbb{F}_q)$. Let k be the unique subfield of $\mathbb{F}_q(Q)$ such that $[k : \mathbb{F}_q] = l$ and let us define

$$\tilde{D} := Q + \sigma^l Q + \sigma^{2l} Q + \sigma^{3l} Q \quad \in \mathrm{Div}_k(E)\,.$$

We can do a sort of "base change to k" and work with $\tilde{D}$. Suppose we have an algorithm to find a divisor $\tilde{D}' \in \mathrm{Div}_k(E)$ such that

$$\mathrm{absdeg}\tilde{D}' \leq 16q^2\,, \quad \mathrm{essdeg}_k \tilde{D}' \mid 2\,,$$

and a function $g \in k(E)$ such that

$$\mathrm{div}(g) = \tilde{D} - \tilde{D}'\,, \quad g(\tau(P_1)) = 1 \quad \text{for all } \tau \in \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)\,. \tag{4.5.1}$$

Then the divisor

$$D' := \tilde{D}' + \sigma(\tilde{D}') + \ldots \sigma^{l-1}(\tilde{D}')\,,$$

satisfies the conditions in Theorem 4.4.1: the absolute and essential degree of D' are easy to estimate and we have $\log_{\mathfrak{m}} D = \log_{\mathfrak{m}} D'$ because the rational function $f := gg^{\sigma} \cdots g^{\sigma^{l-1}}$ satisfies $f(P_1) = 1$ and $\mathrm{div}(f) = D - D'$.

Hence, in order to prove Theorem 4.4.1, it is enough to describe a probabilistic algorithm that takes k and $\tilde{D}$ as input and, in expected polynomial time in ql, computes a good divisor $\tilde{D}'$ with the properties above. We do it in two steps and we replace the second part of Equation (4.5.1) with a stronger requirement: we ask that $g(P) = 1$ for all the points $P \in E(\overline{\mathbb{F}_q})$ such that $\phi(P) = P + P_0$. Moreover, the hypothesis that l is a power of 2 is not necessary.

Proposition 4.5.2. *There is an algorithm, described in the proof, with the following property*

- *it takes as input an $(E/\mathbb{F}_q, P_0)$-presentation, a finite field extension $\mathbb{F}_q \subset k$ of degree $l \geq 80$ and a divisor $D \in \mathrm{Div}_k(E)$ such that $\mathrm{essdeg}_k D = 4$*
- *it computes a rational function $g \in k(E)$ and a divisor $D' = D_1 + D_2 \in \mathrm{Div}_k(E)$ such that*

$$D - D' = \mathrm{div}(g)\,, \quad g(P) = 1 \text{ for all } P \in E(\overline{\mathbb{F}_q}) \text{ such that } \phi(P) = P + P_0\,,$$
$$\mathrm{essdeg}_k(D_1) \mid 3\,, \quad \mathrm{essdeg}_k(D_2) \mid 2\,, \quad \mathrm{absdeg} D_1 + \mathrm{absdeg} D_2 \leq 2q\mathrm{absdeg} D\,;$$

- *it is probabilistic and runs in expected polynomial time in $q \cdot \log(\#k) \cdot \mathrm{absdeg}(D)$.*

Proposition 4.5.3. *There is an algorithm, described in the proof, with the following property*

- *it takes as input an $(E/\mathbb{F}_q, P_0)$-presentation, an extension of finite fields $\mathbb{F}_q \subset k$ of degree at least 80 and a divisor $D \in \mathrm{Div}_k(E)$ such that $\mathrm{essdeg}_k D = 3$;*
- *it computes a rational function $g \in k(E)$ and a divisor $D' \in \mathrm{Div}_k(E)$ such that*

$$D - D' = \mathrm{div}(g)\,, \quad g(P) = 1 \text{ for all } P \in E(\overline{\mathbb{F}_q}) \text{ such that } \phi(P) = P + P_0\,,$$
$$\mathrm{essdeg}_k(D') \mid 2\,, \quad \mathrm{absdeg}(D') \leq 2q\mathrm{absdeg}(D)\,;$$

- *it is probabilistic and runs in expected polynomial time in $q \cdot \log(\#k) \cdot \mathrm{absdeg}(D)$.*

We now describe our strategy to prove the above two propositions. Let $D \in \mathrm{Div}_k(E)$ be a divisor such that $\epsilon := \mathrm{essdeg}_k(D)$ is either equal to 3 (the case of Proposition 4.5.3) or 4 (the case of Proposition 4.5.2). Let x, y be the usual coordinates on E and let $h \to h^{\phi}$ be the automorphism of $k(E)$ such that $x^{\phi} = x$, $y^{\phi} = y$ and $\alpha^{\phi} = \alpha^q$ for all

$\alpha \in k$. As before we can suppose that D is good and irreducible over k. In other words, we suppose

$$D = Q + \ldots + \sigma^{\varepsilon-1}Q\,,$$

where Q is a good point on E defined over an extension of k of degree ε and σ is a generator of $\mathrm{Gal}(k(Q)/k)$. For every point $P \in E(\overline{\mathbb{F}_q})$ such that $\phi(P) = P + P_0$ and for every function $f \in k(E)$ regular on P we have

$$f(P)^q = f^\phi(\phi(P)) = f^\phi(P + P_0) = (f^\phi \circ \tau_{P_0})(P)\,, \tag{4.5.4}$$

where τ_{P_0} is the translation by P_0 on E. Hence, for any choice of $a, b, c, d \in k$ such that $cf^{q+1}+df^q+af+b$ does not vanish on P, we have

$$\frac{(cf+d)(f^\phi \circ \tau_{P_0}) + af + b}{cf^{q+1} + df^q + af + b}(P) = 1\,.$$

Hence we look for a function g as in Propositions 4.5.2 or 4.5.3 having the shape

$$g = \frac{(cf+d)(f^\phi \circ \tau_{P_0}) + af + b}{cf^{q+1} + df^q + af + b}\,, \tag{4.5.5}$$

for some $a, b, c, d \in k$ and $f \in k(E)$. Heuristically, the advantage of such a g, is that, if f has few poles, then the numerator in the above expression also has few poles and the denominator has a probability about $1/q^3$ of splitting into linear polynomials in f.

We now look for conditions on f and a, b, c, d implying that the function g and the divisor

$$D' := D - \mathrm{div}(g)\,, \tag{4.5.6}$$

have the desired properties. If P is a pole of g, then P is either a pole of f, a pole of $f^\phi \circ \tau_{P_0}$ or a zero of $cf^{q+1}+df^q+af+b$. Since all poles P of g appear in the support of D', we want all these poles to satisfy the inequality $[k(P) : k] \leq \varepsilon - 1$. This happens if the following conditions are satisfied:

(I) the function f has at most $\varepsilon-1$ poles counted with multiplicity;

(II) the polynomial $cT^{q+1} + dT^q + aT + b$ splits into linear factors in $k[T]$.

We want Q and all its conjugates to be zeroes of g. If the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ has rank 0 or 1, then $g = (a'f^\phi+b')/(a'f^q+b')$ for some $a', b' \in k$ and this, together with condition (I), prevents Q from being a zero of g. We deduce that the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ must be invertible. Moreover we notice that the definition of g only depends on the class of $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\mathrm{PGL}_2(k)$. Assuming (I) and (II), the point Q is neither a pole of f nor a zero of the denominator in (4.5.5). Hence Q and all its conjugates are zeroes of g if and only if they are zeroes of

the numerator of (4.5.5). Assuming (I) and (II), the function $cf+d$ never vanishes on Q or its conjugates. Hence, using the natural action of PGL_2 on $\mathbb{P}^1$, we see that Q and its conjugates are zeroes of g if and only if

(III) $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot f(\sigma^i Q) = -f^{\phi}(\sigma^i Q + P_0) \quad$ for $i = 0, 1, \ldots, \varepsilon-1$.

Assuming (I), the numerator of 4.5.5 has at most $2(\varepsilon-1)$ poles and $2(\varepsilon-1)$ zeroes counted with multiplicity. Assuming also (III), the numerator of 4.5.5 has at most $\varepsilon-2$ zeroes that are different from $\sigma^i Q$ and this set of points is stable under the action of $\mathrm{Gal}(\overline{k}/k)$. We deduce that all the zeros $P \neq \sigma^i Q$ of g satisfy the inequality $[k(P) : k] \leq \epsilon-1$. Hence the same inequality is satisfied by all the points in the support of D' . As noticed when defining g, we want that

(IV) for every point P on E such that $\phi(P) = P + P_0$, the function f is regular on P and $cf^{q+1}+df^q+af+b$ does not vanish on P.

Condition (I) implies that $\mathrm{absdeg}(D')$ is at most $2q\epsilon$.

We showed that the conditions (I), (II), (III), (IV) imply that the function g in (4.5.5) and the divisor $D' = D-\mathrm{div}(g)$ satisfy the requirements of Proposition 4.5.2 or Proposition 4.5.3.

Remark 4.5.7. If $Q \notin \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \cdot P_1$ is a point such that $\phi(Q) = Q + P_0$, then Equation 4.5.4 implies that conditions (III) and (IV) exclude each other. This explains why such points Q create problems to our strategy and need to be marked as *traps*.

In Section 4.7 and Section 4.8 we prove that there are many such pairs $(f, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right))$ and we give a procedure to find them when $\varepsilon = 3$, $\varepsilon = 4$ respectively:

- We choose a family of functions f satisfying (I) and we parametrize them with k-points on a variety $\mathcal{F}$.
- We impose some conditions slightly stronger than (II), (III), (IV), describing a variety $\mathcal{C} \subset \mathcal{F}\times\mathrm{PGL}_2\times\mathbb{A}^1$ with the following property: for any point $(f, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), z) \in \mathcal{C}(k)$, the pair $(f, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right))$ satisfies (I), (II), (III), (IV).

  In particular, $\mathcal{C}$ is a curve in the case $\epsilon = 3$, a surface in the case $\epsilon = 4$
- We prove that the geometrically irreducible components of $\mathcal{C}$ are defined over k and we deduce that $\mathcal{C}(k)$ has cardinality at least $\frac{1}{2}(\#k)^{\dim \mathcal{C}}$; this is the point in the proof where we use the technical hypothesis $[k : \mathbb{F}_q] \geq 80$ (details after Equations (4.7.3.3) and 4.8.4.3).

Using $\mathcal{C}$ we can easily describe the algorithms of Proposition 4.5.2 and Proposition 4.5.3, when D is an irreducible divisor defined over k: one first looks for a point

$(f, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), z)$ in $\mathcal{C}(k)$ and then computes g and D using the formulas (4.5.5) and (4.5.6). This procedure takes average polynomial time in $q \log(\#k)$ because, as explained in Sections 4.7.3 and 4.8.4, the variety $\mathcal{C}$ is a closed subvariety of $\mathbb{A}^9$ with degree $O(q^9)$.

4.6 A technical lemma

In this section we take a break from our main topic and we prove Lemma 4.6.6. This lemma is useful to study the variety $\mathcal{C}$ used in the algorithms of Propositions 4.5.2 and 4.5.3. We split the proof into two propositions.

Because of condition (II), we are interested in the splitting field over a finite extension $\mathbb{F}_q \subset k$ of polynomials of the form $c'T^{q+1}+d'T^q+a'T+b' \in k[T]$. In particular, in Sections 4.7 and 4.8 the matrix $\left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right)$ varies in an algebraic family: we have a variety $\mathcal{B}$ and $\left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)(P)$ where $a, b, c, d \in k(\mathcal{B})$ and P is a point varying in $\mathcal{B}(k)$. We are interested in studying the splitting field of polynomials $cT^{q+1}+dT^q+aT+b$ over function fields, as in the next proposition.

For any extension of fields $k \subset \mathbb{K}$, its *field of constants* is the subfield of $\mathbb{K}$ containing all the elements that are algebraic over k. For any irreducible variety $\mathcal{C}/k$ we have that $\mathcal{C}$ is geometrically irreducible if and only if k is the field of constants of the extension $k \subset k(\mathcal{C})$.

Proposition 4.6.1. *Let $\mathbb{F}_q \subset k$ be an extension of finite fields and let $k \subset \mathbb{K}$ be a field extension with field of constants k. Let $v : \mathbb{K}^\times \to \mathbb{Z}$ be a valuation with ring of integral elements $\mathcal{O}_v \subset \mathbb{K}$ and generator π_v of the maximal ideal of $\mathcal{O}_v$. Let a, b, c, d be elements of $\mathcal{O}_v$ such that*

$$\begin{aligned} &v(ad-bc) = 1, \qquad v(d^q c - a c^q) = 0 \qquad \text{and} \\ &c\lambda^q - c^q(ad-bc)\lambda^{-1} \not\equiv d^q c - a c^q \pmod{\pi_v^2} \quad \forall \lambda \in \mathcal{O}_v^\times . \end{aligned} \tag{4.6.1.1}$$

Then the splitting field of the polynomial

$$F(T) := cT^{q+1} + dT^q + aT + b \quad \in \mathbb{K}[T] ,$$

is an extension of k having field of constants equal to k.

Proof. For any field extension $\mathbb{K} \subset \widetilde{\mathbb{K}}$, we denote $\widetilde{\mathbb{K}}(F)$ the splitting field of F over $\widetilde{\mathbb{K}}$, which is a separable extension of $\widetilde{\mathbb{K}}$ because the discriminant of F is a power of $ad-bc$ and $ad-bc \neq 0$. Since the field of constants of $k \subset \mathbb{K}$ is equal to k, then $\mathbb{K}' := \mathbb{K} \otimes_k \overline{k}$ is a field and the statement of the proposition is equivalent to the equality

$$\mathrm{Gal}(\mathbb{K}(F)/\mathbb{K}) = \mathrm{Gal}(\mathbb{K}'(F)/\mathbb{K}') .$$

By [23, Theorems 2.5 and 3.2] there exists a bijection between the roots of F and $\mathbb{P}^1(\mathbb{F}_q)$ that identifies the action of $\mathrm{Gal}(\mathbb{K}(F)/\mathbb{K})$ on the roots with the action of a subgroup of $G := \mathrm{PGL}_2(\mathbb{F}_q)$ on $\mathbb{P}^1(\mathbb{F}_q)$. We choose such a bijection and we identify $\mathrm{Gal}(\mathbb{K}(F)/\mathbb{K})$ and $\mathrm{Gal}(\mathbb{K}'(F)/\mathbb{K}')$ with two subgroups of G. If we prove that $\mathrm{Gal}(\mathbb{K}'(F)/\mathbb{K}')$ contains a Borel subgroup B of G the proposition follows: the only subgroups of PGL_2 containing B are the whole G and B itself and, since B is not normal inside G, we deduce that either $\mathrm{Gal}(\mathbb{K}(F)/\mathbb{K}) = \mathrm{Gal}(\mathbb{K}(F)/\mathbb{K}') = B$ or $\mathrm{Gal}(\mathbb{K}(F)/\mathbb{K}) = \mathrm{Gal}(\mathbb{K}'(F)/\mathbb{K}') = G$.

In the rest of the proof we show that $\mathrm{Gal}(\mathbb{K}'(F)/\mathbb{K}')$ contains a Borel subgroup working locally at v. We choose an extension of v to $\mathbb{K}'$ and consider the completion $\mathbb{K}'_v$ of $\mathbb{K}'$. Since $\mathrm{Gal}(\mathbb{K}'_v(F)/\mathbb{K}'_v)$ is a subgroup of $\mathrm{Gal}(\mathbb{K}'(F)/\mathbb{K}')$, it is enough to show that $\mathrm{Gal}(\mathbb{K}'_v(F)/\mathbb{K}'_v)$ is a Borel subgroup to prove the proposition. Since $ad-bc \equiv 0$ and $c \not\equiv 0$ modulo π_v, we have

$$F(T) \equiv c\Big(T^q + \frac{a}{c}\Big)\Big(T + \frac{d}{c}\Big) \pmod{\pi_v},$$

and, since $d^q c \neq a c^q \bmod \pi_v$, we deduce that $-\frac{d}{c}$ is a simple root of $F \bmod \pi_v$. By Hensel's Lemma, there exists a root $r_0 \in \mathbb{K}'_v$ of F that is v-integral and congruent to $-\frac{d}{c}$ modulo π_v. The group $\mathrm{Gal}(\mathbb{K}'_v(F)/\mathbb{K}'_v) \subset G$ stabilizes the element of $\mathbb{P}^1(\mathbb{F}_q)$ corresponding to r_0, hence it is contained in a Borel subgroup of G. Since Borel subgroups have cardinality $q(q-1)$, in order to prove the proposition it is enough showing that $[\mathbb{K}'(F) : \mathbb{K}']$ is at least $q(q-1)$. We show that the inertia degree of $\mathbb{K}' \subset \mathbb{K}'(F)$ is at least $q(q-1)$.

