J. Inst. Math. Jussieu (2021), 1–55
doi:10.1017/S1474748021000244

GEOMETRIC QUADRATIC CHABAUTY

BAS EDIXHOVEN AND GUIDO LIDO

Mathematisch Instituut Universiteit Leiden, Postbus 9512, 2300 RA Leiden, The Netherlands
(edix@math.leidenuniv.nl, guidomaria.lido@gmail.com)

(Received 22 August 2020; revised 10 May 2021; accepted 11 May 2021)

Abstract Since Faltings proved Mordell's conjecture in [16] in 1983, we have known 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) [10] 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. Under the condition that the Mordell–Weil rank is less than the genus, Chabauty's method, in combination with other methods such as the Mordell–Weil sieve, has been applied successfully to determine all rational points in many cases.

Minhyong Kim's nonabelian 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).

Keywords: rational points, curves, Chabauty, nonabelian, quadratic, geometric

2020 Mathematics subject classification: Primary 14G05
Secondary 11G30

Contents

1 Introduction **2**
2 Algebraic geometry **3**
3 From algebraic geometry to formal geometry **6**
4 Integral points, closure and finiteness **7**
5 Parametrisation of integral points, and power series **11**
5.1 Logarithm and exponential 11
5.2 Parametrisation by power series 13
5.3 The p-adic closure 15
6 Explicit description of the Poincaré torsor **15**
6.1 Norms 16
6.2 Norms along finite relative Cartier divisors 17
6.3 Explicit description of the Poincaré torsor of a smooth curve 18
6.4 Explicit isomorphism for norms along equivalent divisors 21

6.5 Symmetry of the norm for divisors on smooth curves 22
6.6 Explicit residue disks and partial group laws 24
6.7 Extension of the Poincaré biextension over Néron models 28
6.8 Explicit description of the extended Poincaré bundle 28
6.9 Integral points of the extended Poincaré torsor 31
7 Description of the map from the curve to the torsor 33
8 An example with genus 2, rank 2 and 14 points 36
8.2 The torsor on the Jacobian 37
8.3 Some integral points on the biextension 38
8.4 Some residue disks of the biextension 39
8.5 Geometry mod p^2 of integral points 41
8.6 The rational points with a specific image mod 5 44
8.7 Determination of all rational points 44
9 Some further remarks 45
9.1 Complex uniformisations of some of the objects involved 45
9.2 Finiteness of rational points 48
9.3 The relation with p-adic heights 52
Acknowledgements 53
References 53

1. Introduction

Faltings proved in 1983 [16] 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. There is a fair amount of evidence (mainly hyperelliptic curves of small genus [3]) that Chabauty's method, in combination with other methods such as the Mordell–Weil sieve, does determine all rational points when $r < g$, with r the Mordell–Weil rank and g the genus of C.

For a general introduction to Chabauty's method and Coleman's effective version of it, we highly recommend [24] and, for an implementation of it that is 'geometric' in the sense of this article, [17], 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 nonabelian Chabauty programme aims to remove the condition that $r < g$. 'Nonabelian' here 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 [5] – a technical tour de force – to the so-called cursed curve ($r = g = 3$). For more details, we recommend the introduction to [5].

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 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. In §2 we describe the geometric method in fewer than three pages, §§3–5 give the necessary theory, §§6 and 7 give descriptions that are suitable for computer calculations and §8 treats an example with $r = g = 2$ and 14 rational points. As explained in the remarks following Theorem 4.12, we expect that this approach will make it possible to treat many more curves. In §9.1 we give 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 homology group of the curve. In §9.2 we re-prove the finiteness of $C(\mathbb{Q})$, for C with $r < g+\rho-1$, where ρ is the rank of the $\mathbb{Z}$-module of symmetric endomorphisms of the Jacobian of C. It also shows that a version of Theorem 4.12 that uses higher p-adic precision will always give a finite upper bound for $C(\mathbb{Q})$. In §9.3 we give, 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 4.12 can be useful; this has been worked out and implemented in [30]. We recommend this work as a gentle introduction to the geometric approach taken in this article. A generalisation from $\mathbb{Q}$ to number fields is given in [13]. For a generalisation of the cohomological approach, see [2] (quadratic Chabauty) and [14] (nonabelian Chabauty).

Although this article is about geometry, it contains no pictures. Fortunately, many pictures can be found in [19], and some in [15].

2. Algebraic geometry

Let C be a scheme over $\mathbb{Z}$, proper, flat, regular, with $C_{\mathbb{Q}}$ of dimension 1 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 by $\lambda\colon J \to J^\vee$ 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

$$P^\times_{\mathbb{Q}} = \mathbf{Isom}_{J_{\mathbb{Q}} \times J^\vee_{\mathbb{Q}}}\left(\mathcal{O}_{J_{\mathbb{Q}} \times J^\vee_{\mathbb{Q}}}, P_{\mathbb{Q}}\right). \tag{2.1}$$

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, $\left(P^\times_{\mathbb{Q}}\right)_S$ 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 $\mathbb{G}_{\mathrm{m}}$; for the details of this notion, we recommend [26, §I.2.5], Grothendieck's Exposés VII and VIII [29] 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

$$(x_1,y)^*P_\mathbb{Q} \otimes_{\mathcal{O}_S} (x_2,y)^*P_\mathbb{Q} = (x_1+x_2,y)^*P_\mathbb{Q}. \tag{2.2}$$

This induces a morphism of schemes

$$(x_1,y)^*P_\mathbb{Q}^\times \times_S (x_2,y)^*P_\mathbb{Q}^\times \longrightarrow (x_1+x_2,y)^*P_\mathbb{Q}^\times \tag{2.3}$$

as follows. For any S-scheme T, and z_1 in $\left((x_1,y)^*P_\mathbb{Q}^\times\right)(T)$ and z_2 in $\left((x_2,y)^*P_\mathbb{Q}^\times\right)(T)$, 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 $\left((x_1+x_2,y)^*P_\mathbb{Q}^\times\right)(T)$. This gives $P_\mathbb{Q}^\times \to J_\mathbb{Q}^\vee$ the structure of a commutative group scheme, which is an extension of $J_\mathbb{Q}$ by $\mathbb{G}_\mathrm{m}$ over the base $J_\mathbb{Q}^\vee$. We denote this group law, and the one on $J_\mathbb{Q}\times J_\mathbb{Q}^\vee$, as

$$\begin{tikzcd}
(z_1,z_2) \arrow[r, mapsto] \arrow[d, mapsto] & z_1+_1 z_2 \arrow[d, mapsto] & \\
((x_1,y),(x_2,y)) \arrow[r, mapsto] & (x_1,y)+_1(x_2,y) \arrow[r, equal] & (x_1+x_2,y).
\end{tikzcd} \tag{2.4}$$

In the same way, $P_\mathbb{Q}^\times \to J_\mathbb{Q}$ has a group law $+_2$ that makes it an extension of $J_\mathbb{Q}^\vee$ by $\mathbb{G}_\mathrm{m}$ over the base $J_\mathbb{Q}$. Therefore, $P_\mathbb{Q}^\times$ is both the universal extension of $J_\mathbb{Q}$ by $\mathbb{G}_\mathrm{m}$ and the universal extension of $J_\mathbb{Q}^\vee$ 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 $J_\mathbb{Q}^\vee(S)$ and all i and j in $\{1,2\}$, $z_{i,j}$ in $\left((x_i,y_j)^*P_\mathbb{Q}^\times\right)(S)$, we have

$$\begin{tikzcd}
(z_{1,1}+_1 z_{2,1})+_2(z_{1,2}+_1 z_{2,2}) \arrow[r, equal] \arrow[d, mapsto] & (z_{1,1}+_2 z_{1,2})+_1(z_{2,1}+_2 z_{2,2}) \arrow[d, mapsto] \\
(x_1+x_2,y_1)+_2(x_1+x_2,y_2) \arrow[r, equal] & (x_1,y_1+y_2)+_1(x_2,y_1+y_2),
\end{tikzcd} \tag{2.5}$$

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

Now we extend this geometry 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 $J^\vee$. [29, Exposé VIII, Theorem 7.1] gives that $P_\mathbb{Q}^\times$ extends uniquely to a $\mathbb{G}_\mathrm{m}$-biextension

$$P^\times \longrightarrow J\times J^{\vee 0} \tag{2.6}$$

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

$$j_b\colon C^{\mathrm{sm}} \longrightarrow J, \tag{2.7}$$

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 $\mathrm{Hom}\left(J_{\mathbb{Q}}, J_{\mathbb{Q}}^{\vee}\right)^{+}$, the $\mathbb{Z}$-module of self-dual morphisms from $J_{\mathbb{Q}}$ to $J_{\mathbb{Q}}^{\vee}$. This torsor will be the product of pullbacks of $P^{\times}$ via morphisms

$$(\mathrm{id}, m\cdot \circ \mathrm{tr}_c \circ f) \colon J \to J \times J^{\vee 0}, \tag{2.8}$$

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 $\Phi\left(\overline{\mathbb{F}}_p\right)$ with p ranging over all primes and $m\cdot$ the map of multiplication by m 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 $(\mathrm{id}, m\cdot \circ \mathrm{tr}_c \circ f)^* P_{\mathbb{Q}}^{\times}$ if and only if $j_b^*(\mathrm{id}, m\cdot \circ \mathrm{tr}_c \circ f)^* P_{\mathbb{Q}}^{\times}$ 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

$$j_b^* = -\lambda^{-1} \colon J_{\mathbb{Q}}^{\vee} \to J_{\mathbb{Q}}, \tag{2.9}$$

(see [25, Propositions 2.7.9 and 2.7.10]). This implies that for f such that this degree is 0, there is a unique c such that $j_b^*(\mathrm{id}, \mathrm{tr}_c \circ f)^* P_{\mathbb{Q}}^{\times}$ is trivial on $C_{\mathbb{Q}}$, and hence also its mth power $j_b^*(\mathrm{id}, m\cdot \circ \mathrm{tr}_c \circ f)^* P_{\mathbb{Q}}^{\times}$.