Since $\frac{a}{c}$ is a q-th power modulo π_v, then there exists a v-integral element $\gamma \in \mathbb{K}'_v$ such that $F(T) \equiv c(T+\gamma)^q(T + d/c) \bmod \pi_v$. Up to the substitution $F(T) \mapsto F(T-\gamma)$, which does not change $\mathbb{K}'_v(F)$ nor the quantities c, $ad-bc$ and $d^q c - a c^q$, we can suppose that

$$F(T) \equiv c\,T^q\Big(T + \frac{d}{c}\Big) \pmod{\pi_v}.$$

This implies that $v(d/c) = 0$, $v(a) \geq 1$ and $v(b) \geq 1$. If we had $v(b) \geq 2$, then the choice $\lambda := d$ would contradict the last congruence in (4.6.1.1). Hence we have $v(b) = 1$. The Newton polygon of F tells us that the roots $r_0, \ldots, r_q$ of F in the algebraic closure $\overline{\mathbb{K}'_v}$ of $\mathbb{K}'_v$ satisfy

$$v(r_0) = 0\,, \quad v(r_1) = \ldots = v(r_q) = \frac{1}{q}\,. \tag{4.6.2}$$

We now consider the polynomial

$$F_1(T) := F(T + r_1) = c_1 T^{q+1} + d_1 T^q + a_1 T + b_1 = c T^{q+1} + d_1 T^q + a_1 T \quad \in \overline{\mathbb{K}'_v}[T]\,.$$

The roots of F_1 are $r_i - r_1$. Using Equation (4.6.2), we deduce $v(c_1) = v(d_1) = 0$ and $v(a_1) > 0$. Using $a_1 d_1 - b_1 c_1 = ad - bc$, we see that $v(a_1) = v(a_1 d_1 - c_1 b_1) = v(ad-bc) = 1$.

The Newton polygon of F_1 tells us that

$$v(r_2 - r_1) = \ldots = v(r_q - r_1) = \frac{1}{q-1}\,.$$

This, together with Equation (4.6.2) and the fact that $\mathbb{K} \subset \mathbb{K}'$ is unramified, imply that the inertia degree of $\mathbb{K}'_v \subset \mathbb{K}'_v(F)$ is a multiple of $q(q-1)$ and consequently that $\mathrm{Gal}(\mathbb{K}'_v(F)/\mathbb{K}')$ is a Borel subgroup of G. □

We now prove that, for certain choices of $a, b, c, d \in \mathbb{K}$, Equation (4.6.1.1) is satisfied.

Proposition 4.6.3. *Let $\mathbb{K}$ be a field extension of $\mathbb{F}_q$, let $u_1, u_2, u_3, w_1, w_2, w_3$ be distinct elements of $\mathbb{K}$ and let $a, b, c, d \in \mathbb{K}$ be the elements defined by the following equality in $GL_2(\mathbb{K})$*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} w_3^q & w_1^q \\ 1 & 1 \end{pmatrix} \begin{pmatrix} w_1^q - w_2^q & 0 \\ 0 & w_2^q - w_3^q \end{pmatrix} \begin{pmatrix} u_2 - u_3 & 0 \\ 0 & u_1 - u_2 \end{pmatrix} \begin{pmatrix} 1 & -u_1 \\ -1 & u_3 \end{pmatrix}\,.$$

Then $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ sends the three elements $u_1, u_2, u_3 \in \mathbb{P}^1(\mathbb{K})$ to $w_1^q, w_2^q, w_3^q \in \mathbb{P}^1(\mathbb{K})$ respectively.

Suppose, moreover, that $\mathbb{K}$ is equipped with a discrete valuation $v : \mathbb{K}^\times \to \mathbb{Z}$, that u_i, w_i are v-integral, that $v(w_i - w_j) = v(w_3 + u_i) = v(u_2 - u_3) = 0$ for $i \neq j$ and that $v(u_1 - u_2) = 1$. Then a, b, c, d satisfy (4.6.1.1).

Proof. To prove first part we notice that, given distinct elements $x, y, z \in \mathbb{K}$, the matrix

$$N_{x,y,z} := \begin{pmatrix} z & x \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x - y & 0 \\ 0 & y - z \end{pmatrix}$$

is invertible and acts on $\mathbb{P}^1(\mathbb{K})$ sending $0, 1, \infty = \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right]$ to x, y, z respectively. Using this definition we have $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \det(N_{u_1,u_2,u_3}) N_{w_1^q,w_2^q,w_3^q} N^{-1}_{u_1,u_2,u_3}$, hence $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ acts on $\mathbb{P}^1(\mathbb{K})$ sending

$$u_1 \mapsto 0 \mapsto w_1^q\,, \quad u_2 \mapsto 1 \mapsto w_2^q\,, \quad u_3 \mapsto \infty \mapsto w_3^q\,.$$

Now the second part of the lemma. Computing $\det(N_{u_1,u_2,u_3})$ and $\det(N_{w_1^q,w_2^q,w_3^q})$ we see that

$$ad - bc = (u_1 - u_2)(u_2 - u_3)(u_1 - u_3)(w_1 - w_2)^q (w_2 - w_3)^q (w_1 - w_3)^q$$

hence $v(ad - bc) = v(u_1 - u_2) + v(u_3 - u_1) = 1$ (the element $u_3 - u_1$ has valuation zero because it is the sum of $u_3 - u_2$ and $u_2 - u_1$ that have valuation 0, respectively 1. Writing

a, b, c, d as polynomials in the u_i's and the w_i's, we check that there is a multivariate polynomial f such that

$$\begin{aligned} d^q c - ac^q =& f(u_1,u_2,u_3,w_1,w_2,w_3)\cdot\big(u_1-u_2\big)^q \\ &+ (u_1-u_3)^q(w_1-w_2)^{q^2}(w_1-w_3)^q(u_2+w_2)^q\cdot\big(u_1-u_2\big) \\ &- (w_1-w_2)^{q^2+q}(u_1-u_3)^{q+1}(u_1+w_3)^q\,. \end{aligned} \tag{4.6.4}$$

Since $v(w_2-w_1) = v(u_3-u_1) = v(w_3+u_1) = 0$, we have $v(d^qc-ac^q) = 0$. Let $\mathcal{O}_v$ be the integral subring of $\mathbb{K}$, let $\pi_v := u_1-u_2$, which is a generator of the maximal ideal of $\mathcal{O}_v$. Now suppose by contradiction that there exists $\lambda \in \mathcal{O}_v^\times$ such that

$$c\lambda^q - a^q(ad-bc)\lambda^{-1} \equiv d^qc - ac^q \pmod{\pi_v^2}\,. \tag{4.6.5}$$

Using $ad-bc \equiv 0 \bmod \pi_v$ and the equality $c = (w_1-w_2)^q(u_1-u_3) - \pi_v(w_1-w_3)^q$, we deduce

$$\lambda^q \equiv \frac{d^qc-ac^q}{c} \equiv \Big(-(u_1-u_3)(u_1+w_3)(w_1-w_2)^q\Big)^q \pmod{\pi_v}\,,$$

If we replace λ by some $\lambda' \equiv \lambda$ modulo π_v, then the congruences (4.6.1.1) are still satisfied, hence we may suppose $\lambda = -(u_1-u_3)(u_1+w_3)(w_1-w_2)^q$. Substituting λ and (4.6.4) in (4.6.5) we get

$$\begin{aligned} 0 &\equiv c^q(ad-bc) + (d^qc-ac^q)\lambda - c\lambda^{q+1} \\ &\equiv -\pi_v(w_1-w_2)^{q^2+q}(w_1-w_3)^q(u_1-u_3)^{q+1}(w_2-w_3)^q(w_3+u_3) \qquad \pmod{\pi_v^2} \end{aligned}$$

which is absurd because $v(w_i-w_j) = v(u_1-u_3) = v(w_3+u_3) = 0$. □

We now prove the main result of this section. Varieties like $\mathcal{C}$ in the following lemma arise in Sections 4.7 and 4.8 when imposing conditions (II) and (III). Proving that the components of such curves are defined over k is useful to prove that such varieties have "many" k-rational points and consequently that conditions (II) and (III) are "often" true.

Lemma 4.6.6. *Let $\mathbb{F}_q \subset k$ be an extension of finite fields and let $\mathcal{B}/k$ be a geometrically irreducible variety. Let u_1, u_2, u_3, w_1, w_2, w_3 be distinct elements of $\overline{k}(\mathcal{B})$ and suppose there exists an irreducible divisor $Z \subset \mathcal{B}_{\overline{k}}$, generically contained in the smooth locus of $\mathcal{B}$, such that u_i, w_i are defined on the generic point of Z and such that*

Z is a zero of order 1 of u_1-u_2 and it is not a zero of $w_3+u_i, u_2-u_3, w_i-w_j$ for $i\neq j$.

Let $\mathcal{C} \subset \mathcal{B}\times \mathrm{PGL}_2 \times \mathbb{A}^1$ be the variety whose the points are the tuples $(R, \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right), z)$ such that

$$u_i(R) \text{ are defined and distinct,} \quad w_i(R) \text{ are defined and distinct,} \quad d^qc-ac^q \neq 0,$$
$$\left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right)\cdot u_i(R) = w_i^q(R) \text{ for } i=1,2,3 \qquad \text{and}$$
$$(d^qc-ac^q)^{q+1}(z^q-z)^{q^2-q} = c^{q^2+1}(ad-bc)^q\Big((z^{q^2}-z)/(z^q-z)\Big)^{q+1}$$

If $\mathcal{C}$ is defined over k, then its geometrically irreducible components are defined over k and pairwise disjoint.

Proof. We first look at the variety $\mathcal{B}_0 \subset \mathcal{B} \times \mathrm{PGL}_2$ whose points are the pairs (R, A) such that

$$u_i(R) \text{ are defined and distinct}, \quad w_i(R) \text{ are defined and distinct},$$
$$A \cdot u_i(R) = w_i^q(R) \text{ for } i = 1, 2, 3\,.$$

Since an element PGL_2 is uniquely determined by its action on three distinct points of $\mathbb{P}^1$, the projection $\mathcal{B}_0 \to \mathcal{B}$ is a birational equivalence, whose inverse, by the first part of Proposition 4.6.3, is given by $R \mapsto \left(\begin{smallmatrix} a_1 & b_1 \\ c_1 & d_1 \end{smallmatrix}\right)(R)$, where $a_1, b_1, c_1, d_1 \in \overline{k}(\mathcal{B})$ are defined by the following equality in $\mathrm{GL}_2(\overline{k}(\mathcal{B}))$

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} = \begin{pmatrix} w_3^q & w_1^q \\ 1 & 1 \end{pmatrix} \begin{pmatrix} w_1^q - w_2^q & 0 \\ 0 & w_2^q - w_3^q \end{pmatrix} \begin{pmatrix} u_2 - u_3 & 0 \\ 0 & u_1 - u_2 \end{pmatrix} \begin{pmatrix} 1 & -u_1 \\ -1 & u_3 \end{pmatrix}.$$

Let $v\colon \overline{k}(\mathcal{B})^\times \to \mathbb{Z}$ be the valuation that determines the order of vanishing in Z of a rational function. The second part of Proposition 4.6.3 implies that a_1, b_1, c_1, d_1 satisfy (4.6.1.1), over the field $\overline{k}(\mathcal{B})$. In particular we have $c_1 \neq 0$ and $v(c_1) = 0$. Hence we can define the following rational functions on $\mathcal{C}$

$$a_2 := a_1/c_1\,, \quad b_2 := b_1/c_1\,, \quad c_2 := 1\,, \quad d_2 := d_1/c_1$$

which again satisfy (4.6.1.1) over the field $\overline{k}(\mathcal{B})$. The advantage of a_2, b_2, c_2, d_2 is that, as we now show, they are defined over k. Let $\mathcal{B}_1$ be the projection of $\mathcal{C}$ inside $\mathcal{B} \times \mathrm{PGL}_2$: since $\mathcal{C}$ is defined over k, the variety $\mathcal{B}_1$ is defined over k and, since $\mathcal{B}_1$ is a dense open subvariety of $\mathcal{B}_0$, the variety $\mathcal{B}_1$ is birational equivalent to $\mathcal{B}$ through the natural projection. Since a/c is a rational function on $\mathcal{B}_1$ defined over k, we deduce that $a_2 = a/c$ lies in $k(\mathcal{B}_1) = k(\mathcal{B})$ and analogously $b_2, c_2, d_2 \in k(\mathcal{B})$. A fortiori a_2, b_2, c_2, d_2 satisfy (4.6.1.1) inside the field $\mathbb{K} = k(\mathcal{B})$. By Proposition 4.6.1, k is the field of constants of the extension $k \subset \Sigma$, where Σ is the splitting field of

$$F(T) := c_2 T^{q+1} + d_2 T^q + a_2 T + b_2\,,$$

over $k(\mathcal{B})$. We deduce that there exists a geometrically irreducible variety $\mathcal{E}/k$ having field of rational functions Σ. Let $\pi\colon \mathcal{E} \dashrightarrow \mathcal{B}$ be the rational map induced by $k(\mathcal{B}) \subset \Sigma$ and let $r_0, \ldots, r_q \in \Sigma$ be the roots of F, interpreted as rational functions on $\mathcal{E}$. Using [23, Lemma 2.3] we see that, for any choice of integers $0 \leq i < j < m \leq q$,

$$z = z_{i,j,k} := \frac{r_i - r_j}{r_i - r_k} \in \Sigma = k(\mathcal{E}) \quad \text{satisfies}$$
$$(d_2^q c_2 - a_2 c_2^q)^{q+1} (z^q - z)^{q^2-q} = C_2^{q^2+1} (a_2 d_2 - b_2 c_2)^q \left((z^{q^2} - z)/(z^q - z)\right)^{q+1}$$

Hence, for each $0 \leq i < j < m \leq q$ we get a map

$$\phi_{i,j,m} \colon \mathcal{E} \dashrightarrow \mathcal{C}, \qquad S \longmapsto \left(\pi(S), \left(\begin{smallmatrix} a_2 & b_2 \\ c_2 & d_2 \end{smallmatrix}\right)(S), z_{i,j,m}(S)\right) .$$

Since all the $z_{i,j,m}$ are different, the union of all the images $\phi_{i,j,m}(\mathcal{E})$ is dense inside $\mathcal{C}$. Hence, up to shrinking $\mathcal{C}$, every geometrically irreducible component of $\mathcal{C}$ is also a geometrically irreducible component of $\phi_{i,j,m}(\mathcal{E})$ for some (i,j,m). Since $\mathcal{E}$ is defined over k and geometrically irreducible, the variety $\phi_{i,j,m}(\mathcal{E})$ is also defined over k and geometrically irreducible. We deduce that the irreducible components of $\mathcal{C}$ are defined over k.

Finally, we prove that the components of $\mathcal{C}$ are pairwise disjoint. The projection $\pi \colon \mathcal{C} \to \mathcal{B}_1$ has finite fibers whose number of $\overline{k}$-points counted with multiplicity is q^3-q , that is the degree, in z, of the polynomial

$$(d^q c - a c^q)^{q+1}(z^q - z)^{q^2-q} - c^{q^2+1}(ad-bc)^q \left((z^{q^2} - z)/(z^q - z)\right)^{q+1} .$$

If, by contradiction, there is a point $(R', \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right), z')$ lying in the intersection of two components of $\mathcal{C}$, then the fiber $\pi^{-1}(R', \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right))$ has cardinality smaller than q^3-q. In other words the polynomial

$$G(z) := (d'^q c' - a' c'^q)^{q+1}(z^q - z)^{q^2-q} - c'^{q^2+1}(a'd' - b'c')^q \left((z^{q^2} - z)/(z^q - z)\right)^{q+1} \in \overline{\mathbb{F}_q}[z]$$

has less than q^3-q roots. Since $a'd'-b'c' \neq 0$ and $d^q c' - a' c'^q \neq 0$, there is no root of G that is also a root of $z^q - z$ or $\frac{z^{q^2}-z}{z^q-z}$. In other words, G has no root lying in the finite field $\mathbb{F}_{q^2} \subset \overline{\mathbb{F}_q}$ with q^2 elements. Since z' is a root of G and since G is a $\overline{\mathbb{F}_q}$-linear combination of powers of $z^q - z$ and $\frac{z^{q^2}-z}{z^q-z}$, for any matrix $A \in \mathrm{PGL}_2(\mathbb{F}_q)$, the number $A \cdot z'$ is also a root of G. Since $\#\mathrm{PGL}_2(\mathbb{F}_q) = q^3-q$ is larger than the set of roots of G, there exists a matrix $A \in \mathrm{PGL}_2(\mathbb{F}_q)$ such that $A \cdot z' = z'$, implying that z' lies in $\mathbb{F}_q^2$, which is absurd. □

Remark 4.6.7. Let $\mathbb{F}_q \subset k$ be a field extension and let $F(T) = cT^{q+1} + dT^q + aT + b$ be a polynomial with coefficients in k such that, $ad-bc \neq 0$ and $a^q c - d c^q \neq 0$. By [23, Theorem 4.3 and Lemma 2.3], the polynomial F splits in linear factors over k if and only if there exists an element $z \in k$ such that

$$(d^q c - a c^q)^{q+1}(z^q - z)^{q^2-q} = c^{q^2+1}(ad-bc)^q \left((z^{q^2} - z)/(z^q - z)\right)^{q+1} .$$

In particular, in the notation of the proof of Lemma 4.6.6, we have $\Sigma = k(\mathcal{B})(z_{i,j,m})$ for any choice of integers $0 \leq i < j < m \leq q$. In particular, the map $\phi_{i,j,m}$ is injective, hence it is a birational equivalence between $\mathcal{E}$ and an irreducible component of $\mathcal{C}$. In other words the field of rational functions of an irreducible component of $\mathcal{C}$ is the splitting field of F over $k(\mathcal{B})$.

4.7 Descent 3-to-2

In this section we prove Proposition 4.5.3 for a good irreducible divisor D. Following the notation of Section 4.5 when $\varepsilon = 3$, let k be a finite extension of $\mathbb{F}_q$ of degree at least 80, let Q be a good point on E such that $[k(Q) : k] = 3$, and let σ be a generator of $\mathrm{Gal}(k(Q)/k)$. Then, we look for a function $f \in k(E)$ and a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{PGL}_2(k)$ satisfying properties (I), (II), (III), (IV): we describe a curve $\mathcal{C}$ whose k-points give such pairs $(f, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right))$, and we prove that there are many k-points on $\mathcal{C}$.

4.7.1 The definition of $\mathcal{C}$

Property (I) requires that $f \in k(E)$ has at most two poles: we look for f of the form

$$f_P := \frac{y - y(P)}{x - x(P)} \tag{4.7.1.1}$$

for some P in $E(k) \setminus \{O_E\}$, since such f_P has exactly two simple poles, namely O_E and $-P$. As explained in Remark 4.6.7, in order to ensure condition (II), it is sufficient imposing that $d^q c \neq a c^q$ and that there exists z in k such that

$$(d^q c - a c^q)^{q+1} (z^q - z)^{q^2-q} = c^{q^2+1} (ad - bc)^q \left((z^{q^2} - z)/(z^q - z) \right)^{q+1} . \tag{4.7.1.2}$$

Notice that definition (4.7.1.1) makes sense for $P \in E(\overline{\mathbb{F}_q}) \setminus \{O_E\}$ and that we have the following symmetry: for any $P, P' \in E(\overline{\mathbb{F}_q}) \setminus O_E$, we have $f_P(P') = f_{P'}(P)$. Using this and the fact that $h^\phi(\phi(P)) = h(P)^q$ for all $h \in \overline{\mathbb{F}_q}(E)$ and $P \in E(\overline{\mathbb{F}_q})$, we have

$$f_P(\sigma^i Q) = f_{\sigma^i Q}(P) , \quad f_P^\phi(\sigma^i Q + P_0) = f_P^\phi(\phi(\sigma^i R)) = f_P(\sigma^i R)^q = f_{\sigma^i R}(P)^q ,$$

where R is the unique point on E such that $\phi(R) = Q + P_0$. Hence (III) is equivalent to

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot f_{\sigma_i Q}(P) = -f_{\sigma^i R}(P)^q \quad \text{for each } i = 0, 1, 2 . \tag{4.7.1.3}$$

We now impose (IV). Let B be a point on E such that $\phi(B) = B + P_0$. If the rational function $c f_P^{q+1} + d f_P^q + a f_P + b$ vanishes on B, then $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot f_B(P) = -f_B(P)^q$. This and Equation (4.7.1.3), when $f_{\sigma^i Q}$ are distinct, imply that the cross ratio of $f_Q(P)$, $f_{\sigma Q}(P)$, $f_{\sigma^2 Q}(P)$, $f_B(P)$ equals the cross ratio of $f_R(P)^q, f_{\sigma R}(P)^q, f_{\sigma^2 R}(P)^q$, $f_B(P)^q$. The poles of f_P are O_E and $-P$. Hence, assuming (4.7.1.3) and the distinctness of $f_{\sigma^i Q}(P)$, condition (IV) is implied by

(4.7.1.4)

$$\text{for all } B \text{ such that } \phi(B) = B + P_0 : \qquad P \neq -B \quad \text{and}$$

$$\mathrm{CrRat}\big(f_Q(P), f_{\sigma Q}(P), f_{\sigma^2 Q}(P), f_B(P)\big) \neq \mathrm{CrRat}\big(f_R(P)^q, f_{\sigma R}(P)^q, f_{\sigma^2 R}(P)^q, f_B(P)^q\big) ,$$

where, given four elements $\lambda_1, \lambda_2, \lambda_3, \lambda_4 \in \mathbb{P}^1(\overline{\mathbb{F}_q})$, we write

$$\mathrm{CrRat}(\lambda_1, \lambda_2, \lambda_3, \lambda_4) = \frac{(\lambda_3 - \lambda_1)(\lambda_4 - \lambda_2)}{(\lambda_2 - \lambda_1)(\lambda_4 - \lambda_3)} \in \mathbb{P}^1(\overline{\mathbb{F}_q}),$$

for their cross-ratio, which is defined unless three of the λ_i's are equal.

Finally we define $E' := E \setminus \{O_E, -Q, -R, \dots, -\sigma^2 Q, -\sigma^2 R\}$, so that $f_{\sigma^i R}$ and $f_{\sigma^i Q}$ are regular on E', and we define $\mathcal{C} \subset E' \times \mathrm{PGL}_2 \times \mathbb{A}^1$ as the curve made of points $(P, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), z)$ that satisfy Equations (4.7.1.3), (4.7.1.2) and (4.7.1.4), and such that $d^q c - a c^q \neq 0$ and the $f_{\sigma^i Q}(P)$ are distinct.

Notice that $\mathcal{C}$ is defined over k: even though the equations $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) f_{\sigma^i Q}(P) = -f^q_{\sigma^i R}(P)$ on $E' \times \mathrm{PGL}_2$ have coefficients in the field $k(Q)$, the Galois group of $k \subset k(Q)$ permutes these equations. We constructed $\mathcal{C}$ so that, for any point $(P, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), z) \in \mathcal{C}(k)$, the pair $(f_P, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right))$ satisfies properties (I), (II), (III) and (IV).

4.7.2 The irreducible components of $\mathcal{C}$

In this subsection we prove that all the geometrically irreducible components of $\mathcal{C}$ are defined over k. We can leave out (4.7.1.4) from the definition of $\mathcal{C}$. Our strategy is applying Lemma 4.6.6 to the variety $\mathcal{B} = E'$, using the rational functions $u_i = f_{\sigma^{i-1} Q}$, $w_i = -f_{\sigma^{i-1} R}$ and the irreducible divisor Z equals to the point $-Q - \sigma Q \in \mathcal{B}(\overline{\mathbb{F}_q}) \subset E(\overline{\mathbb{F}_q})$.

Notice that, given distinct points $P', P'' \in E(\overline{\mathbb{F}_q}) \setminus \{O_E\}$, the function $f_{P'} - f_{P''}$ is regular at O_E and moreover $(f_{P'} - f_{P''})(O_E) = 0$. Since the sum of zeroes and poles of a rational function is equal to O_E in the group $E(\overline{\mathbb{F}_q})$, we deduce that, given distinct points $P', P'' \in E(\overline{\mathbb{F}_q}) \setminus \{O_E\}$,

(4.7.2.1)

$f_{P'} - f_{P''}$ has two simple poles, namely $-P'$ and $-P''$
and two zeroes counted with multiplicity, namely O_E and $-P' - P''$.

Let $Z := -Q - \sigma Q$. By (4.7.2.1) and the fact that Q is not a trap, the point Q is not a pole of any of the u_i and the w_i and it is not a zero of any of the functions $u_2 - u_3$, $w_3 + u_i$ and $w_i - w_j$ for $i \neq j$: if, for example, $-f_{\sigma R}$ is not regular on Z, then $Z = -R$. Hence, using that σ acts as ϕ^l on $E(\overline{\mathbb{F}_q})$ for $l := [k : \mathbb{F}_q]$, we have

$$Q + P_0 = \phi(R) = \phi(-Z) = \phi^{l+1}(Q) + \phi(Q) \quad \Longrightarrow \quad \phi^{l+1}(Q) = (1 - \phi)(Q) + P_0,$$

hence

(4.7.2.2)

$$\begin{aligned} \phi^3(Q) &= \phi^{3l+3}(Q) = \phi^{2l+2}\left((1-\phi)(Q) + P_0\right) = \left((1-\phi) \circ \phi^{2l+2}\right)(Q) + P_0 \\ &= \left((1-\phi) \circ \phi^{l+1}\right)\left((1-\phi)(Q) + P_0\right) + P_0 = \left((1-\phi) \circ (1-\phi)\right)(\phi^{l+1}(Q)) + P_0 \\ &= (1-\phi)^2\left((1-\phi)(Q) + P_0\right) + P_0 = (1-\phi)^3(Q) + P_0, \end{aligned}$$

implying that

$$((2\phi-1)\circ(\phi^2-\phi+1))(Q) = (\phi^3+(\phi-1)^3)(Q) = P_0\,,$$

which contradicts the hypothesis that Q was not a trap point. Moreover, by (4.7.2.1), the function $f_Q - f_{\sigma Q}$ has a simple zero in Z. Hence, by Lemma 4.6.6, all the geometrically irreducible components of $\mathcal{C}$ are defined over k and disjoint.

4.7.3 k-rational points on $\mathcal{C}$

We now prove that $\#\mathcal{C}(k)$ is larger than $\frac{1}{2}\#k$. The curve $\mathcal{C}$ is contained in the open subset of $(E\setminus\{O_E\})\times \mathrm{PGL}_2\times\mathbb{A}^1$ made of points $((x,y),\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right),z)$ such that $c\neq 0$. Hence $\mathcal{C}$ is contained in $\mathbb{A}^6$, with variables x, y, a, b, d, z and it is defined by the following equations:

- $0 = p_1 := W(x,y)$, the Weierstrass equation defining E;
- $0 = p_2 := (d^q-a)^{q+1}(z^q-z)^{q^2-q} - (ad-b)^q(\frac{z^{q^2}-z}{z^q-z})^{q+1}$, the dehomogenization of (4.7.1.2) in c;
- $0 = p_i(x,y,a,b,d)$ for $i=3,4,5$, obtained by (4.7.1.3) after dehomogenizing in c, substituting $f_{\sigma^i Q}(P)$ and $f_{\sigma^i R}(P)$ by their expressions in x, y and clearing denominators;
- a number of conditions $0\neq q_j$ ensuring that $P\neq -\sigma^i Q$, $P\neq -\sigma^i R$, $d^q-a\neq 0$, $ad-b\neq 0$, that $f_{\sigma^i Q}(P)$ are pairwise distinct and that (4.7.1.4) is satisfied.

In particular, $\mathcal{C}$ can be seen as a closed subvariety of $\mathbb{A}^7$, with variables x, y, a, b, d, z and t defined by the equations $p_1=0,\dots,p_5=0$ and $0=p_6 := tq_1\cdots q_r - 1$.

Let $\mathcal{C}_1,\dots,\mathcal{C}_s$ be the irreducible components of $\mathcal{C}$. By [46, Remark 11.3], we have

$$\#\mathcal{C}(k) \geq \#\mathcal{C}_1(k) \geq \#k - (\delta-1)(\delta-2)(\#k)^{\frac{1}{2}} - K(\mathcal{C}_1)\,, \tag{4.7.3.1}$$

where δ is the degree of $\mathcal{C}_1$ and $K(\mathcal{C}_1)$ is the sum of the Betti numbers of $\mathcal{C}$ relative to the compact ℓ-adic cohomology. Since $\mathcal{C}_1$ is a component of $\mathcal{C}$ then

$$\delta \leq \deg(p_1)\cdots\deg(p_6)\,. \tag{4.7.3.2}$$

Since $\mathcal{C}$ is the disjoint union of the $\mathcal{C}_i$, the Betti numbers of $\mathcal{C}$ are the sums of the Betti numbers of the $\mathcal{C}_i$ and using [58, Corollary of Theorem 1] we deduce that

$$K(\mathcal{C}_1) \leq K(\mathcal{C}) \leq 6\cdot 2^6\cdot\left(3+7\max_{i=1,\dots,6}\{\deg(p_i)\}\right)^8\,. \tag{4.7.3.3}$$

Since $\deg p_1\leq 3$, $\deg p_2\leq q^3+q$, $\deg p_3,\dots,\deg p_5\leq q+2$, $\deg p_7\leq 8q^2+29q+29$, then Equations (4.7.3.1), (4.7.3.2) and (4.7.3.3) imply that $\#\mathcal{C}(k) > \frac{1}{2}(\#k)$ when $\#k\geq q^{80}$ and $q\geq 3$.

4.8 Descent 4-to-3

In this section we prove Proposition 4.5.2 for a good irreducible divisor D. Following the notation of section 4.5 when $\varepsilon = 4$, let k be a finite extension of $\mathbb{F}_q$ of degree at least 80, let Q be a good point on E such that $[k(Q) : k] = 4$, and let σ be a generator of $\mathrm{Gal}(k(Q)/k)$. Then, we look for a function $f \in k(E)$ and a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{PGL}_2(k)$ satisfying properties (I), (II), (III), (IV): we describe a surface $\mathcal{C}$ whose k-points give such pairs $(f, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right))$, and we prove that there are many k-points on $\mathcal{C}$.

4.8.1 The definition of $\mathcal{C}$

Property (I) requires that $f \in k(E)$ has at most 3 poles: we look for f of the form

$$f = f_{\alpha,\beta,P} := \frac{f_P + \alpha}{f_{\widetilde{P}} + \beta}\,. \tag{4.8.1.1}$$

where α, β are elements of k, the points $P, \widetilde{P}$ lie in $E(k) \setminus \{O_E\}$ and f_P is the rational function defined in (4.7.1.1). For the rest of the article we let α, β and P vary and we fix $\widetilde{P}$ so that

$$f_Q(\widetilde{P}), f_{\sigma Q}(\widetilde{P}), f_{\sigma^2 Q}(\widetilde{P}), f_{\sigma^3 Q}(\widetilde{P}), f_R(\widetilde{P}), f_{\sigma R}(\widetilde{P}), f_{\sigma^2 R}(\widetilde{P}), f_{\sigma^3 R}(\widetilde{P}) \text{ are pairwise distinct.}$$

There is at least one such point $\widetilde{P}$ because $\#(E(k) \setminus \{O_E\}) > \binom{8}{2}$ and by (4.7.2.1) for each $P' \neq P'' \in E(\overline{\mathbb{F}_q}) \setminus \{O_E\}$ there is at most one point $\widetilde{P} \in (E(k) \setminus \{O_E\})$ such that $f_{P'}(P) = f_{P''}(P)$. Notice that the above definition makes sense for any $P \in E(\overline{\mathbb{F}_q})$ and $\alpha, \beta \in \overline{\mathbb{F}_q}$ and that, for any such choice, the function $f_{\alpha,\beta,P}$ has at most three poles counted with multiplicity, namely $-P$ and the zeroes of $f_{\widetilde{P}}+\beta$. Hence condition (I) is automatically satisfied. We write f for $f_{\alpha,\beta,P}$, unless we want to stress the dependence on α, β, P, like in the equations defining $\mathcal{C}$.