The map

$$\mathrm{Hom}\left(J_{\mathbb{Q}}, J_{\mathbb{Q}}^{\vee}\right) \longrightarrow \mathrm{Pic}(J_{\mathbb{Q}}) \longrightarrow \mathrm{NS}_{J_{\mathbb{Q}}/\mathbb{Q}}(\mathbb{Q}) = \mathrm{Hom}\left(J_{\mathbb{Q}}, J_{\mathbb{Q}}^{\vee}\right)^{+} \tag{2.10}$$

sending f to the class of $(\mathrm{id}, f)^* P_{\mathbb{Q}}$ sends f to $f + f^{\vee}$, and hence its kernel is $\mathrm{Hom}\left(J_{\mathbb{Q}}, J_{\mathbb{Q}}^{\vee}\right)^{-}$, the group of antisymmetric morphisms. But actually, for f antisymmetric, its image in $\mathrm{Pic}(J_{\mathbb{Q}})$ is already zero (see, e.g., example [6] and the references therein). Hence the image of $\mathrm{Hom}\left(J_{\mathbb{Q}}, J_{\mathbb{Q}}^{\vee}\right)$ in $\mathrm{Pic}(J_{\mathbb{Q}})$ is free of rank ρ, and its subgroup of classes with degree 0 on $C_{\mathbb{Q}}$ is free of rank $\rho - 1$. Let $f_1, \ldots, f_{\rho-1}$ be elements of $\mathrm{Hom}\left(J_{\mathbb{Q}}, J_{\mathbb{Q}}^{\vee}\right)$ whose images in $\mathrm{Pic}(J_{\mathbb{Q}})$ form a basis of this subgroup, and let $c_1, \ldots, c_{\rho-1}$ 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 $(\mathrm{id}, m\cdot \circ \mathrm{tr}_{c_i} \circ f_i)^* P_{\mathbb{Q}}^{\times}$, 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 $C_{\mathbb{F}_q}^{\mathrm{sm}}$, 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

$$\begin{tikzcd} & (\mathrm{id}, m\cdot \circ \mathrm{tr}_{c_i} \circ f_i)^* P^{\times} \arrow[d] \\ U \arrow[ur, "\widetilde{j_b}"] \arrow[r, "j_b"] & J, \end{tikzcd} \tag{2.11}$$

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 $T_i := (\mathrm{id}, m\cdot \circ \mathrm{tr}_{c_i} \circ f_i)^* P^\times$:

$$\begin{tikzcd}
 & T \arrow[r] \arrow[d] & P^{\times,\rho-1} \arrow[d] \\
U \arrow[ur, "\widetilde{j_b}"] \arrow[r, "j_b"] & J \arrow[r, "\left(\mathrm{id}, m\cdot\circ\mathrm{tr}_{c_i}\circ f_i\right)_i"] & J \times \left(J^{\vee 0}\right)^{\rho-1}.
\end{tikzcd} \tag{2.12}$$

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 $\widetilde{j_b}\left(U\left(\mathbb{Z}_p\right)\right)$ and the closure $\overline{T(\mathbb{Z})}$ of $T(\mathbb{Z})$ in $T\left(\mathbb{Z}_p\right)$ 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.

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 $x \in X\left(\mathbb{F}_p\right)$, let us describe the set $X\left(\mathbb{Z}_p\right)_x$ of elements of $X\left(\mathbb{Z}_p\right)$ whose image in $X\left(\mathbb{F}_p\right)$ 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, $x_l \in X\left(\mathbb{Z}_p\right)_x$ is a lift of x such that $t_1(x_l) = \ldots t_d(x_l) = 0$, then we say that the t_is are *parameters at* x_l. The t_i can be evaluated on all the points in $X(\mathbb{Z}_p)_x$, inducing a bijection $t := (t_1, \ldots, t_d)\colon X\left(\mathbb{Z}_p\right)_x \to \left(p\mathbb{Z}_p\right)^d$. We get a bijection

$$\tilde{t} := \left(\tilde{t}_1, \ldots, \tilde{t}_d\right) = \left(\frac{t_1}{p}, \ldots, \frac{t_d}{p}\right) : X\left(\mathbb{Z}_p\right)_x \xrightarrow{\sim} \mathbb{Z}_p^d. \tag{3.1}$$

This bijection can be interpreted geometrically as follows. Let $\pi\colon \widetilde{X}_x \to X$ denote the blowup 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 étale and $t^{-1}\left\{0_{\mathbb{F}_p}\right\} = \{x\}$. Then $\pi\colon \widetilde{X}_x \to X$ is the pullback of the blowup 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 $\mathbb{Z}_p[t_1, \ldots, t_d] \to \mathbb{Z}_p\left[\tilde{t}_1, \ldots, \tilde{t}_d\right]$ with $t_i \mapsto p\tilde{t}_i$. It follows that the p-adic completion $\mathcal{O}\left(\widetilde{X}^p_x\right)^{\wedge p}$ of $\mathcal{O}\left(\widetilde{X}^p_x\right)$ is the p-adic completion $\mathbb{Z}_p\left\langle\tilde{t}_1, \ldots, \tilde{t}_d\right\rangle$ of $\mathbb{Z}_p\left[\tilde{t}_1, \ldots, \tilde{t}_d\right]$. Explicitly, we have

$$\mathbb{Z}_p\left\langle\tilde{t}_1,\ldots,\tilde{t}_d\right\rangle=\left\{\sum_{I\in\mathbb{N}^d} a_I\tilde{t}^I\in\mathbb{Z}_p\left[\left[\tilde{t}_1,\ldots,\tilde{t}_d\right]\right]:\forall n\geq 0,\ \forall^{\mathrm{almost}} I, v_p(a_I)\geq n\right\}. \tag{3.2}$$

With these definitions, we have

$$\begin{aligned} X\left(\mathbb{Z}_p\right)_x&=\widetilde{X}_x^p\left(\mathbb{Z}_p\right)=\operatorname{Hom}\left(\mathbb{Z}_p\left\langle\tilde{t}_1,\ldots,\tilde{t}_d\right\rangle,\mathbb{Z}_p\right)=\mathbb{A}^d\left(\mathbb{Z}_p\right),\\ \left(\widetilde{X}_x^p\right)_{\mathbb{F}_p}&=\operatorname{Spec}\left(\mathbb{F}_p\left[\tilde{t}_1,\ldots,\tilde{t}_d\right]\right). \end{aligned} \tag{3.3}$$

The affine space $\left(\widetilde{X}_x^p\right)_{\mathbb{F}_p}$ 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 and $f\colon X\to Y$ be a morphism over $\mathbb{Z}_p$, and define $y:=f(x)\in Y\left(\mathbb{F}_p\right)$. Then the ideal in $\mathcal{O}_{\widetilde{X}_x^p}$ generated by the image of $m_{f(x)}$ is generated by p. That gives us a morphism $\widetilde{X}_x^p\to\widetilde{Y}_{f(x)}^p$, and then a morphism from $\mathcal{O}\left(\widetilde{Y}_{f(x)}^p\right)^{\wedge_p}$ to $\mathcal{O}\left(\widetilde{X}_x^p\right)^{\wedge_p}$. Reduction mod p then gives a morphism $\left(\widetilde{X}_x^p\right)_{\mathbb{F}_p}\to\left(\widetilde{Y}_{f(x)}^p\right)_{\mathbb{F}_p}$, 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 $t_1,\ldots,t_{d_y}$ in $\mathcal{O}_{Y,y}$ such that $p,t_1,\ldots,t_{d_y}$ are parameters at y and such that $t_{d_x+1},\ldots,t_{d_y}$ generate the kernel of $\mathcal{O}_{Y,y}\to\mathcal{O}_{X,x}$. Then the images in $\mathcal{O}_{X,x}$ of $p,t_1,\ldots,t_{d_x}$ are parameters at x, and $\mathcal{O}\left(\widetilde{Y}_{f(x)}^p\right)^{\wedge_p}\to\mathcal{O}\left(\widetilde{X}_x^p\right)^{\wedge_p}$ is $\mathbb{Z}_p\left\langle\tilde{t}_1,\ldots,\tilde{t}_{d_y}\right\rangle\to\mathbb{Z}_p\left\langle\tilde{t}_1,\ldots,\tilde{t}_{d_x}\right\rangle$, with kernel generated by $\tilde{t}_{d_x+1},\ldots,\tilde{t}_{d_y}$.