As explained in Remark 4.6.7, when $d^q c - a c^q \neq 0$, condition (II), is satisfied if and only if there exists $z \in k$ such that

$$(d^q c - a c^q)^{q+1}(z^q - z)^{q^2-q} = c^{q^2+1}(ad - bc)^q \left((z^{q^2} - z)/(z^q - z)\right)^{q+1}\,. \tag{4.8.1.2}$$

Since $h^\phi(\phi(P)) = h(P)^q$ for all $h \in \overline{\mathbb{F}_q}(E)$ and $P \in E(\overline{\mathbb{F}_q})$, we have

$$-f^\phi(\sigma^i Q + P_0) = -f^\phi(\phi(\sigma^i R)) = -f(\sigma^i R)^q\,,$$

where $R \in E(\overline{\mathbb{F}_q})$ is the unique point such that $\phi(R) = Q + P_0$. Hence property (III) is equivalent to

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot f_{\alpha,\beta,P}(\sigma^i Q) = -f_{\alpha,\beta,P}(\sigma^i R)^q \quad \text{for } i = 0, 1, 2, 3\,. \tag{4.8.1.3}$$

Since cross-ratio is invariant under the action of PGL_2 on $\mathbb{P}^1$, the above equation implies that either the cross-ratio of $f(\sigma^0 Q), \ldots, f(\sigma^3 Q)$ is equal to the cross ratio of $f(\sigma^0 R), \ldots$, $f(\sigma^3 R)$, or one of the two cross-ratios is not defined. Hence, assuming that $f(\sigma^i Q)$ are distinct and that $f(\sigma^i R)$ are distinct, Equation (4.8.1.3) implies

(4.8.1.4)
$$\mathrm{CrRat}\big(f_{\alpha,\beta,P}(\sigma^0 Q), \ldots, f_{\alpha,\beta,P}(\sigma^3 Q)\big) = \mathrm{CrRat}\big(f_{\alpha,\beta,P}(\sigma^0 R)^q, \ldots, f_{\alpha,\beta,P}(\sigma^3 R)^q\big).$$

Moreover, supposing that $f(\sigma^i Q)$ and $f(\sigma^i R)$ are distinct, the properties of cross-ratio imply that Equation (4.8.1.3) is equivalent to Equation (4.8.1.4) together with

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot f_{\alpha,\beta,P}(\sigma^i Q) = -f_{\alpha,\beta,P}(\sigma^i R)^q \quad \text{for } i = 0, 1, 2\,. \tag{4.8.1.5}$$

We now impose (IV). Let B be a point on E such that $\phi(B) = B + P_0$. If the rational function $cf^{q+1} + df^q + af + b$ vanishes on B, then $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) f(B) = -f(B)^q$. This, together with Equation (4.8.1.5) and the fact that $f(\sigma^i Q)$ are all distinct, implies that the cross-ratio of $f(Q), f(\sigma Q), f(\sigma^2 Q), f(B)$ is equal to the cross-ratio of $f^q(R), f^q(\sigma R), f^q(\sigma^2 R)$, $f^q(B)$. A pole of $f_{\alpha,\beta,P}$ is either equal to $-P$ or to a zero of $f_{\widetilde{P}} + \beta \in \overline{\mathbb{F}_q}(E)$. Hence, assuming Equation (4.8.1.5) and the distinctness of $f(\sigma^i Q)$, condition (IV) is implied by

(4.8.1.6)
$$\text{for all } B \text{ such that } \phi(B) = B + P_0 : \qquad P \neq -B\,, \quad \beta + f_{\widetilde{P}}(B) \neq 0 \quad \text{and}$$
$$\mathrm{CrRat}\big(f(Q), f(\sigma Q), f(\sigma^2 Q), f(B)\big) \neq \mathrm{CrRat}\big(f(R)^q, f(\sigma R)^q, f(\sigma^2 R)^q, f(B)^q\big)\,.$$

Let $E' := E \setminus \{O_E, -\sigma^0 Q, -\sigma^0 R, \ldots, -\sigma^3 Q, -\sigma^3 R\}$ and let $\mathcal{C} \subset \mathbb{A}^2 \times E' \times \mathrm{PGL}_2 \times \mathbb{A}^1$ be the surface made of points $(\alpha, \beta, P, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), z)$ that satisfy Equations (4.8.1.4), (4.8.1.5), (4.8.1.2) and (4.8.1.6), and such that $\beta + f_{\widetilde{P}}(\sigma^i Q) \neq 0$, $\beta + f_{\widetilde{P}}(\sigma^i R) \neq 0$, $d^q c - a c^q \neq 0$, the $f(\sigma^i Q)$ are distinct and the $f(\sigma^i R)$ are distinct.

The definition of E' and the conditions $\beta + f_{\widetilde{P}}(\sigma^i Q) \neq 0$, $\beta + f_{\widetilde{P}}(\sigma^i R) \neq 0$, ensure that $f(\sigma^i Q)$ and $f(\sigma^i R)$ are well defined. As in subsection 4.7.1, the surface $\mathcal{C}$ is defined over k. If $(\alpha, \beta, P, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), z)$ is a k-point on $\mathcal{C}$, then $(f_{\alpha,\beta,P}\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right))$ satisfies (I), (II) and (III) and (IV).

4.8.2 Irreducibility of a projection of $\mathcal{C}$

Before studying the irreducible components of $\mathcal{C}$, we study the closure in $\mathbb{P}^2 \times E$ of the projection of $\mathcal{C}$ in $\mathbb{A}^2 \times E$. Let $\mathcal{B}' \subset \mathbb{A}^2 \times E'$ be the surface whose points are the tuples (α, β, P) such that

$$f_{\alpha,\beta,P}(\sigma^i Q) \text{ are pairwise distinct}\,, \quad f_{\alpha,\beta,P}(\sigma^i R) \text{ are pairwise distinct},$$
$$f_{\widetilde{P}}(\sigma^i Q) + \beta \neq 0\,, \quad f_{\widetilde{P}}(\sigma^i R) + \beta \neq 0\,,$$
$$\mathrm{CrRat}\big(f_{\alpha,\beta,P}(\sigma^0 Q), \ldots, f_{\alpha,\beta,P}(\sigma^3 Q)\big) = \mathrm{CrRat}\big(f_{\alpha,\beta,P}(\sigma^0 R)^q, \ldots, f_{\alpha,\beta,P}(\sigma^3 R)^q\big)\,,$$

and let $\mathcal{B}$ be the closure of $\mathcal{B}'$ inside $\mathbb{P}^2 \times E$. Since the action of PGL_2 on $\mathbb{P}^1$ is triply transitive, the projection $\mathbb{A}^2 \times E \times \mathrm{PGL}_2 \times \mathbb{A}^1 \to \mathbb{A}^2 \times E$ gives a dominant morphism $\mathcal{C} \to \mathcal{B}$ (this is the same argument used in the proof of Lemma 4.6.6 to show that $\mathcal{B}_0 \to \mathcal{B}$ is dominant). Since $\mathcal{C}$ is defined over k, the variety $\mathcal{B}$ is defined over k. In the rest of the subsection we prove that for all but a few choices of $P \in E(k)$ the curve $\mathcal{B}_P := \mathcal{B} \cap (\{P\} \times \mathbb{P}^2)$ is reduced and geometrically irreducible. In other words, we think of P as fixed and we let α and β vary.

We first write an equation for $\mathcal{B}_P$ in $\mathbb{P}^2$. Using the definition of $f_{\alpha,\beta,P}$ we get

$$f_{\alpha,\beta,P}(\sigma^i Q) - f_{\alpha,\beta,p}(\sigma^j Q) = \frac{L_{i,j}(\alpha,\beta,1)}{\big(l_i+\beta\big)\big(l_j+\beta\big)}, \quad f_{\alpha,\beta,P}(\sigma^i R) - f_{\alpha,\beta,P}(\sigma^j R) = \frac{R_{i,j}(\alpha,\beta,1)}{\big(r_i+\beta\big)\big(r_j+\beta\big)},$$

where $l_i := f_{\widetilde{P}}(\sigma^i Q)$, $r_i := f_{\widetilde{P}}(\sigma^i R)$ and $L_{i,j}, R_{i,j} \in \overline{\mathbb{F}_q}[\alpha,\beta,\gamma]$ are the linear polynomials

$$\begin{aligned} L_{i,j} &:= \big(l_j - l_i\big)\alpha + \big(f_{\sigma^i Q}(P) - f_{\sigma^j Q}(P)\big)\beta + \big(f_{\sigma^i Q}(P) l_j - f_{\sigma^j Q}(P) l_i\big)\gamma, \\ R_{i,j} &:= \big(r_j - r_i\big)\alpha + \big(f_{\sigma^i R}(P) - f_{\sigma^j R}(P)\big)\beta + \big(f_{\sigma^i R}(P) r_j - f_{\sigma^j R}(P) r_i\big)\gamma\,. \end{aligned} \tag{4.8.2.1}$$

Then, for a fixed P, Equation (4.8.1.4) is equivalent to

$$(L_{0,2} L_{1,3} R_{0,1}^q R_{2,3}^q)(\alpha,\beta,1) = (L_{0,1} L_{2,3} R_{0,2}^q R_{1,3}^q)(\alpha,\beta,1)\,,$$

and $\mathcal{B}_P$ is the vanishing locus of the homogenous polynomial

$$M(\alpha,\beta,\gamma) := L_{0,2} L_{1,3} R_{0,1}^q R_{2,3}^q - L_{0,1} L_{2,3} R_{0,2}^q R_{1,3}^q \quad \in \overline{\mathbb{F}_q}[\alpha,\beta,\gamma]\,. \tag{4.8.2.2}$$

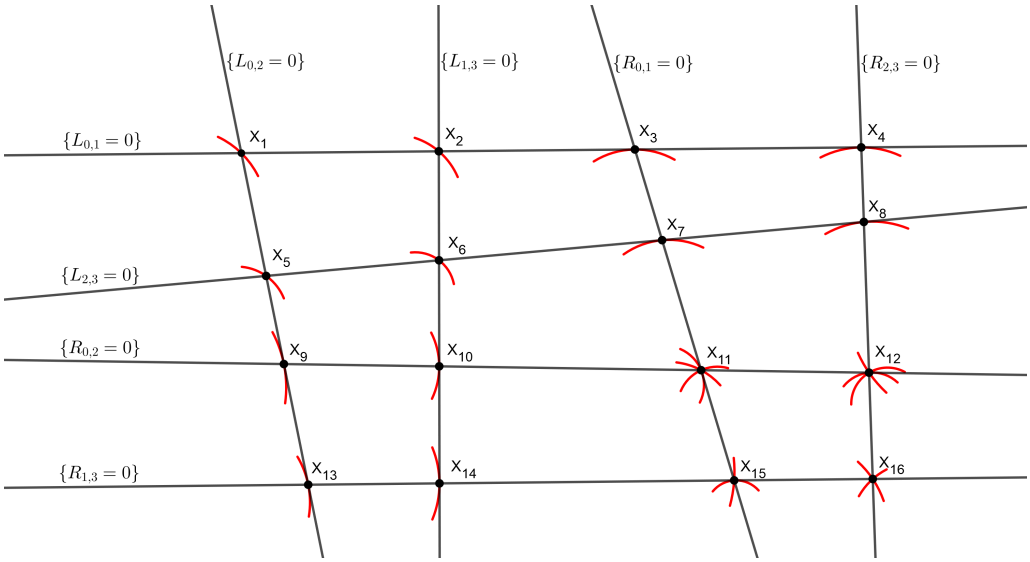
Notice that for each pair $(i,j) \in \{(0,1),(0,2),(1,3),(2,3)\}$ the varieties $\{L_{i,j} = 0\}$ and $\{R_{i,j} = 0\}$ are lines inside $\mathbb{P}^2$ and that it is easy to determine the intersections $\mathcal{B}_P \cap \{L_{i,j}{=}0\}$ and $\mathcal{B}_P \cap \{R_{i,j}{=}0\}$: such divisors are linear combinations of the points X_k's defined in Figure 4.1 as intersections between lines in $\mathbb{P}^2$. The following proposition says that the points X_k are well-defined and distinct.

Claim 4.8.2.3. *We consider the lines $\{L_{i,j} = 0\}$ and $\{R_{i,j} = 0\}$ for (i,j) in the set $\{(0,1),(2,3),(0,2),(1,3)\}$ and the points X_i defined in Figure 4.1 as intersections of some of these lines. For all but at most 450 choices of $P \in E(k)$, this lines are distinct and the points X_i are distinct.*

Proof. Since Q is not a trap, we have $\phi^4(Q) \neq Q + 4P_0$. Hence the points $\sigma^0 Q, \sigma^0 R, \ldots, \sigma^3 Q, \sigma^4 R$ are pairwise distinct: clearly $\sigma^0 Q, \ldots, \sigma^3 Q$ are distinct and $\sigma^0 R, \ldots, \sigma^3 R$ are distinct and if we had $\sigma^i Q = \sigma^j R$, then, for $l := [k : \mathbb{F}_q]$ and $m := i - j$, we would have

$$\begin{aligned} Q + P_0 = \phi(R) = \phi(\sigma^{i-j} Q) = \phi(\phi^{l(i-j)} Q) = \phi^{lm+1}(Q) \\ \implies \quad \phi^4(Q) = \phi^{4(lm+1)}(Q) = Q + 4P_0\,. \end{aligned}$$

Figure 4.1: The intersections X_i of the curve $\mathcal{B}_P$ with certain lines $L_{i,j}, R_{i,j}$.



This implies that for any point $P \in \{\sigma^0 Q, \sigma^0 R, \ldots, \sigma^3 Q, \sigma^4 R\}$ there is exactly one of the rational functions $f_{\sigma^0 Q}, f_{\sigma^0 R}, \ldots, f_{\sigma^3 Q}, f_{\sigma^4 R}$ that has a pole in $-P$, namely f_P.

If the lines $\{L_{0,2} = 0\}$ and $\{L_{1,3} = 0\}$ are equal, then the matrix of their coefficients

$$n(P) = \begin{pmatrix} l_2 - l_0 & (f_Q - f_{\sigma^2 Q})(P) & (l_2 f_Q - l_0 f_{\sigma^2 Q})(P) \\ l_3 - l_1 & (f_{\sigma Q} - f_{\sigma^3 Q})(P) & (l_3 f_{\sigma Q} - l_1 f_{\sigma^3 Q})(P) \end{pmatrix}$$

has rank 1 hence, computing the deteminant of a submatrix of n, P is a zero of the rational function $(l_0 - l_2)(f_{\sigma^3 Q} - f_{\sigma Q}) - (l_1 - l_3)(f_{\sigma^2 Q} - f_Q)$. We have chosen $\widetilde{P}$ so that $l_0 \neq l_2$ and $l_1 \neq l_3$ hence this rational function is non-zero and has five poles counted with multiplicity. So it has at most five zeroes. Hence for all but at most five choices of $P \in E(k)$, the matrix $n(P)$ has rank 2 and consequently the lines $\{L_{0,2} = 0\}$ and $\{L_{1,3} = 0\}$ are distinct.

For any other pair of lines Λ, Λ' in Figure 4.1, one can prove with similar arguments that $\Lambda \neq \Lambda'$ for all but at most five choices of $P \in E(k)$. We prove that, for all $i \neq j$, we have $X_i \neq X_j$, for all but six choices of $P \in E(k)$. We treat only a couple of cases here.

If $X_9 = X_{12}$, then the lines $\{R_{1,3} = 0\}$, $\{R_{2,3} = 0\}$ and $\{L_{0,2} = 0\}$ are concurrent,

hence the following matrix, that contains their coefficients, is not invertible

$$M = M(P) = \begin{pmatrix} r_2 - r_0 & (f_R - f_{\sigma^2 R})(P) & (r_2 f_R - r_0 f_{\sigma^2 R})(P) \\ r_3 - r_2 & (f_{\sigma^2 R} - f_{\sigma^3 R})(P) & (r_3 f_{\sigma^2 R} - r_2 f_{\sigma^3 R})(P) \\ l_2 - l_0 & (f_Q - f_{\sigma^2 Q})(P) & (l_2 f_Q - l_0 f_{\sigma^2 Q})(P) \end{pmatrix},$$

implying that P is a zero of the rational function $\det(M)$. Writing out the $\det(M)$ we see that there is a rational function g, regular in $-\sigma^2 R$, such that

$$\det(M) = (l_2 - l_0)(r_0 - r_3) f_{\sigma^2 R}^2 + f_{\sigma^2 R}\, g\,,$$

and since $l_0 \neq l_2$ and $r_0 \neq r_3$ we deduce that $\det(M)$ has a pole of order 2 in $-\sigma^2 R$ and in particular $\det(M)$ is a non-zero rational function with at most 6 poles counted with multiplicity. Hence $\det(M)$ has at most 6 zeroes, implying that $X_9 \neq X_{12}$, for all but 6 choices of $P \in E(k)$.