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, ρ, etc., is as at the end of §2. We assume moreover that p does not divide n (n as in the start of §2) and that $p>2$ (for $p=2$, everything that follows can probably be adapted by working with residue polydisks mod 4).

Let u be in $U\left(\mathbb{F}_p\right)$ and define $t:=\widetilde{j_b}(u)$. We want a description of the closure $\overline{T(\mathbb{Z})_t}$ of $T(\mathbb{Z})_t$ in $T\left(\mathbb{Z}_p\right)_t$. 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 $\tilde{t}\in T(\mathbb{Z})_t$ and we define $x_{\tilde{t}}\in J(\mathbb{Z})$ to be the projection of $\tilde{t}$. Let $f=\left(f_1,\ldots,f_{\rho-1}\right):J\to J^{\vee,\rho-1}$ and let $c=\left(c_1,\ldots,c_{\rho-1}\right)\in J^{\vee,\rho-1}(\mathbb{Z})$. We denote by $P^{\times,\rho-1}$ the product over $J\times\left(J^{\vee 0}\right)^{\rho-1}$ 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 $\left(J^{\vee 0}\right)^{\rho-1}$ 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 $x_1,\ldots,x_r$ of the free $\mathbb{Z}$-module $J(\mathbb{Z})_0$, the kernel of $J(\mathbb{Z})\to J\left(\mathbb{F}_p\right)$. For each $i,j\in\{1,\ldots,r\}$, we choose $P_{i,j}$, $R_{i,\tilde{t}}$ and $S_{\tilde{t},j}$ in $P^{\times,\rho-1}(\mathbb{Z})$ whose images in $\left(J\times\left(J^{\vee 0}\right)^{\rho-1}\right)(\mathbb{Z})$ are $\left(x_i,f\left(mx_j\right)\right)$, $\left(x_i,(m\cdot\circ\mathrm{tr}_c\circ f)\left(x_{\tilde{t}}\right)\right)$ and $\left(x_{\tilde{t}},f\left(mx_j\right)\right)$:

$$\begin{tikzcd}
P_{i,j} \arrow[d, mapsto] & R_{i,\widetilde{t}} \arrow[d, mapsto] & S_{\widetilde{t},j} \arrow[d, mapsto] & P^{\times,\rho-1} \arrow[d] \\
(x_i, f(mx_j)), & (x_i, (m\cdot \circ \mathrm{tr}_c \circ f)(x_{\widetilde{t}})), & (x_{\widetilde{t}}, f(mx_j)), & J \times \left(J^{\vee 0}\right)^{\rho-1}.
\end{tikzcd} \tag{4.1}$$

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

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

$$\begin{tikzcd}
A_{\widetilde{t}}(n) = \displaystyle\sum_{j=1}^{r}{}_{2}\, n_j \cdot_2 S_{\widetilde{t},j} \arrow[d, mapsto] & B_{\widetilde{t}}(n) = \displaystyle\sum_{i=1}^{r}{}_{1}\, n_i \cdot_1 R_{i,\widetilde{t}} \arrow[d, mapsto] \\
\left(x_{\widetilde{t}}, \displaystyle\sum_{i=1}^{r} n_i f(mx_i)\right), & \left(\displaystyle\sum_{i=1}^{r} n_i x_i, (m\cdot \circ \mathrm{tr}_c \circ f)(x_{\widetilde{t}})\right),
\end{tikzcd} \tag{4.2}$$

$$\begin{tikzcd}
C(n) = \displaystyle\sum_{i=1}^{r}{}_{1}\, n_i \cdot_1 \left(\displaystyle\sum_{j=1}^{r}{}_{2}\, n_j \cdot_2 P_{i,j}\right) \arrow[d, mapsto] \\
\left(\displaystyle\sum_{i=1}^{r} n_i x_i, \displaystyle\sum_{i=1}^{r} n_i f(mx_i)\right),
\end{tikzcd} \tag{4.3}$$

where $\sum_1$ and $\cdot_1$ denote iterations of the first partial group law $+_1$ as in formula (2.4), and analogously for the second group law. We define, for all $n \in \mathbb{Z}^r$,

$$D_{\widetilde{t}}(n) := (C(n) +_2 B_{\widetilde{t}}(n)) +_1 \left(A_{\widetilde{t}}(n) +_2 \widetilde{t}\right) \in P^{\times,\rho-1}(\mathbb{Z}), \tag{4.4}$$

which is mapped to

$$\left(x_{\widetilde{t}} + \sum_{i=1}^{r} n_i x_i, (m\cdot \circ \mathrm{tr}_c \circ f)\left(x_{\widetilde{t}} + \sum_{i=1}^{r} n_i x_i\right)\right) \in \left(J \times \left(J^{\vee 0}\right)^{\rho-1}\right)(\mathbb{Z}). \tag{4.5}$$

Hence $D_{\widetilde{t}}(n)$ 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 n in $(p-1)\mathbb{Z}^r$, $D_{\widetilde{t}}(n)$ is in $T(\mathbb{Z})_t$. Let n' be in $\mathbb{Z}^r$ and let $n = (p-1)n'$. 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

$$A_{\widetilde{t}}(n) = (p-1)\cdot_2 A_{\widetilde{t}}(n') = 1 \text{ in } \mathbb{F}_p^{\times,\rho-1}. \tag{4.6}$$

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 $B_{\widetilde{t}}(n) = 1$, and, similarly in $P^{\times,\rho-1}(0,0) = \mathbb{F}_p^{\times,\rho-1}$, we have $C(n) = 1$. So, with apologies for the mix of additive and multiplicative notations, in $P^{\times,\rho-1}(\mathbb{F}_p)$ we have

$$D_{\tilde{t}}(n) = (1 +_2 1) +_1 (1 +_2 t) = t, \tag{4.7}$$

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

$$\begin{aligned} &((0,0) +_2 ((0,(m\cdot \circ \mathrm{tr}_c \circ f)(j_b(u))))) +_1 ((j_b(u),0) +_2 (j_b(u),(m\cdot \circ \mathrm{tr}_c \circ f)(j_b(u)))) \\ &= (j_b(u),(m\cdot \circ \mathrm{tr}_c \circ f)(j_b(u))). \end{aligned} \tag{4.8}$$

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

So we now have the map

$$\kappa_{\mathbb{Z}} \colon \mathbb{Z}^r \to T(\mathbb{Z})_t, \qquad n \mapsto D_{\tilde{t}}((p-1)n). \tag{4.9}$$

The following theorem will be proved in Section 5:

Theorem 4.10. *Let $x_1,\ldots,x_g$ 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 $v_1,\ldots,v_{\rho-1}$ be in $\mathcal{O}_{T,t}$ such that $p,x_1,\ldots,x_g,v_1,\ldots,v_{\rho-1}$ are parameters of $\mathcal{O}_{T,t}$. As in §3, these parameters, divided by p, give a bijection*

$$T(\mathbb{Z}_p)_t \longrightarrow \mathbb{Z}_p^{g+\rho-1}. \tag{4.10.1}$$

The composition of $\kappa_{\mathbb{Z}}$ with the map (4.10.1) is given by uniquely determined $\kappa_1,\ldots,\kappa_{g+\rho-1}$ in $\mathcal{O}\left(\mathbb{A}^r_{\mathbb{Z}_p}\right)^{\wedge_p} = \mathbb{Z}_p\langle z_1,\ldots,z_r\rangle$. The images in $\mathbb{F}_p[z_1,\ldots,z_r]$ of $\kappa_1,\ldots,\kappa_g$ are of degree at most 1, and the images of $\kappa_{g+1},\ldots,\kappa_{g+\rho-1}$ are of degree at most 2. The map $\kappa_{\mathbb{Z}}$ extends uniquely to the continuous map

$$\kappa = (\kappa_1,\ldots,\kappa_{g+\rho-1}) \colon \mathbb{A}^r(\mathbb{Z}_p) = \mathbb{Z}_p^r \longrightarrow T(\mathbb{Z}_p)_t, \tag{4.10.2}$$

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 §3, $\widetilde{j_b} \colon \widetilde{U}^p_u \to \widetilde{T}^p_t$ is, after reduction mod p, an affine linear embedding of codimension $g+\rho-2$, $\widetilde{j_b}^* \colon \mathcal{O}\left(\widetilde{T}^p_t\right)^{\wedge_p} \to \mathcal{O}\left(\widetilde{U}^p_u\right)^{\wedge_p}$ is surjective and its kernel is generated by elements $f_1,\ldots,f_{g+\rho-2}$ (we apologise for using the same letter as for the components of $f \colon J \to J^{\vee,\rho-1}$), whose images in $\mathbb{F}_p \otimes \mathcal{O}\left(\widetilde{T}^p_t\right)$ are of degree at most 1 and such that $f_1,\ldots,f_{g-1}$ are in $\mathcal{O}\left(\widetilde{J}^p_{j_b(u)}\right)^{\wedge_p}$. The pullbacks $\kappa^* f_i$ are in $\mathbb{Z}_p\langle z_1,\ldots,z_r\rangle$; let I be the ideal in $\mathbb{Z}_p\langle z_1,\ldots,z_r\rangle$ generated by them, and define

$$A := \mathbb{Z}_p\langle z_1,\ldots,z_r\rangle / I. \tag{4.11}$$

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 4.12. *For $i \in \{1,\ldots,g+\rho-2\}$, let $\kappa^*\overline{f_i}$ be the image of $\kappa^* f_i$ in $\mathbb{F}_p[z_1,\ldots,z_r]$, and let $\overline{I}$ be the ideal of $\mathbb{F}_p[z_1,\ldots,z_r]$ generated by them. Then $\kappa^*\overline{f_1},\ldots,\kappa^*\overline{f_{g-1}}$ are of degree at most 1, and $\kappa^*\overline{f_g},\ldots,\kappa^*\overline{f_{g+\rho-2}}$ are of degree at most 2. Assume that $\overline{A} := A/pA = \mathbb{F}_p[z_1,\ldots,z_r]/\overline{I}$ 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 $x_1,\ldots,x_g,v_1,\ldots,v_{\rho-1}$, every $\kappa^*\overline{f_i}$ is an $\mathbb{F}_p$-linear combination of $\kappa_1,\ldots,\kappa_{g+\rho-1}$, and hence of degree at most 2. For $i<g$, $\overline{f_i}$ is a linear combination of $x_1,\ldots,x_g$, 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 [1, Thm.10.17]. As J-adic completion is exact on finitely generated R-modules [1, Prop.10.12], it sends the surjection $R \to R/I$ to a surjection $R = R^\wedge \to (R/I)^\wedge$ (see [1, 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 an abelian group, an extension of A/pA by a quotient of A/p^mA. As a $\mathbb{Z}_p$-module, A is generated by any lift of an $\mathbb{F}_p$-basis of $\overline{A}$. Hence A is finitely generated as a $\mathbb{Z}_p$-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 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 4.12 can be used, and what we hope it can do.

Remark 4.13. The $\kappa^*\overline{f_i}$ as in Theorem 4.12 can be computed from their reductions $\mathbb{F}_p^r \to T(\mathbb{Z}/p^2\mathbb{Z})$ of $\kappa_{\mathbb{Z}}$ and (to get the $\overline{f_i}$) from $\widetilde{j_b}\colon U\left(\mathbb{Z}/p^2\mathbb{Z}\right)_u \to T\left(\mathbb{Z}/p^2\mathbb{Z}\right)_t$. 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 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 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 §9.2 proves that one gets an upper bound for the number of elements of $U(\mathbb{Z})$.

Remark 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 [3] or [4, Remark 8.9] – that for all $u \in U(\mathbb{F}_p)$, the upper bound in Theorem 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 [31].

Remark 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 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 [27]. 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 4.12 gives (interpreting $\overline{A}$ as in the end of the proof of the theorem) a subset O_p of $J(\mathbb{Z})$, with O_p 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.

5. Parametrisation of integral points, and power series

In this section we give a proof of Theorem 4.10. The main tools here are the formal logarithm and formal exponential of a commutative smooth group scheme over a $\mathbb{Q}$-algebra [20, 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 $\mathbb{Z}_p\langle z_1,\ldots,z_n\rangle$ to the set of maps $\mathbb{Z}_p^n \to \mathbb{Z}_p$ is injective (induction on n; nonzero 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 $\mathbb{Z}_p\langle z_1,\ldots,z_n\rangle = \mathcal{O}\left(\mathbb{A}^n_{\mathbb{Z}_p}\right)^{\wedge_p}$. This property is stable under composition: composition of polynomials over $\mathbb{Z}/p^k\mathbb{Z}$ gives polynomials.

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 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 definition (3.1), are given by $n+d$ elements of $\mathcal{O}\left(\widetilde{G}^p_{e(s)}\right)^{\wedge_p}$ and $n+d$ elements of $\mathcal{O}\left(\widetilde{T}_{G/S}(e)^p_{0(s)}\right)^{\wedge_p}$.

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 $\mathcal{O}\left(\mathbb{A}^1_{\mathbb{Z}_p} \times_{\mathbb{Z}_p} \widetilde{G}^p_{e(s)}\right)^{\wedge_p}$. The induced morphism $\mathbb{A}^1_{\mathbb{F}_p} \times \left(\widetilde{G}^p_{e(s)}\right)_{\mathbb{F}_p} \to \left(\widetilde{G}^p_{e(s)}\right)_{\mathbb{F}_p}$, where $\left(\widetilde{G}^p_{e(s)}\right)_{\mathbb{F}_p}$ 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 $t_1,\ldots,t_n$ be in $\mathcal{O}_{S,s}$ such that $p,t_1,\ldots,t_n$ are parameters at s. Then we have a bijection

$$\tilde{t}\colon S(\mathbb{Z}_p)_s \to \mathbb{Z}_p^n, \qquad a \mapsto p^{-1}{\cdot}(t_1(a),\ldots,t_n(a)). \tag{5.1.2}$$

Similarly, let $x_1,\ldots,x_d$ 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

$$(t,x)^\sim\colon G(\mathbb{Z}_p)_{e(s)} \to \mathbb{Z}_p^{n+d}, \qquad b \mapsto p^{-1}{\cdot}(t_1(b),\ldots,x_d(b)). \tag{5.1.3}$$

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, $\mathrm{d}\omega_i = 0$ [20, Proposition 1.3]. We also have the dual $\mathcal{O}_{S,s}$-basis ∂_i of $T_{G/S}(e)$ and the bijection

$$(t,x)^\sim\colon (T_{G/S}(e))(\mathbb{Z}_p)_{0(s)} \to \mathbb{Z}_p^{n+d}, \qquad \left(a, \sum_i v_i\partial_i\right) \mapsto p^{-1}{\cdot}(t_1(a),\ldots,t_n(a),v_1,\ldots,v_d). \tag{5.1.4}$$

Then log is given by elements $\log_i$ in $(\mathbb{Q}\otimes\mathcal{O}_{S,s})[[x_1,\ldots,x_d]]$ whose constant term is 0, uniquely determined [20, Proposition 1.1] by the equality

$$\mathrm{d}\log_i = \omega_i \text{ in } \oplus_j \mathcal{O}_{S,s}[[x_1,\ldots,x_d]]{\cdot}\mathrm{d}x_j. \tag{5.1.5}$$

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

$$\log_i = \sum_{J\neq 0} \log_{i,J} x^J \qquad \text{and} \qquad \log_{i,J} \in (\mathbb{Q}\otimes\mathcal{O}_{S,s}), \tag{5.1.6}$$

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

$$|J|{\cdot}\log_{i,J} \in \mathcal{O}_{S,s}. \tag{5.1.7}$$

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

$$\begin{tikzcd}
G(\mathbb{Z}_p)_{e(s)} \arrow[r, "?"] \arrow[d, "(t,x)^{\sim}"] & (T_{G/S}(e))(\mathbb{Z}_p)_{0(s)} \arrow[d, "(t,x)^{\sim}"] \\
\mathbb{Z}_p^{n+d} \arrow[r, "?"] & \mathbb{Z}_p^{n+d},
\end{tikzcd} \tag{5.1.8}$$

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

We have, for each i,

$$p^{-1}\cdot\sum_{J\neq 0}\log_{i,J}\left(\tilde{t}^{-1}(a)\right)(pb)^J = \sum_{J\neq 0}\frac{p^{|J|-1}}{|J|}\left(|J|\log_{i,J}\right)\left(\tilde{t}^{-1}(a)\right)b^J. \tag{5.1.9}$$

For each i, this expression is an element of $\mathbb{Z}_p\langle\tilde{t}_1,\dots,\tilde{t}_n,\tilde{x}_1,\dots,\tilde{x}_d\rangle = \mathcal{O}\left(\widetilde{G}^p_{e(s)}\right)^{\wedge_p}$, 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 equation (5.1.9) in $\mathbb{F}_p\otimes\mathcal{O}\left(\widetilde{G}^p_{e(s)}\right)^{\wedge_p}$ is $\tilde{x}_i$, and on the first n coordinates, log is the identity – so by applying Hensel mod powers of p, log is invertible, and the inverse is also given by $n+d$ elements of $\mathcal{O}\left(\widetilde{T}_{G/S}(e)^p_{0(s)}\right)^{\wedge_p}$.