If $X_3 = X_4$, then the lines $\{L_{0,1} = 0\}$, $\{L_{2,3} = 0\}$ and $\{R_{0,1} = 0\}$ are concurrent, hence the following matrix, that contains the coefficients of $L_{0,1}$, $L_{2,3}$ and $R_{0,1}$, is not invertible

$$N = N(P) = \begin{pmatrix} l_1 - l_0 & (f_Q - f_{\sigma Q})(P) & (l_1 f_Q - l_0 f_{\sigma Q})(P) \\ l_3 - l_2 & (f_{\sigma^2 Q} - f_{\sigma^3 Q})(P) & (l_3 f_{\sigma^2 Q} - l_2 f_{\sigma^3 Q})(P) \\ r_1 - r_0 & (f_R - f_{\sigma R})(P) & (r_1 f_R - r_0 f_{\sigma R})(P) \end{pmatrix}.$$

As before, in order to prove that $X_3 \neq X_4$ for all but at most 6 choices of $P \in E(k) \setminus \{O_E\}$ it is enough proving that $\det(N(P))$, considered as a rational function of P, is not identically zero. We suppose by contradiction that $\det(N)$ is identically zero and for each $i, j \in \{1, 2, 3\}$ we denote $N_{i,j}$ the (i, j)-minor of $N(P)$, considered as a rational function. Since $l_1 \neq l_0$, then $N_{3,3}$ has a simple pole in $\sigma^3 Q$ and consequently $N_{3,3} \neq 0$. Analogously $N_{1,3} \neq 0$ and $N_{2,3} \neq 0$, hence there are rational functions $A, B \in \overline{\mathbb{F}_q}(E)$ such that

$$\begin{cases} (l_1 - l_0) \cdot A + (f_Q - f_{\sigma Q}) \cdot B = l_1 f_Q - l_0 f_{\sigma Q} \\ (l_3 - l_2) \cdot A + (f_{\sigma^2 Q} - f_{\sigma^3 Q}) \cdot B = l_3 f_{\sigma^2 Q} - l_2 f_{\sigma^3 Q} \\ (r_1 - r_0) \cdot A + (f_R - f_{\sigma R}) \cdot B = r_1 f_R - r_0 f_{\sigma R} \end{cases} \tag{4.8.2.4}$$

and, using Cramer's rule, we have

$$B = \frac{N_{1,2}}{N_{1,3}} = \frac{N_{2,2}}{N_{2,3}} = \frac{N_{3,2}}{N_{3,3}}\,.$$

Using the same argument we used for $N_{3,3}$, we see that $N_{1,2}, N_{2,2}, N_{3,2} \neq 0$. Moreover it is easy to compute the poles of $N_{1,2}$, $N_{2,2}$, $N_{3,2}$, $N_{1,3}$, $N_{2,3}$, $N_{3,3}$ and check that they all vanish in $\widetilde{P}$ and O_E, using that for each $P \in E(\overline{\mathbb{F}_q}) \setminus \{O_E\}$ we have $(f_P - \frac{y}{x})(O_E) = 0$. Hence there are positive divisors $D_{l,m}$ of degree 2 on E such that, for each $j = 2, 3$

$$\begin{aligned}
\operatorname{div}(N_{1,j}) &= D_{1,j} + \widetilde{P} + O_E - (-R) - (-\sigma R) - (-\sigma^2 Q) - (-\sigma^3 Q)\,,\\
\operatorname{div}(N_{2,k}) &= D_{2,j} + \widetilde{P} + O_E - (-Q) - (-\sigma Q) - (-R) - (-\sigma R)\,,\\
\operatorname{div}(N_{3,j}) &= D_{3,j} + \widetilde{P} + O_E - (-Q) - (-\sigma Q) - (-\sigma^2 Q) - (-\sigma^3 Q)\,,
\end{aligned}$$

and consequently

$$\operatorname{div}(B) = D_{1,2} - D_{1,3} = D_{2,2} - D_{2,3} = D_{3,2} - D_{3,3}\,.$$

The functions f_Q, $f_{\sigma Q}$, $f_{\sigma^2 Q}$ and $f_{\sigma^3 Q}$ are $\overline{\mathbb{F}_q}$-linearly independent, hence $N_{1,2}$ and $N_{1,3}$ are not $\overline{\mathbb{F}_q}$-multiples. Hence B is not constant. Since every non-constant rational function on E has at least two poles, we deduce that $D_{1,3} = D_{2,3} = D_{3,3}$ is the divisor of poles of B. This implies that the sum, in the group $E(\overline{\mathbb{F}_q})$, of the poles of $N_{1,3}$ is equal to the sum of the poles of $N_{2,3}$ and is also equal to the sum of the poles of $N_{3,3}$. This implies that, in the group $E(\overline{\mathbb{F}_q})$, we have

$$Q + \sigma Q = \sigma^2 Q + \sigma^3 Q = R + \sigma R\,.$$

Hence, using (4.7.2.1), $-Q - \sigma Q$ is a zero of $N_{3,3}$ and consequently the two poles of B are $-Q - \sigma Q$ and $-Q - \sigma Q - \widetilde{P}$. By looking at (4.8.2.4) we deduce that A has exactly one simple pole, namely $-Q - \sigma Q - \widetilde{P}$, which is absurd. Hence $\det(N(P))$ is not identically zero. □

We now study the geometrically irreducible components of $\mathcal{B}_P$ assuming the conclusions of Claim 4.8.2.3. In other words, we avoid the small (compared to q) number of points $P \in E(k)$ such that the lines $L_{i,j}, R_{i,j}$ or the points X_i in Figure 4.1 are not distinct.

Using the equation defining $\mathcal{B}_P$, we can compute the divisor-theoretic intersection

$$\mathcal{B}_P \cap \{L_{0,2} = 0\} = X_1 + X_5 + qX_9 + qX_{13}\,. \tag{4.8.2.5}$$

This intersection contains the point X_1 with multiplicity 1, hence X_1 is a smooth point of $\mathcal{B}_P$. With analogous arguments we can prove that all the points X_i in the figure except the ones of the shape $\{R_{i,j} = 0\} \cap \{R_{l,m} = 0\}$ are smooth points. This helps us studying the geometrically irreducible components of $\mathcal{B}_P$, as in the following Claim.

Claim 4.8.2.6. *Assume the conclusions of Claim 4.8.2.3 hold. The curve $\mathcal{B}_P$ does not contain any conic defined over k.*

Proof. Suppose $F \in k[\alpha, \beta, \gamma]$ is a quadratic equation defining a conic contained in $\mathcal{B}_P$. Since X_9 is a smooth point of $\mathcal{B}_P$, if the conic $\{F = 0\}$ contains X_9, then $\{F = 0\}$ is the only component of $\mathcal{B}_P$ passing through X_9, hence X_9 appears in $\mathcal{B}_P \cap \{L_{0,2} = 0\}$ with multiplicity at most $2 < q$, contradicting Equation (4.8.2.5). Hence $\{F = 0\}$ does not contain X_9 nor, by a similar argument, X_{13}.

This, together with Equation (4.8.2.5), implies that X_1 and X_5 belong to $\{F = 0\}$. Analogously X_2 and X_6 belong to $\{F = 0\}$. Both the conics $\{L_{0,1}L_{2,3} = 0\}$ and $\{L_{0,2}L_{1,3} = 0\}$ pass through the points X_1, X_2, X_5, X_6, hence, using that X_1, X_2, X_5, X_6 are in general position, there are $\lambda_0, \lambda_1 \in \overline{\mathbb{F}_q}$ such that

$$F = \lambda_0 L_{0,1}L_{2,3} + \lambda_1 L_{0,2}L_{1,3}\,.$$

We extend σ to an element in $\mathrm{Gal}(\overline{\mathbb{F}_q}/k)$ and we look at the action of σ on $\overline{\mathbb{F}_q}[\alpha, \beta, \gamma]$. For each $i, j \in \{0, 1, 2, 3\}$ we have $\sigma L_{i,j} = L_{i+1,j+1} = -L_{j+1,i+1}$, considering the indices modulo 4, hence

$$\lambda_0 L_{0,1}L_{2,3} + \lambda_1 L_{0,2}L_{1,3} = F = \sigma F = \sigma(\lambda_0)L_{2,3}L_{3,0} + \sigma(\lambda_1)L_{0,2}L_{1,3}\,.$$

Some cumbersome computations imply that the line $\{L_{1,2} = 0\}$ is the line through X_2 and X_5 and the line $\{L_{3,0} = 0\}$ is the line through X_1 and X_6. In particular the lines $\{L_{i,j} = 0\}$ appearing in the above equation are pairwise distinct. Hence $\lambda_0 = \sigma(\lambda_0) = 0$, and consequently $\{F = 0\} = \{L_{0,2}L_{1,3} = 0\}$, which is not contained in $\mathcal{B}_P$. Contradiction. □

Claim 4.8.2.6 implies that $\mathcal{B}_P$ does not contain a line of $\mathbb{P}^2$. Suppose that Λ is a line contained in $\mathcal{B}_P$. Neither X_9 nor X_{13} are contained in Λ since they are smooth points of $\mathcal{B}_P$ and, by Equation (4.8.2.5, the unique components of $\mathcal{B}_P$ passing through them must have degree at least q inside $\mathbb{P}^2$. Hence $\Lambda \cap \{L_{0,2} = 0\} \in \{X_1, X_5\}$ and consequently

$$(\Lambda \cup \sigma^2\Lambda) \cap \{L_{0,2} = 0\} = X_1 + X_5\,. \tag{4.8.2.7}$$

This implies that $\sigma^2\Lambda \neq \Lambda$ and that $\sigma^2\Lambda$ and Λ are all the $\mathrm{Gal}(\overline{\mathbb{F}_q}/k)$-conjugates of Λ: since $\mathcal{B}_P$ is defined over k, then all the $\mathrm{Gal}(\overline{\mathbb{F}_q}/k)$-conjugates of Λ are components of $\mathcal{B}_P$ and if Λ has a conjugate $\Lambda' \neq \Lambda, \sigma^2\Lambda$, then, by the same argument as before, $\Lambda' \cap \{L_{0,2} = 0\} \in \{X_1, X_5\}$ and this, together with Equation (4.8.2.7) contradicts the smoothness of X_1 and X_5. We deduce that $\Lambda \cup \sigma^2\Lambda$ is a conic defined over k and contained in $\mathcal{B}_P$, contradicting Claim 4.8.2.6.

By a similar argument, no conic $\mathcal{Q}$ is a component of $\mathcal{B}_P$: if this happens, since conics have degree $2 < q$ in $\mathbb{P}^2$, then X_9, X_{13} do not belong to any of the $\mathrm{Gal}(\overline{\mathbb{F}_q}/k)$-conjugates of $\mathcal{Q}$, thus, by Equation (4.8.2.5), for all $\tau \in \mathrm{Gal}(\overline{\mathbb{F}_q}/k)$ we have

$$\tau(\mathcal{Q}) \cap \{L_{0,2} = 0\} = X_1 + X_5 = \mathcal{Q} \cap \{L_{0,2} = 0\}$$

hence, by the smoothness of X_1 and X_5, $\mathcal{Q}$ is defined over k, contradicting Claim 4.8.2.6.

We now suppose that $\mathcal{B}_P$ is not geometrically irreducible. Let $\mathcal{B}_1, \ldots, \mathcal{B}_r$ be the geometrically irreducible components of $\mathcal{B}_P$. As we already proved, each $\mathcal{B}_i$ has degree at least 3, hence the intersection $\mathcal{B}_i \cap \{L_{0,2} = 0\}$ is a sum of at least 3 points counted with multiplicity. By Equation (4.8.2.5), this implies that $\mathcal{B}_i$ is passing through X_9 or X_{13} hence each $\mathcal{B}_i$ has degree at least q. Since the sum of the degrees of the $\mathcal{B}_i$'s is equal to $2q+2 < 3q$, we deduce that $r = 2$ and that either $\deg(\mathcal{B}_1) = \deg(\mathcal{B}_2) = q+1$ or, up to reordering, $\deg(\mathcal{B}_1) = q$ and $\deg(\mathcal{B}_2) = q+2$.

If $\deg(\mathcal{B}_1) = \deg(\mathcal{B}_2) = q+1$, Equation (4.8.2.5) implies that, up to reordering, $X_1 \in \mathcal{B}_1(\overline{\mathbb{F}_q})$ and $X_5 \in \mathcal{B}_2(\overline{\mathbb{F}_q})$. Since $\mathcal{B}_P$ is defined over k, then $\mathrm{Gal}(\overline{\mathbb{F}_q}/k)$ acts on $\{\mathcal{B}_1, \mathcal{B}_2\}$ and because of the cardinality of such a set, then σ^2 acts trivially. In particular $X_5 = \sigma^2 X_1$ belongs to $\sigma^2\mathcal{B}_1(\overline{\mathbb{F}_q}) = \mathcal{B}_1(\overline{\mathbb{F}_q})$, hence $X_5 \in \mathcal{B}_1(\overline{\mathbb{F}_q}) \cap \mathcal{B}_2(\overline{\mathbb{F}_q})$, contradicting the smoothness of X_5. This contradiction implies that

$$\deg(\mathcal{B}_1) = q, \quad \deg(\mathcal{B}_2) = q+2\,.$$

For each linear polynomial $L = l_\alpha\alpha + l_\beta\beta + l_\gamma\gamma$ such that $l_\alpha \neq 0$ and for each polynomial $F(\alpha,\beta,\gamma) \in \overline{\mathbb{F}_q}[\alpha,\beta,\gamma]$ we define

$$F|_L = F\left(-\frac{l_\beta\beta + l_\gamma\gamma}{l_\alpha}, \beta, \gamma\right),$$

so that $F|_L$ is the unique element of $\overline{\mathbb{F}_q}[\beta,\gamma]$ such that $F \equiv F|_L \bmod L$. If F is homogenous, then $F|_L$ is also homogenous. Notice that the hypothesis $l_\alpha \neq 0$ is true for $L = L_{i,j}$ when $i \neq j$, because, by the definition (4.8.2.1), the coefficient of α in $L_{i,j}$ is $f_{\sigma^i Q}(\tilde{P}) - f_{\sigma^j Q}(\tilde{P})$ and we have chosen $\tilde{P}$ so that $f_{\sigma^i Q}(\tilde{P}) \neq f_{\sigma^j Q}(\tilde{P})$.

For each $i \in \{1,2\}$ let $M_i \in \overline{\mathbb{F}_q}[\alpha,\beta,\gamma]$ be a homogeneous polynomial defining $\mathcal{B}_i$.

Claim 4.8.2.8. *There exists homogenous polynomials $F_1, F_2, G_2, N_1, N_2 \in \overline{\mathbb{F}_q}[\alpha,\beta,\gamma]$ of respective degree $1,1,1,q-4,q-2$ such that*

$$M_1 = F_1^q + L_{0,1}L_{2,3}L_{0,2}L_{1,3}N_1, \tag{4.8.2.9}$$

$$M_2 = F_2^q L_{0,1}L_{2,3} + G_2^q L_{0,2}L_{1,3} + L_{0,1}L_{2,3}L_{0,2}L_{1,3}N_2 \tag{4.8.2.10}$$

Proof. We start from the first part. Since $\deg \mathcal{B}_1 = q$ and since X_1, X_5, X_9 and X_{13} are smooth, Equation (4.8.2.5 implies that $\mathcal{B}_1 \cap \{L_{0,2} = 0\}$ is either qX_{13} or qX_9, hence $M_1|_{L_{0,2}}$ is the q-th power of a linear polynomial. We deduce the existence of polynomials $A_1, B_1 \in \overline{\mathbb{F}_q}[\alpha,\beta,\gamma]$ such that A_1 is linear homogenous and

$$M_1 = A_1^q + B_1 L_{0,2}\,.$$

Similarly to $\mathcal{B}_1 \cap \{L_{0,2} = 0\}$, we have that $\mathcal{B}_1 \cap \{L_{1,3} = 0\}$ is either qX_{14} or qX_{10}, hence there exists a linear polynomial $A_2 \in \overline{\mathbb{F}_q}[\beta, \gamma]$ such that

$$A_2^q = M_1|_{L_{1,3}} = A_1|_{L_{1,3}}^q + B_1|_{L_{1,3}} L_{0,2}|_{L_{1,3}} \quad \Longrightarrow \quad B_1|_{L_{1,3}} L_{0,2}|_{L_{1,3}} = (A_2 - A_1|_{L_{1,3}})^q.$$

In the last equation either both sides are zero or the right hand side gives the prime factorization of the left hand side (we use that $A_2 - A_1$ has degree at most 1 and that $\overline{\mathbb{F}_q}[\beta, \gamma]$ is a UFD). In both cases there exists $\lambda_1 \in \overline{\mathbb{F}_q}$ such that $B_1|_{L_{1,3}} = \lambda_1 L_{0,2}|_{L_{1,3}}^{q-1}$, hence

$$B_1 = \lambda_1 L_{0,2}^{q-1} + B_2 L_{1,3} \quad \Longrightarrow M_1 = (A_1 + \lambda_1 L_{0,2})^q + B_2 L_{0,2} L_{0,3} = A_3^q + B_2 L_{0,2} L_{0,3}$$

for certain homogenous polynomials $A_3, B_2 \in \overline{\mathbb{F}_q}[\alpha, \beta, \gamma]$, with A_3 linear. Similarly to $\mathcal{B}_1 \cap \{L_{0,2} = 0\}$, we have that $\mathcal{B}_1 \cap \{L_{0,1} = 0\}$ is either qX_3 or qX_4. Hence, using the piece of notation $l = L_{0,1}$, there exists a linear polynomial $A_4 \in \overline{\mathbb{F}_q}[\beta, \gamma]$ such that

$$A_4^q = M_1|_l = A_3|_l^q + B_2|_l \, L_{0,2}|_l \, L_{1,3}|_l \quad \Longrightarrow \quad B_2|_l \, L_{0,2}|_l \, L_{1,3}|_l = (A_4 - A_3|_l)^q.$$

Again, in the last equation either both sides are zero or the right hand side gives the prime factorization of the left hand side. The latter is not possible, since the points $X_1 = \{L_{0,1} = 0\} \cap \{L_{0,2} = 0\}$ and $X_2 = \{L_{0,1} = 0\} \cap \{L_{1,3} = 0\}$ are distinct and consequently $L_{0,2}|_l$ and $L_{1,3}|_l$ are relatively prime. We deduce that $B_2|_l = 0$, or equivalently B_2 is divisible by $L_{0,1}$. A similar argument proves that B_2 is also divisible by $L_{2,3}$, implying Equation (4.8.2.9).