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. □

5.2. Parametrisation by power series

The notation and assumptions are as in the beginning of §4; in particular, $p>2$ and T is as defined in diagram (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 $n\in\mathbb{Z}^r$ such that $Q=\varepsilon\cdot D_{\tilde{t}}(n)$: the image of Q in $J(\mathbb{Z})$ is in $J(\mathbb{Z})_{j_b(u)}$, and 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 $0\in J(\mathbb{F}_p)$), $\sum_i n_ix_i$ for a unique $n\in\mathbb{Z}^r$, and hence $D_{\tilde{t}}(n)$ and Q are in $T(\mathbb{Z})$ and have the same image in $J(\mathbb{Z})$, which gives the unique ε. So we have a bijection

$$\begin{aligned}\mathbb{Z}^{\times,\rho-1}\times\mathbb{Z}^r \longrightarrow T(\mathbb{Z})_{j_b(u)} &= \{Q\in T(\mathbb{Z}) : Q\mapsto j_b(u)\in J(\mathbb{F}_p)\},\\ (\varepsilon,n) &\mapsto \varepsilon\cdot D_{\tilde{t}}(n).\end{aligned} \tag{5.2.1}$$

But a problem that we are facing is that the map $\mathbb{Z}^r\to T(\mathbb{F}_p)_{j_b(u)}$ sending n to the image of $D_{\tilde{t}}(n)$ depends on the (unknown) images of the $P_{i,j}$, $R_{i,\tilde{t}}$ and $S_{\tilde{t},j}$ from formula (4.1) in $P^{\times,\rho-1}(\mathbb{F}_p)$, and so we do not know for which n and ε the point $\varepsilon\cdot D_{\tilde{t}}(n)$ is in $T(\mathbb{Z})_t$. Luckily, we have the $\mathbb{Z}_p^{\times,\rho-1}$-action on $T(\mathbb{Z}_p)$. Using the fact 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 n in $\mathbb{Z}^r$ there is a unique $\xi(n)$ in $\mathbb{F}_p^{\times,\rho-1}$ such that $\xi(n)\cdot D_{\tilde{t}}(n)$ is in $T(\mathbb{Z}_p)_t$.

We define

$$D'(n) := \xi(n)\cdot D_{\tilde{t}}(n). \tag{5.2.2}$$

Then for all n in $\mathbb{Z}^r$,

$$\kappa_{\mathbb{Z}}(n) = D_{\tilde{t}}((p-1)\cdot n) = D'((p-1)\cdot n), \tag{5.2.3}$$

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

$$T(\mathbb{Z})_t \subset D'(\mathbb{Z}^r). \tag{5.2.4}$$

The following lemma proves the existence and uniqueness of the κ_i of Theorem 4.10 and the claims on the degrees of the $\overline{\kappa}_i$:

Lemma 5.2.5. *After any choice of parameters of $\mathcal{O}_{T,t}$ as in Theorem 4.10, D' is given by elements $\kappa'_1,\ldots,\kappa'_{g+\rho-1}$ of $\mathcal{O}\left(\mathbb{A}^r_{\mathbb{Z}_p}\right)^{\wedge_p}$, and then $\kappa_{\mathbb{Z}}$ is given by $\kappa_1,\ldots,\kappa_{g+\rho-1}$ with, for all $i\in\{1,\ldots,g+\rho-1\}$ and all $a\in\mathbb{Z}_p^r$,*

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

For all i in $\{1,\ldots,g+\rho-1\}$, we let $\overline{\kappa}'_i$ be the reduction mod p of κ'_j. Then $\overline{\kappa}'_1,\ldots,\overline{\kappa}'_g$ 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 $D'(n)$, we introduce variants of the $P_{i,j}$, $R_{i,\tilde{t}}$ and $S_{\tilde{t},j}$ as follows. The images in $\left(J\times\left(J^{\vee 0}\right)^{\rho-1}\right)(\mathbb{F}_p)$ of these points are of the form $(0,*)$, $(0,*)$ and $(*,0)$, respectively. Hence the fibres over them of $P^{\times,\rho-1}$ are rigidified – that is, equal to $\mathbb{F}_p^{\times,\rho-1}$. We define their variants $P'_{i,j}$, $R'_{i,\tilde{t}}$ and $S'_{\tilde{t},j}$ 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 these $P_{i,j}$, $R_{i,\tilde{t}}$ and $S_{\tilde{t},j}$ in formulas (4.2) and (4.3) by $P'_{i,j}$, $R'_{i,\tilde{t}}$ and $S'_{\tilde{t},j}$ gives variants A', B' and C', and using these in definition (4.4) gives a variant $D'_{\tilde{t}}(n)$ of definition (5.2.2).

Then for all n in $\mathbb{Z}^r$, we have that $D'_{\tilde{t}}(n)$ and $D'(n)$ (as in definition (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 n in $\mathbb{Z}^r$,

$$\begin{aligned} A'(n) &= \sum_{j=1}^{r}{}_2\, n_j\cdot_2 S'_{\tilde{t},j}, \qquad B'(n) = \sum_{i=1}^{r}{}_1\, n_i\cdot_1 R'_{i,\tilde{t}}, \\ C'(n) &= \sum_{i=1}^{r}{}_1\, n_i\cdot_1\left(\sum_{j=1}^{r}{}_2\, n_j\cdot_2 P'_{i,j}\right), \\ D'(n) &= \left(C'(n)+_2 B'(n)\right)+_1\left(A'(n)+_2\tilde{t}\right). \end{aligned} \tag{5.2.6}$$

This shows how the map $n\mapsto D'(n)$ 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 5.1.1 gives that the iterations are given by integral convergent power series. The functoriality in §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 $n \mapsto D'(n)$ is given by elements $\kappa'_1,\ldots,\kappa'_{g+\rho-1}$ of $\mathbb{Z}_p\langle z_1,\ldots,z_r\rangle$.

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 $\overline{\kappa}'_1,\ldots,\overline{\kappa}'_{g+\rho-1}$ in $\mathbb{F}_p[z_1,\ldots,z_r]$ 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

$$C'_2\colon \mathbb{Z}^r \times \mathbb{Z}^r \longrightarrow P^{\times,\rho-1}(\mathbb{Z}_p), \qquad C'_2(n,m) = \sum_{i=1}^{r}{}_1\, n_i \cdot_1 \left(\sum_{j=1}^{r}{}_2\, m_j \cdot_2 P'_{i,j}\right). \tag{5.2.7}$$

Then the mod p coordinate functions of C'_2, elements of $\mathbb{F}_p[x_1,\ldots,x_r,y_1,\ldots,y_r]$, 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 first and second 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 the results of A', B' and C' using the partial group laws, we conclude that $\overline{\kappa}'_1,\ldots,\overline{\kappa}'_g$ are of degree at most 1, and the remaining $\overline{\kappa}_j$ are of degree at most 2. The same holds then for all $\overline{\kappa}_j$. □

5.3. The p-adic closure

We know from equation (5.2.3) that $\kappa_{\mathbb{Z}}(\mathbb{Z}^r) = D'((p-1)\mathbb{Z}^r)$. From formula (4.9) we know that $\kappa_{\mathbb{Z}}(\mathbb{Z}^r) \subset T(\mathbb{Z})_t$, and from formula (5.2.4) we know that $T(\mathbb{Z})_t \subset D'(\mathbb{Z}^r)$. So together we have

$$D'((p-1)\mathbb{Z}^r) = \kappa_{\mathbb{Z}}(\mathbb{Z}^r) \subset T(\mathbb{Z})_t \subset D'(\mathbb{Z}^r). \tag{5.3.1}$$

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, $D'\left(\mathbb{Z}_p^r\right)$ 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 $D'\left(\mathbb{Z}_p^r\right)$ and equal to $\kappa\left(\mathbb{Z}_p^r\right)$. This finishes the proof of Theorem 4.10.

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 making computations when applying Theorem 4.12. The main results are as follows. Proposition 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 6.4.8 shows how to deal with linear equivalence of divisors. Lemma 6.5.4 makes the symmetry of $P^\times$ explicit. Lemma 6.6.8 gives parametrisations of residue polydisks of $P^\times\left(\mathbb{Z}/p^2\mathbb{Z}\right)$, and Lemma 6.6.13 gives partial group laws on these residue polydisks. Proposition 6.8.7 describes the unique extension over $J \times J^{\vee,0}$ of the Poincaré torsor on

$\big(J\times J^{\vee,0}\big)_{\mathbb{Z}[1/n]}$, in terms of line bundles and divisors on C. Finally, Proposition 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 [25, §2]. We note that there 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 (§§6.1 and 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 can adapt the definition directly to our use of it.

6.1. Norms

Let S be a scheme, and let $f\colon S'\to S$ 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 an $\mathcal{O}_S$-module of rank n, and $\mathcal{O}_{S'}^\times$ is a subsheaf of groups of $\mathrm{GL}_{\mathcal{O}_S}(\mathcal{O}_{S'})$. Then the norm morphism is the composition

$$\begin{tikzcd}\mathcal{O}_{S'}^\times \arrow[r, hook] \arrow[rr, bend left, "\mathrm{Norm}_{S'/S}"] & \mathrm{GL}_{\mathcal{O}_S}(\mathcal{O}_{S'}) \arrow[r, "\det"] & \mathcal{O}_S^\times\,. \end{tikzcd} \tag{6.1.1}$$

Our viewing of $\mathcal{O}_{S'}$ as a sheaf on S does not change the notion of $\mathcal{O}_{S'}^\times$-torsor, because of the equivalence with invertible $\mathcal{O}_{S'}$-modules: triviality locally on S' implies triviality locally on S.

For T an $\mathcal{O}_{S'}^\times$-torsor, we let $\mathrm{Norm}_{S'/S}(T)$ be the $\mathcal{O}_S^\times$-torsor

$$\mathrm{Norm}_{S'/S}(T):=\mathcal{O}_S^\times\otimes_{\mathcal{O}_{S'}^\times}T=\big(\mathcal{O}_S^\times\times T\big)/\mathcal{O}_{S'}^\times, \tag{6.1.2}$$

with – for every open U of S and every $u\in\mathcal{O}_{S'}^\times(U)$ – u acting as $(v,t)\mapsto\big(v\cdot\mathrm{Norm}_{S'/S}(u),u^{-1}\cdot t\big)$. This is functorial in T: a morphism $\varphi\colon T_1\to T_2$ induces an isomorphism $\mathrm{Norm}_{S'/S}(\varphi)$. 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 $\mathcal{O}_{S'}^\times\big|_U$-torsors $\mathcal{O}_{S'}^\times\big|_U\to T|_U$ 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 (6.1.2) is multiplicative:

$$\mathrm{Norm}_{S'/S}\big(T_1\otimes_{\mathcal{O}_{S'}}T_2\big)=\mathrm{Norm}_{S'/S}(T_1)\otimes_{\mathcal{O}_S}\mathrm{Norm}_{S'/S}(T_2) \tag{6.1.3}$$

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

$$\mathrm{Norm}_{S'/S}(t_1\otimes t_2)\mapsto\mathrm{Norm}_{S'/S}(t_1)\otimes\mathrm{Norm}_{S'/S}(t_2). \tag{6.1.4}$$

Let $\mathcal{L}$ be an invertible $\mathcal{O}_{S'}$-module; locally on S, it is free of rank 1 as an $\mathcal{O}_{S'}$-module. This gives us the $\mathcal{O}_{S'}^\times$-torsor (on S) $\mathrm{Isom}_{\mathcal{O}_{S'}}(\mathcal{O}_{S'},\mathcal{L})$, which gives back $\mathcal{L}$ 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

$$\mathrm{Norm}_{S'/S}(\mathcal{L}) := \mathcal{O}_S \otimes_{\mathcal{O}_S^\times} \mathrm{Norm}_{S'/S}\left(\mathrm{Isom}_{\mathcal{O}_{S'}}(\mathcal{O}_{S'}, \mathcal{L})\right). \tag{6.1.5}$$

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

6.2. Norms along finite relative Cartier divisors

This part is inspired by [21, §1.1]. Let S be a scheme and $f\colon X \to S$ 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 nonzero divisor (equivalently, I_D is locally free of rank 1 as an $\mathcal{O}_X$-module). For such a D and an invertible $\mathcal{O}_X$-module $\mathcal{L}$, the norm of $\mathcal{L}$ along D is defined, using definition (6.1.5), as

$$\mathrm{Norm}_{D/S}(\mathcal{L}) := \mathrm{Norm}_{D/S}(\mathcal{L}|_D). \tag{6.2.1}$$

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

Lemma 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 definition* (6.2.1) *is multiplicative in $\mathcal{L}$:*

$$\mathrm{Norm}_{D/S}(\mathcal{L}_1 \otimes \mathcal{L}_2) = \mathrm{Norm}_{D/S}(\mathcal{L}_1) \otimes_{\mathcal{O}_S} \mathrm{Norm}_{D/S}(\mathcal{L}_2), \tag{6.2.3}$$

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 $\mathcal{L}_i|_V$ –

$$\mathrm{Norm}_{D/S}(l_1 \otimes l_2) = \mathrm{Norm}_{D/S}(l_1) \otimes \mathrm{Norm}_{D/S}(l_2). \tag{6.2.4}$$

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 and the closed subscheme $D_1 + D_2$ defined by it is a finite effective relative Cartier divisor on f. The norm functor in definition (6.2.1) *is additive in D:*

$$\mathrm{Norm}_{(D_1+D_2)/S}(\mathcal{L}) = \mathrm{Norm}_{D_1/S}(\mathcal{L}) \otimes_{\mathcal{O}_S} \mathrm{Norm}_{D_2/S}(\mathcal{L}), \tag{6.2.5}$$

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 $\mathcal{L}|_{D_1+D_2}$ –

$$\mathrm{Norm}_{(D_1+D_2)/S}(l) = \mathrm{Norm}_{D_1/S}(l) \otimes \mathrm{Norm}_{D_2/S}(l). \tag{6.2.6}$$

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

$$\begin{tikzcd} I_{D_2}/I_{D_1+D_2} \arrow[r, hook] \arrow[d, equal] & \mathcal{O}_{D_1+D_2} \arrow[r, two heads] & \mathcal{O}_{D_2} \\ (I_{D_2})|_{D_1} & & \end{tikzcd} \tag{6.2.7}$$

shows that $\mathcal{O}_{D_1+D_2}$ is locally free as an $\mathcal{O}_S$-module, whose rank is 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 equation (6.2.5) by proving the required statement about sheaves of groups. The diagram

$$\begin{tikzcd} \mathcal{O}^\times_{D_1+D_2} \arrow[r] \arrow[rrr, bend left, "\mathrm{Norm}_{(D_1+D_2)/S}"] & \mathcal{O}^\times_{D_1} \times \mathcal{O}^\times_{D_2} \arrow[r, "\mathrm{Norm}_{D_1/S}\times\mathrm{Norm}_{D_2/S}"] & \mathcal{O}^\times_S \times \mathcal{O}^\times_S \arrow[r, "\cdot"] & \mathcal{O}^\times_S, \\ u \arrow[rrr, mapsto] & & & \mathrm{Norm}_{D_1/S}(u)\mathrm{Norm}_{D_2/S}(u), \end{tikzcd} \tag{6.2.8}$$

commutes, because multiplication by u on $\mathcal{O}_{D_1+D_2}$ preserves the short exact sequence (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. □

6.3. Explicit description of the Poincaré torsor of a smooth curve

Let g be in $\mathbb{Z}_{\geq 1}$, 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 0 on C, rigidified at b.

Let $d \geq 0$ and $C^{(d)}$ be the dth symmetric power of $C \to S$ (we note that the quotient $C^d \to C^{(d)}$ is finite and 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

$$\mathcal{N}_d := \mathrm{Norm}_{D_J/\left(J\times_S C^{(d)}\right)}\left(\mathcal{L}^{\mathrm{univ}}_{C^{(d)}}\right). \tag{6.3.1}$$

This invertible $\mathcal{O}$-module $\mathcal{N}_d$ on $J \times_S C^{(d)}$, rigidified at the zero-section of J, gives 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 equation (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 6.3.2. *The pullback of P by $\left(j_b, j_b^{*,-1}\right) : C \times_S J \to J \times_S J^\vee$ 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 $\mathcal{M} := \left(\mathrm{id} \times j_b^{*,-1}\right)^* P$, this is:

$$\begin{tikzcd}
\mathcal{L}^{\mathrm{univ}} & P \arrow[l] \arrow[r] & \mathcal{M} \arrow[r, "\widetilde{\mathrm{id}\times\Sigma}"] & \mathcal{N}_d, \\
C \times_S J \arrow[r, "j_b \times j_b^{*,-1}"] & J \times_S J^\vee & J \times_S J \arrow[l, "\mathrm{id}\times j_b^{*,-1}"'] & J \times_S C^{(d)}. \arrow[l, "\mathrm{id}\times\Sigma"']
\end{tikzcd} \tag{6.3.3}$$

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

$$P\left(x, j_b^{*,-1}(y)\right) = \mathcal{M}(x,y) = \mathrm{Norm}_{D/T}(\mathcal{L}). \tag{6.3.4}$$

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

$$\mathcal{M}\left(j_b(c_1), j_b(c_2)\right) = c_2^*\left(\mathcal{O}_C(c_1 - b)\right) \otimes b^*\left(\mathcal{O}_C(b - c_1)\right), \tag{6.3.5}$$