Since $\deg \mathcal{B}_2 = q + 2$ and since X_1, X_5, X_9 and X_{13} are smooth, Equation (4.8.2.5) implies that $\mathcal{B}_2 \cap \{L_{0,2}\}$ is either $X_1 + X_5 + qX_{13}$ or $X_1 + X_5 + qX_9$, hence

$$M_1|_{L_{0,2}} = L_{0,1}|_{L_{0,2}} L_{2,3}|_{L_{0,2}} A_5^q \quad \Longrightarrow \quad M_2 = A_5^q L_{0,1} L_{2,3} + B_3 L_{0,2},$$

for some homogenous polynomials $A_5, B_3 \in \overline{\mathbb{F}_q}[\alpha, \beta, \gamma]$, with A_5 linear. In a similar fashion we have $\mathcal{B}_2 \cap \{L_{1,3}\}$ is either $X_2 + X_6 + qX_{14}$ or $X_2 + X_6 + qX_{10}$, hence, using the piece of notation $r = L_{1,3}$, we have

$$\begin{aligned} L_{0,1}|_r L_{2,3}|_r A_6^q = M_1|_r = L_{0,1}|_r L_{2,3}|_r A_5|_r^q + B_3|_r L_{0,2}|_r \\ \Longrightarrow \quad B_3|_r L_{0,2}|_r = L_{0,1}|_r L_{2,3}|_r (A_6 - A_5)|_r^q \end{aligned}$$

Again, in the last equation either both sides are zero or the right hand side gives the prime factorization of the left hand side. In both cases $B_3|_{L_{1,3}}$ is a scalar multiple of $L_{0,1}|_r L_{2,3}|_r L_{0,2}|_r^{q-1}$: in the last case this is obvious, in the first case we use that, since X_1, X_2, X_5 and X_6 are distinct, the polynomials $L_{0,1}|_r$, $L_{2,3}|_r$ and $L_{0,2}|_r$ are relatively

prime. Hence there exist homogenous polynomials $A_7, B_4 \in \overline{\mathbb{F}_q}[\alpha,\beta,\gamma]$ such that A_7 is linear and

$$M_2 = A_7^q L_{0,2} L_{1,3} + B_4 L_{0,1} L_{2,3}.$$

Iterating similar arguments we prove Equation 4.8.2.10. □

Let F_1, F_2, G_1, N_1 and N_2 as in Claim 4.8.2.8. Up to multiplying M_1 with an element of $\overline{\mathbb{F}_q}^\times$, we can suppose that $M = M_1 M_2$. Reducing this equality modulo $L_{0,2}L_{1,3}$ we see that

$$L_{0,2}L_{1,3} \text{ divides } L_{0,1}L_{2,3}(F_1F_2 + R_{0,2}R_{1,3})^q.$$

The linear polynomials $L_{i,j}$ in the above equation are coprime since they define distinct lines. Hence $L_{0,2}L_{1,3}$ divides $F_1F_2+R_{0,2}R_{1,3}$. Since $F_1F_2+R_{0,2}R_{1,3}$ is homogenous of degree at most 2, then it is a scalar multiple of $L_{0,2}L_{1,3}$. Using a similar argument with $L_{0,1}L_{2,3}$ we prove that there exist $\lambda, \mu \in \mathbb{F}_q$ such that

$$F_1F_2 + R_{0,2}R_{1,3} = \lambda L_{0,2}L_{1,3}, \quad F_1G_2 - R_{0,1}R_{2,3} = \mu L_{0,1}L_{2,3}\,. \tag{4.8.2.11}$$

We have $\lambda \neq 0$, otherwise F_1 would be a scalar multiple of either $R_{0,2}$ or $R_{1,3}$: in the first case Equation 4.8.2.9 would imply that $\mathcal{B}_1$ contains X_9 but not $X_{14} = \tau(X_9)$, implying that $\tau(\mathcal{B}_1)$ is a component of $\mathcal{B}$ different from $\mathcal{B}_1$, that is $\tau(\mathcal{B}_1) = \mathcal{B}_2$ which contradicts the inequality $\deg(\mathcal{B}_2) > \deg(\mathcal{B}_1)$; in the second case Equation 4.8.2.9 would imply that $\mathcal{B}_1$ contains X_{13} but not $X_{10} = \tau(X_{13})$, leading to the same contradiction.

Using Equations (4.8.2.9), (4.8.2.10) and (4.8.2.11) and the equality $M_1M_2{=}M$, we see that

$$\begin{aligned} 0 &= \frac{M_1M_2 - M}{L_{0,1}L_{2,3}L_{0,2}L_{1,3}} = \\ &= \mu^q L_{0,1}^{q-1}L_{2,3}^{q-1} + \lambda^q L_{0,2}^{q-1}L_{1,3}^{q-1} + F_1^q N_2 + F_2^q N_1 L_{0,1}L_{2,3} + G_2^q N_1 L_{0,2}L_{1,3} + N_1N_2L_{0,1}L_{2,3}L_{0,2}L_{1,3} \\ &\equiv \lambda^q (L_{0,2}L_{1,3})^{q-1} + F_1^q N_2 + G_2^q N_1 L_{0,2}L_{1,3} \pmod{L_{0,1}}. \end{aligned}$$

For any $F \in \overline{\mathbb{F}_q}[\alpha,\beta,\gamma]$ we define $\tilde{F} := F_{L_{0,1}}$ and we rewrite the above congruence as

$$\lambda^q \tilde{L}_{0,2}^{q-1}\tilde{L}_{1,3}^{q-1} + \tilde{F}_1^q \tilde{N}_2 + \tilde{G}_2^q \tilde{N}_1 \tilde{L}_{0,2}\tilde{L}_{1,3} = 0. \tag{4.8.2.12}$$

Since then $\mathcal{B}_1 \cap L_{0,1}$ does not contain the point $X_1 = \{L_{0,2}{=}0\} \cap \{L_{0,1}{=}0\}$ nor the point $X_3 = \{L_{1,3}{=}0\} \cap \{L_{0,1}{=}0\}$, then $\tilde{F}_1$ is relatively prime with both $\tilde{L}_{0,2}$ and $\tilde{L}_{1,3}$. Hence both $\tilde{L}_{0,2}$ and $\tilde{L}_{1,3}$ divide $\tilde{N}_2$. Since $X_1 = \{L_{0,2}{=}0\} \cap \{L_{0,1}{=}0\}$ and $X_3 = \{L_{1,3}{=}0\} \cap \{L_{0,1}{=}0\}$ are distinct, then $\tilde{L}_{0,2}$ is relatively prime with $\tilde{L}_{1,2}$ and we can write $\tilde{N}_2 = \tilde{L}_{0,2}\tilde{L}_{1,3}N_3$ for some homogenous polynomial $N_3 \in \overline{\mathbb{F}_q}[\beta,\gamma]$. Substituting in Equation 4.8.2.12 we have

$$\lambda^q \tilde{L}_{0,2}^{q-2}\tilde{L}_{1,3}^{q-2} + \tilde{F}_1^q N_3 + \tilde{G}_2^q \tilde{N}_1 = 0.$$

Since $\lambda \neq 0$, since all the polynomials of the form $\tilde{F}$ are contained in $\overline{\mathbb{F}_q}[\beta,\gamma]$ and since $\tilde{L}_{0,2}$ is relatively prime with $\tilde{L}_{1,2}$, the above equation contradicts Lemma 4.8.2.13 below.

In particular the assumption of the reducibility of $\mathcal{B}$ led to contradiction, together with the conclusions of Claim 4.8.2.3. We deduce that for all but at most 450 choices of $P \in E(k)$ the curve $\mathcal{B}_P$ is geometrically irreducible. Since $\#E(k) > 450$ and since all the components of $\mathcal{B}$ project surjectively to E, we deduce that $\mathcal{B}$ is reduced and geometrically irreducible.

Lemma 4.8.2.13. *Let $L_1, L_2 \in \overline{\mathbb{F}_q}[\beta,\gamma]$ be relatively prime homogenous linear polynomials. Then there exist no homogenous polynomial $A, B, C, D \in \overline{\mathbb{F}_q}[\beta,\gamma]$ such that*

$$L_1^{q-2} L_2^{q-2} = A^q B + C^q D.$$

Proof. The zeroes of L_1 and L_2 in $\mathbb{P}^1$ are distinct, hence, up to a linear transformation we can suppose that their zeroes are 0 and ∞. In particular, up to scalar multiples we can suppose $L_1 = \beta$ and $L_2 = \gamma$, implying that $A^q B + C^q D = \beta^{q-2}\gamma^{q-2}$. This is absurd because any monomial appearing in A^q or in B^q is either a multiple of β^q of a multiple of γ^q, hence the same is true for all the monomials appearing in $A^q B + C^q D$. □

4.8.3 The irreducible components of $\mathcal{C}$

In this subsection we prove that all the geometrically irreducible components of $\mathcal{C}$ are defined over k. To do so, we can ignore (4.8.1.6) in the definition of $\mathcal{C}$. The strategy is applying Lemma 4.6.6 to the variety $\mathcal{B}$, using the rational functions

$$\begin{aligned} u_1, u_2, u_3 \colon \mathcal{B} \dashrightarrow \mathbb{P}^1\,, \qquad & u_i(\alpha,\beta,1,P) = f_{\alpha,\beta,P}(\sigma^{i-1}Q)\,, \\ w_1, w_2, w_3 \colon \mathcal{B} \dashrightarrow \mathbb{P}^1\,, \qquad & w_i(\alpha,\beta,1,P) = -f_{\alpha,\beta,P}(\sigma^{i-1}R)\,, \end{aligned}$$

and the irreducible divisor $Z \subset \mathcal{B}$ being the Zariski closure of

(4.8.3.1)

$$\left\{ (\alpha,\beta,P) \in (\mathbb{A}^2 \times E')(\overline{\mathbb{F}_q}) : \begin{array}{c} P = -Q - \sigma Q - \sigma^3 Q - \widetilde{P}\,, \\ \alpha = \big((f_Q(P) - f_{\sigma Q}(P))\beta + l_1 f_Q(P) - l_0 f_{\sigma Q}(P)\big)/(l_0 - l_1) \end{array} \right\}.$$

Claim 4.8.3.2. *The variety Z is generically contained in the smooth locus of $\mathcal{B}$ and the rational function $u_1 - u_2$ vanishes on Z with multiplicity 1.*

Proof. We restrict to an open subset $U \subset \mathbb{P}^2 \times E$ containing the generic point of Z. Up to shrinking U, the rational functions u_i, w_i can be extended to regular functions on U using the definition (4.8.1.1) of $f_{\alpha,\beta,P}$, and we have

$$u_1 - u_2 = \frac{L_{0,1}(\alpha,\beta,1,P)}{\big(l_0+\beta\big)\big(l_1+\beta\big)}\,,$$

where $L_{i,j}(\alpha,\beta,\gamma,P) \in \overline{\mathbb{F}_q}[U]$ is defined as in (4.8.2.1), as well as $R_{i,j}(\alpha,\beta,\gamma,P)$. Since we can assume that $l_0+\beta, l_1+\beta$ are invertible on U and since Z is generically smooth, it is enough showing that $Z\cap U$ is a component of $(\mathcal{B}\cap U)\cap\{L_{0,1}=0\}$ having multiplicity one. Up to shrinking U, the closed $\mathcal{B}\cap U\subset U$ is the vanishing locus of

$$M(\alpha,\beta,P) := (L_{0,2}L_{1,3}R_{0,1}^qR_{2,3}^q - L_{0,1}L_{2,3}R_{0,2}^qR_{1,3}^q)(\alpha,\beta,1,P) \quad \in \overline{\mathbb{F}_q}[U]\,.$$

Since the restriction of M to $\{L_{0,1}=0\}$ is equal to the restriction of $L_{0,2}L_{1,3}R_{0,1}^qR_{2,3}^q$, it is enough showing that $L_{0,2}$, $R_{0,1}$, $R_{2,3}$ do not vanish on Z and that $\{L_{1,3}=0\}\cap\{L_{0,1}=0\}$ contains $Z\cap U$ with multiplicity 1. We start from the latter. Eliminating the variable α we see that, up to shrinking U, $\{L_{1,3}=0\}\cap\{L_{0,1}=0\}$ is defined by the equations

$$\lambda(P)=0 \quad\text{and}\quad (l_1-l_0)\alpha+(f_Q(P)-f_{\sigma Q}(P))\beta+l_1f_Q(P)-l_0f_{\sigma Q}(P)=0\,, \tag{4.8.3.3}$$

where

$$\lambda(P) := (l_1-l_0)f_{\sigma^3Q}(P)+(l_3-l_1)f_Q(P)+(l_0-l_3)f_{\sigma Q}(P) \quad \in \overline{\mathbb{F}_q}(E)\,.$$

The function λ has three simple poles, namely $-Q,-\sigma Q,-\sigma^3Q$, and we easily verify that $\lambda(\widetilde{P})=\lambda(O_E)=0$. We deduce that $P=-Q-\sigma Q-\sigma^3Q-P_0$ is a simple zero of λ. This, together with the fact that the second equation in (4.8.3.3) is equal to the second equation in the definition (4.8.3.1) of Z, implies that $\{L_{1,3}=0\}\cap\{L_{0,1}=0\}$ contains $Z\cap U$ with multiplicity 1.

We now suppose by contradiction that $R_{0,1}$ vanishes on $Z\cap U$. Substituting α and P in $R_{0,1}$ as in the definition (4.8.3.1) of Z, we see that

$$R_{0,1}(\alpha,\beta,1,P)|_{Z\cap U} = \frac{\lambda_0(-Q-\sigma Q-\sigma^3Q-\widetilde{P})}{l_0-l_1}\beta + \frac{\lambda_1(-Q-\sigma Q-\sigma^3Q-\widetilde{P})}{l_0-l_1}\,,$$

where

$$\begin{aligned}\lambda_0(P) :=& (r_1-r_0)(f_Q-f_{\sigma Q})(P)-(l_1-l_0)(f_R-f_{\sigma R})(P)\,,\\ \lambda_1(P) :=& (r_1-r_0)(l_1f_Q(P)-l_0f_{\sigma Q}(P))-(l_1-l_0)(r_1f_R(P)-r_0f_{\sigma R}(P))\,,\end{aligned}$$

and we deduce that both λ_0 and λ_1 vanish on $P=-Q-\sigma Q-\sigma^3Q-\widetilde{P}$. Both λ_0 and λ_1 have 4 poles and 4 zeroes counted with multiplicity: they have the same poles they share three zeroes, namely $O_E,\widetilde{P}$ and $-Q-\sigma Q-\sigma^3Q-\widetilde{P}$. Since, in the group on $E(\overline{\mathbb{F}_q})$, the sum of the zeroes of an element of $\overline{\mathbb{F}_q}(E)^\times$ is equal to the sum of the poles, then λ_0 and λ_1 also share the fourth zero, hence λ_0 and λ_1 differ by a multiplicative constant in $\overline{\mathbb{F}_q}$. This is absurd because $l_0\neq l_1$ and because the functions f_Q, $f_{\sigma Q}$, f_R, $f_{\sigma R}$ are $\overline{\mathbb{F}_q}$-independent.

A similar argument implies that $R_{2,3}$ does not vanish on $Z \cap U$, while the case of $L_{0,2}$ is easier. Substituting α and P in $L_{0,2}(\alpha, \beta, 1, P)$ as in the definition (4.8.3.1) of Z we get

$$L_{0,2}(\alpha, \beta, 1, P)|_{Z\cap U} = \frac{(\beta + l_0)\lambda_2(-Q-\sigma Q-\sigma^3 Q-\widetilde{P})}{l_0 - l_1},$$

where

$$\lambda_2(P) := (l_2-l_1)f_Q(P) + (l_0-l_2)f_{\sigma Q}(P) + (l_1-l_0)f_{\sigma^2 Q}(P) \quad \in \overline{\mathbb{F}_q}(E).$$

Analogously to λ, we see that the zeroes of λ_2 are $\widetilde{P}, O_E$ and $-Q-\sigma Q-\sigma^2 Q-P_0$, hence λ_2 does not vanish on $-Q-\sigma Q-\sigma^3 Q-P_0$, implying that $L_{0,2}$ does not vanish on $Z \cap U$. □

We can show that u_2-u_3, w_3+u_3, w_3+u_1 and w_i-w_j do not vanish on $Z \cap U$ with similar arguments to the ones used to prove that $R_{0,1}$ and $L_{0,2}$ do not vanish on Z. Hence we can apply Lemma 4.6.6 and deduce that all the components of $\mathcal{C}$ are defined over k.