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

$$(j_b \times j_b)^* \mathcal{M} = \mathcal{O}(\Delta) \otimes \mathrm{pr}_1^* \mathcal{O}(-b) \otimes \mathrm{pr}_2^* \mathcal{O}(-b) \otimes \mathrm{pr}_\emptyset^* b^* T_{C/S}. \tag{6.3.6}$$

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) and D_1 and D_2 in $C^{(d_1)}(S)$ and $C^{(d_2)}(S)$, the isomorphism

$$\mathcal{M}(x, \Sigma(D_1 + D_2)) = \mathcal{M}(x, \Sigma(D_1)) \otimes \mathcal{M}(x, \Sigma(D_2)) \tag{6.3.7}$$

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

$$\begin{aligned} \mathcal{N}_{d_1+d_2}(x, D_1 + D_2) &= \mathrm{Norm}_{(D_1+D_2)/T}(\mathcal{L}) = \mathrm{Norm}_{D_1/T}(\mathcal{L}) \otimes \mathrm{Norm}_{D_2/T}(\mathcal{L}) \\ &= \mathcal{N}_{d_1}(x, D_1) \otimes \mathcal{N}_{d_2}(x, D_2), \end{aligned} \tag{6.3.8}$$

using Lemma 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

$$\mathcal{M}(x_1 + x_2, \Sigma(D)) = \mathcal{M}(x_1, \Sigma(D)) \otimes \mathcal{M}(x_2, \Sigma(D)) \tag{6.3.9}$$

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

$$\begin{aligned}\mathcal{N}_d(x_1+x_2,D) &= \mathrm{Norm}_{D/T}(\mathcal{L}_1\otimes\mathcal{L}_2) = \mathrm{Norm}_{D/T}(\mathcal{L}_1)\otimes\mathrm{Norm}_{D/T}(\mathcal{L}_2)\\ &= \mathcal{N}_d(x_1,D)\otimes\mathcal{N}_d(x_2,D),\end{aligned} \tag{6.3.10}$$

using Lemma 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. Define $z := j_b^{*,-1}(x)$ 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 [25, Equation 2.7.1, Lemma 2.7.5 and Equation 2.7.7], using equation (2.9).

Now we prove equation (6.3.4). Let T and x be as before, 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,

$$\begin{aligned} P\left(x, j_b^{*,-1}(y)\right) &= P\left(y, j_b^{*,-1}(x)\right) = P\left(\Sigma(D), j_b^{*,-1}(x)\right)\\ &= P\left(\sum_i j_b(c_i), j_b^{*,-1}(x)\right) = \bigotimes_i P\left(j_b(c_i), j_b^{*,-1}(x)\right)\\ &= \bigotimes_i \mathcal{L}^{\mathrm{univ}}(c_i,x) = \bigotimes_i \mathcal{L}(c_i) = \mathrm{Norm}_{D/T}(\mathcal{L}).\end{aligned} \tag{6.3.11}$$

Identities (6.3.5) and (6.3.6) follow directly from equation (6.3.4).

Now we prove the claimed compatibility between the isomorphisms in equations (6.3.9) and (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 two 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 two 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 the isomorphisms in equations (6.3.7) and (6.3.8) is proved analogously. □

Remark 6.3.12. From Proposition 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

$$\mathcal{M}(x, \Sigma(D_1)-\Sigma(D_2)) = \mathrm{Norm}_{D_1/T}(\mathcal{L})\otimes\mathrm{Norm}_{D_2/T}(\mathcal{L})^{-1}, \tag{6.3.13}$$

satisfying the analogous compatibilities as in Proposition 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 equation (6.3.13) is independent of the choice of $\mathcal{L}$, given x.

6.4. Explicit isomorphism for norms along equivalent divisors

Let g be in $\mathbb{Z}_{\geq 1}$, 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, which we also view as elements of $C^{(d)}(S)$. Recall from Proposition 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 $\operatorname{div}(f) = D_2 - D_1$. Proposition 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

$$\begin{aligned}\operatorname{Norm}_{D_1/S}(\mathcal{L}) = \mathcal{N}_d(\mathcal{L}, D_1) = \mathcal{M}(\mathcal{L}, \Sigma(D_1)) = \mathcal{M}(\mathcal{L}, \Sigma(D_2)) = \mathcal{N}_d(\mathcal{L}, D_2)\\ = \operatorname{Norm}_{D_2/S}(\mathcal{L}).\end{aligned} \tag{6.4.1}$$

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

$$\varphi_{\mathcal{L}, D_1, D_2}\colon \operatorname{Norm}_{D_1/S}(\mathcal{L}) \longrightarrow \operatorname{Norm}_{D_2/S}(\mathcal{L}) \tag{6.4.2}$$

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 equation (6.4.1).

We construct $\varphi_{\mathcal{L}, D_1, D_2}$ locally on S, and the functoriality of the construction takes care of making it global. So suppose that f is as before: $f \in \mathcal{O}_C(U)^\times$ and $f\cdot\colon \mathcal{O}_U \to \mathcal{O}_U$ extends to an isomorphism $f\cdot\colon \mathcal{O}_C(D_1) \to \mathcal{O}_C(D_2)$. Set $n \in \mathbb{Z}$ 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 $D_1 + D_2$. Define $D^- := \operatorname{div}(l_1)$, $D^+ := \operatorname{div}(l_0)$ and $V := C \setminus (D^+ + D^-)$. Note that V contains $D_1 + D_2$ and that U contains $D^+ + D^-$. Then on V, $l := l_0/l_1$ is in $\mathcal{L}(V)$ and 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, $\operatorname{div}(l) = D^+ - D^-$. Let

$$f(\operatorname{div}(l)) = f\left(D^+ - D^-\right) := \operatorname{Norm}_{D^+/S}(f|_{D^+}) \cdot \operatorname{Norm}_{D^-/S}(f|_{D^-})^{-1} \in \mathcal{O}_S(S)^\times, \tag{6.4.3}$$

and let $\varphi_{\mathcal{L}, l, f}$ be the isomorphism

$$\begin{aligned}\varphi_{\mathcal{L}, l, f}\colon \operatorname{Norm}_{D_1/S}(\mathcal{L}) &\longrightarrow \operatorname{Norm}_{D_2/S}(\mathcal{L}),\\ \operatorname{Norm}_{D_1/S}(l) &\longmapsto f(\operatorname{div}(l))^{-1} \cdot \operatorname{Norm}_{D_2/S}(l),\end{aligned} \tag{6.4.4}$$

given in terms of generators. Now suppose that we made other choices n', l_0', l_1'. Then we get ${D^-}'$, ${D^+}'$, V', l' and $\varphi_{\mathcal{L}, l', f}$, and 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

$$\begin{aligned}
\varphi_{\mathcal{L},l',f}(\mathrm{Norm}_{D_1/S}(l)) &= \varphi_{\mathcal{L},l',f}\left(\mathrm{Norm}_{D_1/S}\left(g^{-1}l'\right)\right)\\
&= \varphi_{\mathcal{L},l',f}\left(g^{-1}(D_1)\mathrm{Norm}_{D_1/S}(l')\right)\\
&= g^{-1}(D_1)\cdot\varphi_{\mathcal{L},l',f}\left(\mathrm{Norm}_{D_1/S}(l')\right)\\
&= g^{-1}(D_1)\cdot f(\mathrm{div}(l'))^{-1}\cdot\mathrm{Norm}_{D_2/S}(l')\\
&= g^{-1}(D_1)\cdot f(\mathrm{div}(gl))^{-1}\cdot\mathrm{Norm}_{D_2/S}(gl) \qquad (6.4.5)\\
&= g^{-1}(D_1)\cdot f(\mathrm{div}(g)+\mathrm{div}(l))^{-1}\cdot g(D_2)\cdot\mathrm{Norm}_{D_2/S}(l)\\
&= g^{-1}(D_1)\cdot f(\mathrm{div}(g))^{-1}\cdot g(D_2)\cdot f(\mathrm{div}(l))^{-1}\cdot\mathrm{Norm}_{D_2/S}(l)\\
&= g(\mathrm{div}(f))\cdot f(\mathrm{div}(g))^{-1}\cdot\varphi_{\mathcal{L},l,f}\left(\mathrm{Norm}_{D_1/S}(l)\right)\\
&= \varphi_{\mathcal{L},l,f}\left(\mathrm{Norm}_{D_1/S}(l)\right),
\end{aligned}$$

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 $\varphi_{\mathcal{L},l,f} = \varphi_{\mathcal{L},l',f}$.