4.8.4 k-rational points on $\mathcal{C}$

Finally we prove that $\#\mathcal{C}(k)$ is larger than $\frac{1}{2}(\#k)^2$. The surface $\mathcal{C}$ is contained in the open subset of $\mathbb{A}^2 \times (E\backslash\{O_E\}) \times \mathrm{PGL}_2 \times \mathbb{A}^1$ made of points $(\alpha, \beta, (x, y), \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), z)$ such that $c \neq 0$. Hence $\mathcal{C}$ is contained in $\mathbb{A}^8$, with variables α, β, x, y, a, b, d, z and it is defined by the following equations:.

- $0 = p_1 := W(x, y)$, the Weierstrass equation defining E;
- $0 = p_2 := (d^q-a)^{q+1}(z^q-z)^{q^2-q} - (ad-b)^q(\frac{z^{q^2}-z}{z^q-z})^{q+1}$, the dehomogenization of (4.8.1.2) in c;
- $0 = p_i(\alpha, \beta, x, y, a, b, d)$ for $i = 3, 4, 5, 6$, obtained by (4.8.1.3) after dehomogenizing in c, substituting $f_{\sigma^i Q}, f_{\sigma^i R}$ by their expressions in α, β, x, y and clearing denominators;
- a number of conditions $0 \neq q_j$ ensuring that $P \neq -\sigma^i Q, P \neq -\sigma^i R$, $\beta + f_{\widetilde{P}}(\sigma^i Q) \neq 0$, $\beta + f_{\widetilde{P}}(\sigma^i R) \neq 0$, $d^q - a \neq 0$, $ad - b \neq 0$, that (4.8.1.6) is satisfied, that $f_{\alpha,\beta,P}(\sigma^i Q)$ are distinct and that $f_{\alpha,\beta,P}(\sigma^i R)$ are distinct.

In particular, $\mathcal{C}$ can be seen as a closed subvariety of $\mathbb{A}^9$, with variables α, β, x, y, b, c, d, z and t defined by the seven equations $p_1 = 0, \ldots, p_6 = 0$ and $0 = p_7 := tq_1 \cdots q_r - 1$. Let $\mathcal{C}_1, \ldots, \mathcal{C}_s$ be the geometrically irreducible components of $\mathcal{C}$. By [46, Remark 11.3], we have

$$\#\mathcal{C}(k) \geq \#\mathcal{C}_1(k) \geq (\#k)^2 - (\delta-1)(\delta-2)(\#k)^{\frac{3}{2}} - K(\mathcal{C}_1)(\#k), \tag{4.8.4.1}$$

where δ is the degree of $\mathcal{C}_1$ and $K(\mathcal{C}_1)$ is the sum of the Betti numbers of $\mathcal{C}$ relative to the compact ℓ-adic cohomology. Since $\mathcal{C}_1$ is a component of $\mathcal{C}$ then

$$\delta \leq \deg(p_1) \cdots \deg(p_7)\,. \tag{4.8.4.2}$$

Since $\mathcal{C}$ is the disjoint union of the $\mathcal{C}_i$, the Betti numbers of $\mathcal{C}$ are the sums of the Betti numbers of the $\mathcal{C}_i$. Hence, using [58, Corollary of Theorem 1]

$$K(\mathcal{C}_1) \leq K(\mathcal{C}) \leq 6 \cdot 2^7 \cdot \left(3 + 7 \max_{i=1,\ldots,7}\{\deg(p_i)\}\right)^{10}\,. \tag{4.8.4.3}$$

Combining Equations (4.8.4.1), (4.8.4.2) and (4.8.4.3) and the inequalities $\deg p_1 \leq 3$, $\deg p_2 \leq q^3{+}q$, $\deg p_3, \ldots, \deg p_6 \leq 2q{+}3$, $\deg p_7 \leq 16q^2{+}37q{+}75$, we deduce that $\#\mathcal{C}(k) > \frac{1}{2}(\#k)^2$ when $\#k \geq q^{80}$ and $q \geq 3$.

Bibliography

[1] D. Abramovich, *A linear lower bound on the gonality of modular curves.* International Mathematics Research Notices, 20 (1996) no. 20, 1005-1011

[2] M. Akbas, D. Singerman, *The normalizer of* $\Gamma_0(N)$ *in* $\mathrm{PSL}(2,\mathbf{R})$. Glasgow Mathematical Journal, 32 (1990) no. 3, 317-327

[3] M.F. Atiyah, I.G. Macdonald, *Introduction to commutative algebra.* Addison–Wesley Publishing Co., Reading, Mass.–London–Don Mills, Ont. 1969

[4] A. O. L. Atkin, J. Lehner, *Hecke operators on* $\Gamma_0(m)$. Mathematische Annalen, 185 (1970), 134-160

[5] M. Baker, Y. Hasegawa, *Automorphisms of* $X_0^*(p)$. Journal of Number Theory, 100 (2003) no. 1, 72-87

[6] J. Balakrishnan, A. Besser, F. Bianchi, J. Steffen Müller, *Explicit quadratic Chabauty over number fields.* `https://arxiv.org/abs/1910.04653`

[7] J. Balakrishnan, F. Bianchi, V. Cantoral-Farfán, M. Çiperiani, and A. Etropolski, *Chabauty–Coleman experiments for genus 3 hyperelliptic curves.* Research Directions in Number Theory, Association for Women in Mathematics Series, Vol. 19, Springer, 2019, 67–90.

[8] J. Balakrishnan, N. Dogra, *Quadratic Chabauty and rational points, I: p-adic heights.* With an appendix by J. Steffen Müller. Duke Math. J. 167 (2018), no. 11, 1981–2038.

[9] J. Balakrishnan, N. Dogra, *An effective Chabauty-Kim theorem.* Compos. Math. 155 (2019), no. 6, 1057–1075.

[10] J. Balakrishnan, N. Dogra, J.S. Müller, J. Tuitman, J. Vonk, *Explicit Chabauty-Kim for the split Cartan modular curve of level 13.* Ann. of Math. (2) 189 (2019), no. 3, 885–944.

[11] B. Baran, *Normalizers of non-split Cartan subgroups, modular curves.* Journal of Number Theory, 130 (2010) no. 12, 2753-2772

[12] B. Baran, *A modular curve of level 9 and the class number one problem.* Journal of Number Theory, 129 (2009) no. 3, 715-728

[13] B. Baran, *An exceptional isomorphism between modular curves of level 13.* Journal of Number Theory, 145 (2014), 273-300,

[14] F. Bars, *The group structure of the normalizer of* $\Gamma_0(N)$ *after Atkin-Lehner.* Communications in Algebra, 36 (2008) no. 6, 2160-2170

[15] E. Berlekamp, *Factoring polynomials over large finite fields.* Math. Comp. 24 (1970), 713- 735.

[16] D. Bertrand, B. Edixhoven, *Pink's conjecture on unlikely intersections and families of semi-abelian varieties.* `https://arxiv.org/abs/1904.01788`

[17] Y. Bilu, P. Parent, *Serre's uniformity problem in the split Cartan case.* Annals of Mathematics. Second Series, 173 (2011) no. 1, 569-584

[18] Y. Bilu, P. Parent, M. Rebolledo, *Rational points on* $X_0^+(p^r)$. Université de Grenoble. Annales de l'Institut Fourier, 63 (2013) no. 3, 957-984

[19] R. Barbulescu , P. Gaudry, A. Joux, E. Thomé, *A quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic.* Annual International Conference on the Theory and Applications of Cryptographic Techniques (2014), 1-16.

[20] A. Besser, *p-adic Arakelov theory.* J. Number Theory, 111 (2005), no. 2, 318—371.

[21] A. Betts, *The motivic anabelian geometry of local heights on abelian varieties.*
`https://arxiv.org/abs/1706.04850`

[22] S. Bosch, W. Lütkebohmert, M. Raynaud, *Néron models.* Ergebnisse der Mathematik und ihrer Grenzgebiete (3) 21. Springer-Verlag, Berlin, 1990.

[23] A. W. Bluher, *On $x^{q+1} + ax + b$.* Finite Fields and Their Applications 10 (2004) No. 3, 285–305.

[24] C. Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur á l'unité.* C. R. Acad. Sci. Paris 212 (1941), 882–885.

[25] I. Chen, *The Jacobians of non-split Cartan modular curves.* Proceedings of the London Mathematical Society. Third Series, 77 (1998) no. 1, 1-38

[26] I. Chen, *Jacobians of modular curves associated to normalizers of Cartan subgroups of level p^n.* Comptes Rendus Mathématique. Académie des Sciences. Paris, 339 (2004) no. 3, 187-192

[27] Q. Cheng, D. Wan, J. Zhuang, *Traps to the BGJT-algorithm for discrete logarithms.* LMS Journal of Computation and Mathematics 17 (2014), 218-229.

[28] R. Coleman, G. Gross, *p-adic heights on curves.* Algebraic number theory, 73–81 Adv. Stud. Pure Math., 17 (1989).

[29] P. Coupek, D. Lilienfeldt, L. Xiao, Z. Yao, *Geometric quadratic Chabauty over number fields.* `http://www.math.mcgill.ca/lilien/Chabauty-Part1.pdf`

[30] J. M. Couveignes, R. Lercier, *Elliptic periods for finite fields.* Finite Fields and Their Applications, 15 (2009) No. 1, 1–22.

[31] P. Deligne, *La conjecture de Weil II.* Publ. Math. I.H.E.S. 52 (1981), 313-428

[32] P. Deligne, M. Rapoport, *Les schémas de modules de courbes elliptiques.* Modular functions of one variable, II, (1972), 143-316

[33] W. Diffie, M. Hellman, *New directions in cryptography.* IEEE Trans. Inform. Theory 22 (1976).

[34] N. Dogra, *Unlikely intersections and the Chabauty-Kim method over number fields.*
`https://arxiv.org/abs/1903.05032`

[35] V. Dose, J. Fernández, J. González, R. Schoof, *The automorphism group of the non-split Cartan modular curve of level 11.* Journal of Algebra, 417 (2014), 95-102

[36] V. Dose, P. Mercuri, C. Stirpe, *Double covers of Cartan modular curves.* Journal of Number Theory, 195 (2019), 96-114

[37] V. Dose, *On the automorphisms of the nonsplit Cartan modular curves of prime level.* Nagoya Mathematical Journal, 224 (2016) no. 1, 74-92

[38] F. Diamond, J. Shurman, *A first course in modular forms.* Graduate Texts in Mathematics (2005), Springer-Verlag, New York, xvi+436

[39] B. de Smit, B. Edixhoven, *Sur un résultat d'Imin Chen.* Mathematical Research Letters, 7 (2000) no. 2-3, 147-153

[40] B. Edixhoven, *Geometric quadratic Chabauty.* Lectures at the Arizona Winter School 2020.
`http://swc.math.arizona.edu/index.html`

[41] A. Grothendieck and J. Dieudonné, *Eléments de Géométrie Algébrique I. Le langage des schémas.* Inst. Hautes Études Sci. Publ. Math. 4 (1960)

[42] N. D. Elkies, *The automorphism group of the modular curve* $X_0(63)$. Compositio Mathematica, 74 (1990) no. 2, 203-208, `http://www.numdam.org/item?id=CM_1990__74_2_203_0`

[43] G. Faltings. *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern.* Invent. Math. 73 (1983), no. 3, 349–366.

[44] V. Flynn, *A flexible method for applying Chabauty's theorem.* Compositio Math. 105 (1997), no. 1, 79–94.

[45] A. Fröhlich, *Formal groups.* Vol 74. Springer–Verlag, Berlin–New York, 1957.

[46] S.R. Ghorpade, G. Lachaud, *Étale cohomology, Lefschetz theorems and number of points of singular varieties over finite fields.* Moscow Mathematical Journal 2 (2002) No. 3, 589-631.

[47] J. González, *Automorphism group of split Cartan modular curves.* Bulletin of the London Mathematical Society, 48 (2016) no. 4, 628-636

[48] J. González, *Constraints on the automorphism group of a curve.* Journal de Théorie des Nombres de Bordeaux, 29 (2017) no. 2, 535-548, `http://jtnb.cedram.org/item?id=JTNB_2017__29_2_535_0`

[49] R. Granger, T. Kleinjung, J. Zumbrägel, *On the discrete logarithm problem in finite fields of fixed characteristic*. Transactions of the American Mathematical Society 370 (2018) No. 5, 3129-3145.

[50] *Database of finite groups of small order*. `http://groupnames.org`

[51] S. Hashimoto, *Cartoon guide to finding $\mathbb{Q}$-points with geometric quadratic Chabauty*. `https://github.com/sachihashimoto/cartoon-guide-gqc`

[52] M. C. Harrison, *A New Automorphism Of $X_0(108)$*. ArXiv preprint 1108.5595 (2011)

[53] Y. Hasegawa, *Table of quotient curves of modular curves $X_0(N)$ with genus 2*. Proc. Japan Acad. Ser. A Math. Sci. 71 (1995), no. 10, 235–239 (1996).

[54] T. Honda, *On the theory of commutative formal groups*. Journal of the Mathematical Society of Japan Vol. 22 no. 2 (1970). `https://projecteuclid.org/euclid.jmsj/1259942752`

[55] Ivić, A., *Two inequalities for the sum of divisors functions*. Univ. u Novom Sadu Zb. Rad. Prirod.-Mat. Fak., 7 (1997), 17-22

[56] A. Joux, *A new index calculus algorithm with complexity L(1/4+o(1)) in small characteristic*. Conference on Selected Areas in Cryptography (2013), 355-379.

[57] A. Joux, C. Pierrot, *Algorithmic aspects of elliptic bases in finite field discrete logarithm algorithms*. arXiv preprint 1907.02689 (2019).

[58] N. M. Katz, *Sums of Betti numbers in arbitrary characteristic*. Finite Fields and their Applications 7 (2001) No. 1, 29-44.

[59] N. Katz B. Mazur, *Arithmetic moduli of elliptic curves*. Annals of Mathematics Studies, 108 (1985). Princeton University Press,

[60] M. A. Kenku, F. Momose, *Automorphism groups of the modular curves $X_0(N)$*. Compositio Mathematica, 65 (1988) no. 1, 51-80, `http://www.numdam.org/item?id=CM_1988__65_1_51_0`

[61] K. Khuri-Makdisi, *Asymptotically fast group operations on Jacobians of general curves*. Math. Comp. 76 (2007), no. 260, 2213–2239.

[62] M. Kim, *The motivic fundamental group of* $\mathbb{P}^1 - \{0, 1, \infty\}$ *and the theorem of Siegel.* Invent. Math. 161 no. 3 (2005), 629–656.

[63] M. Kim, *The unipotent Albanese map and Selmer varieties for curves.* Publ. Res. Inst. Math. Sci. 45 no. 1 (2009), 89–133.

[64] T. Kleinjung, B. Wesolowski, *A new perspective on the powers of two descent for discrete logarithms in finite fields.* The Open Book Series 2 (2019) No. 1, 343-352.

[65] T. Kleinjung, B. Wesolowski, *Discrete logarithms in quasi-polynomial time in finite fields of fixed characteristic.* arXiv preprint:1906.10668 (2019)

[66] H.W. Jr. Lenstra, *Finding isomorphisms between finite fields.* Math. Comp. 56 (1991), 329–347.

[67] G. Lido, *Discrete logarithm over finite fields of small characteristic.* Master's thesis, Universitá di Pisa (2016). Available at https://etd.adm.unipi.it/t/etd-08312016-225452.

[68] Q. Liu, *Algebraic geometry and arithmetic curves.* Oxford Graduate Texts in Mathematics, 6. Oxford Science Publications. Oxford University Press, Oxford, 2002.

[69] W. Bosma, J. J. Cannon, C. Fieker, A. Steel, *Handbook of Magma functions.* `http://magma.maths.usyd.edu.au/magma/handbook/`

[70] *A Magma script.* `https://github.com/guidoshore/automorphisms_of_Cartan_modular_curves`, last accessed: 2020-08-08

[71] N. Mascot, *Hensel-lifting torsion points on Jacobians and Galois representations.* Math. Comp. 89 (2020), no. 323, 1417–1455.

[72] B. Mazur, *Rational isogenies of prime degree*, Inventiones Mathematicae, 44 (1978) no. 2, 129-162

[73] B. Mazur and J. Tate, *Canonical height pairings via biextensions.* Arithmetic and geometry, Vol. I, 195–237, Progr. Math., 35, Birkhäuser Boston, Boston, MA, 1983.

[74] P. Mercuri, *Equations and rational points of the modular curves* $X_0^+(p)$. Ramanujan Journal, 47 (2018) no. 2, 291-308

[75] P. Mercuri, R. Schoof, *Modular forms invariant under non-split Cartan subgorup.* accepted by Mathematics of Computation (2020)

[76] L. Moret-Bailly, *Métriques permises.* Seminar on arithmetic bundles: the Mordell conjecture (Paris, 1983/84). Astérisque no. 127 (1985), 29–87. http://www.numdam.org/article/AST_1985__127__29_0.pdf

[77] L. Moret-Bailly, *Pinceaux de variétés abéliennes.* Astérisque no. 129 (1985). http://www.numdam.org/item/AST_1985__129__1_0/

[78] W. McCallum and B. Poonen, *The method of Chabauty and Coleman.* Explicit methods in number theory, 99–117, Panor. Synthèses, 36, Soc. Math. France, Paris, 2012.

[79] S. Müller, *Applying the Mordell–Weil sieve.* Appendix to [8].

[80] D. Mumford, *Biextensions of formal groups.* In Arithmetic algebraic geometry (proceedings of Purdue conference). Harper, 1965

[81] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers.* Springer Monographs in Mathematics (2004)

[82] J. L. Nicolas, G. Robin, *Majorations explicites pour le nombre de diviseurs de N.* Canadian Mathematical Bulletin, 26 (1983) no. 4, 485-492

[83] A. P. Ogg, *Automorphismes de courbes modulaires.* Séminaire Delange-Pisot-Poitou, Théorie des nombres 16 (1975) no. 1, 1-8

[84] A .P. Ogg, *Diophantine equations and modular forms.* Bulletin of the American Mathematical Society, 81 (1997) no. 1, 14-27

[85] A. P. Ogg, *Über die Automorphismengruppe von* $X_0(N)$. Mathematische Annalen, 228 (1977) no. 3, 279-292

[86] M. Raynaud, *Spécialisation du foncteur de Picard.* Inst. Hautes Études Sci. Publ. Math. 38 (1970), 27-76. http://www.numdam.org/article/PMIHES_1970__38__27_0.pdf

[87] G. Robin, *Estimation de la fonction de Tchebychef* θ *sur le k-ième nombre premier et grandes valeurs de la fonction* ω *(n) nombre de diviseurs premiers de n.* Acta Arithmetica, 42 (1998) no. 4, 367-389

[88] G. Robin, *Grandes valeurs de fonctions arithmétiques et problèmes d'optimisation en nombres entiers*. PhD thesis, Université de Limoges ((1998)

[89] J. B. Rosser, L. Schoenfeld, *Approximate formulas for some functions of prime numbers*. Illinois Journal of Mathematics, 6 (1962) no. 1, 64-94

[90] H. G. Rück, *A Note on Elliptic Curves Over Finite Fields*. Mathematics of Computation Vol. 49 No. 179 (1987), pp. 301–304.

[91] *Groupes de monodromie en géométrie algébrique. I.* Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I). Dirigé par A. Grothendieck. Avec la collaboration de M. Raynaud et D.S. Rim. Lecture Notes in Mathematics, Vol 288. Springer–Verlag, Berlin–New York, 1972.

[92] J. P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*. Inventiones Mathematicae, 15 (1972) no. 4, 259-331

[93] J. P. Serre, *Lectures on the Mordell-Weil theorem*. Aspects of Mathematics, 3rd ed., Friedr. Vieweg & Sohn, Braunschweig (1997),

[94] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*. Princeton University Press (1971)

[95] G. Shimura, *Class fields over real quadratic fields and Hecke operators*. Annals of Mathematics, 2nd Series, 95 (1972), 130-190

[96] G. Shimura, *On elliptic curves with complex multiplication as factors of the Jacobians of modular function fields*. Nagoya Mathematical Journal, 43 (1971), 199-208

[97] J. H. Silverman, *The arithmetic of elliptic curves*. Springer Science and Business Media, Vol. 106 (2009).

[98] P. Spelier, *A geometric approach to linear Chabauty*. MSc thesis, Universiteit Leiden, 2020.
`https://www.universiteitleiden.nl/en/science/mathematics/education/theses`

[99] M. Stoll, *Finite coverings and rational points.* Oberwolfach lecture, 2005–07–19.
`http://www.mathe2.uni-bayreuth.de/stoll/workshop2005/oberwolfach2005.pdf`

[100] D. Wan, *Generators and irreducible polynomials over finite fields*, Mathematics of Computation Vol. 66 No. 129 (1997), 1195–1212.

[101] Y. Zarhin, *Neron coupling and quasicharacters.* Izv. Akad. Nauk SSSR Ser. Mat. 36 (1972), 497–509.

Summary

Geometric quadratic Chabauty and other topics in number theory

This thesis consists of three parts.

In the first part we describe a generalization of Chabauty's method which, in certain cases, computes the set of rational points on a curve C of genus $g > 1$. Chabauty's method is to intersect, for a prime number p, in the p-adic Lie group of p-adic points of the jacobian J, the closure of the Mordell-Weil group with the p-adic points of the curve. If the Mordell-Weil rank r is less than the genus, this method produces a finite subset of $C(\mathbb{Q}_p)$ containing $C(\mathbb{Q})$. In our method, we substitute J with a product T of $\mathbb{G}_{\mathrm{m}}$-torsors over it. We take these torsors to be pull backs of the Poincaré torsor of the jacobian, and we use the biextension structure on it to parametrize the integral points on T. When $r-g+1$ is smaller than the rank of the Néron-Severi group of the jacobian, our method produces a finite subset of $C(\mathbb{Q}_p)$ containing $C(\mathbb{Q})$.

The second part of this thesis is devoted to the study of automorphisms of Cartan modular curves. In the literature we usually hit Cartan curves of prime level p, because their non-cuspidal points give elliptic curves E such that the natural Galois representation on the p-torsion of E is not surjective. We also study Cartan curves of composite level and we prove that, if the level is large enough, these curves only have the "expected" automorphisms, namely those automorphisms that lift to the upper half plane $\mathbb{H}$. In particular, we show that, when the level p is prime, this result holds for $p > 11$. The main novelty of our proof is a thorough study, for a wide class of modular curves, of the action of Hecke operators on elliptic points and cuspidal points. Then, we generalize classical methods to bound the field of definition of an automorphism u and we deduce that the u almost commutes with the Hecke operators. We conclude that u preserves both the set of elliptic points and the set of cuspidal points. Basic topological properties of covers imply that u lifts to the upper half plane $\mathbb{H}$.

The last part deals with the discrete logarithm problem in finite fields of small characteristic: given a finite field K of characteristic p and order larger than p^p, given a generator g of the group $K^\times$ and given another element $h \in \mathbb{K}^\times$, the problem is to determine an integer z such that $h = g^z$. In the last chapter of our thesis we describe a probabilistic algorithm that solves this problem in quasi-polynomial time, that is $\log(\#K)^{O(\log\log\#K)}$. A *heuristically quasi-polynomial* algorithm was already proposed by Joux, Barbulescu, Gaudry and Thomé, whose main idea is to look for an element of K on which the Frobenius automorphism acts in a "simple" way. We use this idea but we look for two elements of K on which the Frobenius acts in a "simple" way. In particular, we want these two elements to be the coordinates of a point on an elliptic curve E and we define "simple" using the group structure on E. Because of the abundance of elliptic curves, it is easy to prove that each finite field of small characteristic can be embedded in a slightly larger field containing two such elements. This makes our approach rigorous.

Samenvatting

Geometric quadratic Chabauty and other topics in number theory

Dit proefschrift bestaat uit drie delen.

Het eerste gedeelte betreft een methode van Chabauty die het mogelijk maakt om in bepaalde gevallen de rationale punten van een algebraische kromme C van geslacht $g > 1$ te vinden. Chabauty's methode bestaat eruit om voor een priemgetal p de doorsnede van de Mordell-Weil groep van de Jacobiaan met de p-adische punten van de kromme C te bestuderen. Als de rang r van de Mordell-Weil groep kleiner is dan het geslacht, dan leidt de methode tot een eindige deelverzameling van $C(\mathbb{Q}_p)$ die $C(\mathbb{Q})$ bevat. In onze benadering vervangen we J door een product T van $\mathbb{G}_{\mathrm{m}}$-torsoren over J. Om precies te zijn, T is een product van pullbacks van de Poincaré-torsor en we maken gebruik van de biextensiestructuur om de gehele punten van T te parametriseren. Wanneer $r-g+1$ kleiner is dan de rang van de Néron-Severi-groep van J, dan stelt onze methode ons in staat om een eindige verzameling van $\mathbb{Q}_p$-punten van C te bepalen die $C(\mathbb{Q})$ bevat.

Het tweede gedeelte van dit proefschrift gaat over automorfismen van Cartan modulaire krommen. De meeste literatuur over Cartan modulaire krommen betreft krommen van priem niveau p. De niet-cuspidale rationale punten van deze krommen corresponderen met elliptische krommen waarvoor de Galoisrepresentatie op de p-torsiepunten niet surjectief is. Ons resultaat betreft ook Cartan-krommen die niet noodzakelijk priemniveau hebben. We bewijzen dat als het niveau voldoende hoog is, deze krommen alleen maar de voor de hand liggende, naar het bovenhalfvlak liftbare automorfismen toelaten. Voor Cartan-krommen van priemniveau p is dit al het geval voor $p > 11$. Het belangrijkste nieuwe ingrediënt in ons bewijs is een diepgaande studie, voor een grote klasse van modulaire krommen, van de actie van de Hecke-operatoren op de elliptische punten en de spitsen. We generaliseren een klassieke methode om de graad van het definitielichaam van een automorfisme u te begrenzen. Tenslotte bewijzen we dat u in essentie met de

Hecke-operatoren commuteert. Hieruit volgt dat u zowel de spitsen als de elliptische punten behoudt. Standaard topologische eigenschappen van afdekkingen impliceren dan dat u naar het bovenhalfvlak $\mathbb{H}$ lift.

Het laatste gedeelte van dit proefschrift betreft de discrete logaritme in eindige lichamen van kleine karakteristiek. Het probleem is om, gegeven een eindig lichaam K van karakteristiek p en kardinaliteit $> p^p$ en gegeven een voortbrenger g van K^* en een element $h \in K^*$, een exponent z te bepalen zodat $h = g^z$. We geven een probabilistische algoritme om dit probleem op te lossen in quasi-polynomiale tijd: $\log(\#K)^{O(\log\log\#K)}$. Een heuristisch polynomiaal algoritme was al eerder gegeven door Joux, Barbulescu, Gaudry en Thomé. Hun voornaamste idee bestond eruit een element in K aan te geven waarop het Frobeniusautomorfisme op een "eenvoudige" manier werkt. Ons idee is om niet één maar twee elementen in K te geven. Deze twee elementen zijn de coördinaten van een punt op een elliptische kromme. Dankzij de groepsstructuur is de actie van Frobenius "eenvoudig". Omdat er zoveel keus is voor de elliptische kromme, is het makkelijk in te zien dat elk eindig lichaam van kleine karakteristiek ingebed kan worden in een iets groter lichaam dat twee zulke elementen bevat. Op deze manier kunnen we de heuristieke benadering vervangen door een bewijs dat ons algoritme quasi-polyniomiaal is.

Riassunto

Geometric quadratic Chabauty and other topics in number theory

Questa tesi si compone di tre parti.

Nella prima parte mostriamo una generalizzazione del metodo di Chabauty che, in alcuni casi, permette di calcolare l'insieme dei punti razionali di una curva C di genere $g > 1$. Dato un numero primo p, il metodo di Chabauty consiste nell'intersecare, all'interno del gruppo p-adico di Lie formato dai $\mathbb{Q}_p$-punti della jacobiana J, la chiusura del gruppo di Mordell-Weil con i $\mathbb{Q}_p$-punti della curva. Se il rango di Mordell-Weil r è minore del genere, questo metodo permette di determinare un sottoinsieme finito di $C(Q_p)$ contenente $C(\mathbb{Q})$. Nel nostro metodo sostituiamo J con un prodotto di $\mathbb{G}_{\mathrm{m}}$-torsori su di esso, che denotiamo T. I $\mathbb{G}_{\mathrm{m}}$-torsori che usiamo sono pull-back del torsore di Poincaré della jacobiana. Questo ci permette di parametrizzare i punti interi su T usando la struttura di biestensione presente sul torsore di Poincaré. Quando $r+g-1$ è minore del rango del gruppo di Néron-Severi della jacobiana, il nostro metodo permette di determinare un sottoinsieme finito di $C(\mathbb{Q}_p)$ contenente $C(\mathbb{Q})$.

La seconda parte della tesi è dedicata allo studio degli automorfismi delle curve modulari di tipo Cartan. In letteratura è comune incontrare curve di Cartan di livello primo p, in quanto i loro punti non-cuspidali corrispondono a curve ellittiche la cui rappresentazione di Galois associata alla p-torsione non è surgettiva. Noi studiamo anche curve di Cartan di livello composto e dimostramo che, se il livello è sufficientemente alto, gli unici automorfismi di queste curve sono quelli "attesi", ovvero quegli automorfismi che sollevano ad automorfismi del semipiano superiore $\mathbb{H}$. Quando il livello p è primo, dimostriamo che questo risultato vale per $p > 11$. Nella nostra dimostrazione, la maggiore novità è uno studio accurato, per una classe molto estesa di curve modulari, dell'azione degli operatori di Hecke sui punti cuspidali ed ellittici di una curva modulare. Inoltre, generalizziamo metodi classici per dare un bound sul campo di definizione di un automorfismo u e per dedurre che u commuta, o quasi, con gli operatori di Hecke. Ne concludiamo

che u preserva sia l'insieme delle cuspidi che l'insieme dei punti ellittici. Dimostriamo infine che u si solleva al semipiano superiore $\mathbb{H}$ utilizzando propriet'a topologiche di base dei rivestimenti.

L'ultima parte della tesi riguarda il problema del logaritmo discreto su campi finiti di piccola caratteristica: dato un campo finito K di caratteristica p e ordine maggiore di p^p, dato un generatore g del gruppo $K^\times$ e dato un altro elemento $h \in K^\times$, il problema è determinare un intero z tale che $g^z = h$. Nell'ultimo capitolo della tesi descriviamo un algoritmo probabilistico che risolve questo problema in tempo quasi-polinomiale, ovvero in $\log(\#K)^{O(\log\log\#K)}$ operazioni. Un algoritmo *euristicamente quasi-polinomiale* era già stato proposto da Joux, Barbulescu, Gaudry and Thomé, la cui idea principale è cercare un elemento di K su cui l'automorfismo di Frobenius agisce in un modo "semplice". Noi utilizziamo un'idea simile e cerchiamo due elementi $x, y \in K$ su cui l'automorfismo di Frobenius agisce in un modo "semplice". In particolare, richiediamo che questi due elementi siano coordinate di un punto su una curva ellittica E e definiamo "semplice" utilizzando la struttura di gruppo di E. Data l'abbondanza di curve ellittiche, è facile dimostrare che ogni campo finito di caratteristica piccola è contenuto in un'altro campo finito, leggermente più grande, in cui si trovano tali elementi x, y. Questo rende il nostro approccio rigoroso.

Acknowledgements

There are some people I would like to thank.

My two supervisors, for sharing with me their way of phrasing and tackling problems.

My brother and my parents, for looking at my problems as if they were theirs.

Pietro and Valerio, because we decided to tackle a problem together.

Carlo, because he always looks for new problems, pushing me to do the same.

Jared and Stevan, because sometimes our problems were similar.

Alessandro, Andrea, Andrea, Andrea, Giulio, Martino, because, despite the problem of not seeing each other, we stayed friends.

After talking so much about problems, Giulia.

Curriculum Vitae

Guido Maria Lido was born on the 17th of September 1992 in Roma, in Italy, where he also received his pre-university education. During the high school studies, he grew in his passion for mathematics while participating in the Math Olympiads. In 2011 he joined the Italian team at the IMO, which was held in Amsterdam that year.

In 2011 he enrolled in the "Corso ordinario" (ordinary program) in Mathematics at the Scuola Normale Superiore of Pisa. He obtained his bachelor's degree in 2014 with a thesis titled *André's theorem and unlikely intersections*, supervised by Umberto Zannier. He obtained his master's degree in 2016 with a thesis titled *Discrete logarithm in finite fields of small characteristic*, supervised by René Schoof.

From 2016 to 2020 he conducted a Ph.D. in Mathematics, in cotutelle between the University of Roma Tor Vergata and Leiden University, under the supervision of René Schoof and Bas Edixhoven.

In 2021 he started working for ION Group.