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,

$$\begin{aligned}
\varphi_{\mathcal{L},l,f'}\left(\mathrm{Norm}_{D_1/S}(l)\right) &= (u\cdot f)(\mathrm{div}(l))^{-1}\cdot\mathrm{Norm}_{D_2/S}(l)\\
&= u^{-\deg(\mathrm{div}(l))}f(\mathrm{div}(l))^{-1}\cdot\mathrm{Norm}_{D_2/S}(l) \qquad (6.4.6)\\
&= f(\mathrm{div}(l))^{-1}\cdot\mathrm{Norm}_{D_2/S}(l) = \varphi_{\mathcal{L},l,f}\left(\mathrm{Norm}_{D_1/S}(l)\right).
\end{aligned}$$

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

$$\varphi_{D_1,D_2,\mathcal{L}}\colon \mathrm{Norm}_{D_1/S}(\mathcal{L}) \longrightarrow \mathrm{Norm}_{D_2/S}(\mathcal{L}) \qquad (6.4.7)$$

as the isomorphism $\varphi_{\mathcal{L},l,f}$ in formula (6.4.4) for any local choice of f and l.

Lemma 6.4.8. *With the assumptions as in the beginning of §6.4, the isomorphism $\varphi_{\mathcal{L},D_1,D_2}$ in formula (6.4.7) is equal to the isomorphism in equation (6.4.1).*

Proof. We do this, as in the proof of Proposition 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 two 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 $\varphi_{D_1,D_2,\mathcal{O}_C} = \varphi_{\mathcal{O}_C,1,f}$ is the identity on $\mathcal{O}_S$ (use definition (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 $0 \times C^{(d)}$. □

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

$$\varphi_{D_1,D_2}\colon \mathrm{Norm}_{D_1/S}(\mathcal{O}_C(D_2)) \longrightarrow \mathrm{Norm}_{D_2/S}(\mathcal{O}_C(D_1)) \qquad (6.5.1)$$

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 $\mathbb{Z}_{\geq 0}$, define $U := C^{(d_1)} \times_S C^{(d_2)}$ 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, 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 $(\varphi_{D_1,D_2})_{U^0}$ 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 and 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 an S-scheme to $C^{d_1+d_2-1}$ and hence smooth over S. Now

$$\mathrm{Norm}_{D_1/U'}(\mathcal{O}(D_2)) = \bigotimes_{i,j} P_i^*\mathcal{O}(Q_j), \qquad \mathrm{Norm}_{D_2/U'}(\mathcal{O}(D_1)) = \bigotimes_{i,j} Q_j^*\mathcal{O}(P_i), \tag{6.5.2}$$

and on U'^0,

$$\mathrm{Norm}_{D_1/U'}(1) = \bigotimes_{i,j} 1, \qquad \mathrm{Norm}_{D_2/U'}(1) = \bigotimes_{i,j} 1, \quad \text{in } \mathcal{O}\left(U'^0\right). \tag{6.5.3}$$

The divisor on U' 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 $(\varphi_{D_1,D_2})_{U^0}$ 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 that $P^*\mathcal{O}_C(Q) = P^*\mathcal{O}_C(P)$ is the tangent space of $C \to S$ at P, and hence also at Q, but $\varphi_{P,Q}$ 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 6.5.4. *Let b be an S-point on C. Because of the symmetry in Proposition 6.3.2, using equation (6.3.13)), we have for D_1, D_2 relative effective divisors on C of degree d_1,d_2 over S the following diagram of isomorphisms defining ψ_{D_1,D_2}:*

$$\begin{tikzcd}
\mathcal{M}(\Sigma(D_2),\Sigma(D_1)) \arrow[r, equal] \arrow[d, equal] & \mathrm{Norm}_{D_1/S}(\mathcal{O}_C(D_2 - d_2b)) \otimes b^*\mathcal{O}_C(D_2 - d_2b)^{-d_1} \arrow[d, "\psi_{D_1,D_2}"] \\
\mathcal{M}(\Sigma(D_1),\Sigma(D_2)) \arrow[r, equal] & \mathrm{Norm}_{D_2/S}(\mathcal{O}_C(D_1 - d_1b)) \otimes b^*\mathcal{O}_C(D_1 - d_1b)^{-d_2}.
\end{tikzcd}$$

Then

$$\psi_{D_1,D_2} = \varphi_{D_1,D_2} \otimes \varphi^{-1}_{D_1,d_2b} \otimes \varphi^{-1}_{d_1b,D_2} \otimes \varphi_{d_1b,d_2b}. \tag{6.5.5}$$

Moreover, the isomorphisms φ_{D_1,D_2} and consequently ψ_{D_1,D_2} are compatible with addition of divisors – that is, under equations (6.3.10) and (6.3.8), we have for every triple D_1,D_2,D_3 of relative Cartier divisors on C

$$\varphi_{D_1+D_2,D_3} = \varphi_{D_1,D_3}\otimes\varphi_{D_2,D_3}, \qquad \varphi_{D_1,D_2+D_3} = \varphi_{D_1,D_2}\otimes\varphi_{D_1,D_3}. \tag{6.5.6}$$

Proof. It is enough to prove the lemma 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

$$u\cdot\psi_{D_1,D_2} = \varphi_{D_1,D_2}\otimes\varphi^{-1}_{D_1,d_2b}\otimes\varphi^{-1}_{d_1b,D_2}\otimes\varphi_{d_1b,d_2b}. \tag{6.5.7}$$

Since the symmetry in Proposition 6.3.2 is compatible with the rigidification at $(0,0)\in(J\times J)(S)$, ψ_{d_1b,d_2b} is the identity on $\mathcal{O}_U$, as well as the right-hand side of equation (6.5.5) when $D_i = d_ib$. Hence $u = u(d_1b,d_2b) = 1$, proving equation (6.5.5).

Now we prove equation (6.5.6). As with equation (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

$$\begin{aligned}\varphi_{d_1b+d_2b,d_3b} &= \varphi_{d_1b,d_3b}\otimes\varphi_{d_2b,d_3b} = (-1)^{(d_1+d_2)d_3},\\ \varphi_{d_1b,d_2b+d_3b} &= \varphi_{d_1b,d_2b}\otimes\varphi_{d_1b,d_3b} = (-1)^{d_1(d_2+d_3)}.\end{aligned} \tag{6.5.8}$$

□

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 $b\in C(\mathbb{Z}/p^2)$, g the genus and $\mathcal{M}$ be as in Proposition 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 $\mathcal{M}^\times\left(\mathbb{Z}/p^2\right)_\alpha$, under the assumption that there exists a nonspecial split reduced divisor of degree g on $C_{\mathbb{F}_p}$.

Let $b_1,\ldots,b_g$ in $C\left(\mathbb{Z}/p^2\right)$ have distinct images $\overline{b}_i$ in $C(\mathbb{F}_p)$ such that $h^0(C_{\mathbb{F}_p},\overline{b}_1+\cdots+\overline{b}_g) = 1$ and let $b_{g+1},\ldots,b_{2g}$ in $C\left(\mathbb{Z}/p^2\right)$ 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

$$\begin{aligned} f_1\colon C^g &\longrightarrow J, && (c_1,\ldots,c_g)\longmapsto [\mathcal{O}_C(c_1+\cdots+c_g-(b_1+\cdots+b_g)+D)],\\ f_2\colon C^g &\longrightarrow J, && (c_1,\ldots,c_g)\longmapsto [\mathcal{O}_C(c_1+\cdots+c_g-(b_{g+1}+\cdots+b_{2g})+E)],\end{aligned} \tag{6.6.1}$$

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

$$x_{D,c}\in\mathcal{O}_C(-D)_c \text{ a generator and } x_c\in\mathcal{O}_{C,c} \tag{6.6.2}$$

such that p and x_c generate the maximal ideal of $\mathcal{O}_{C,c}$.

For each $i = 1,\ldots,2g$ we choose x_{b_i} so that $x_{b_i}(b_i) = 0$. For each $\left(\mathbb{Z}/p^2\right)$-point $c\in C\left(\mathbb{Z}/p^2\right)$ 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 $C\left(\mathbb{Z}/p^2\right)_{\overline{c}}$ with $x_{\overline{c}}(c_\lambda) = \lambda p$. Then the map $\lambda\mapsto c_\lambda$ is a bijection $\mathbb{F}_p\to C\left(\mathbb{Z}/p^2\right)_{\overline{c}}$, and hence the maps f_1, f_2 induce bijections

$$\begin{aligned} \mathbb{F}_p^g &\longrightarrow J\left(\mathbb{Z}/p^2\right)_{\overline{D}}, & \lambda &\longmapsto D_\lambda := D + (b_{1,\lambda_1} - b_1) + \cdots + \left(b_{g,\lambda_g} - b_g\right),\\ \mathbb{F}_p^g &\longrightarrow J\left(\mathbb{Z}/p^2\right)_{\overline{E}}, & \mu &\longmapsto E_\mu := E + (b_{g+1,\mu_1} - b_{g+1}) + \cdots + \left(b_{2g,\mu_g} - b_{2g}\right). \end{aligned} \tag{6.6.3}$$

Hence $\mathcal{M}^\times\left(\mathbb{Z}/p^2\right)_{\overline{D},\overline{E}}$ is the union of $\mathcal{M}^\times(D_\lambda, E_\mu)$ as λ and μ vary in $\mathbb{F}_p^g$, and by Proposition 6.3.2 and Remark 6.3.12 we have

$$\begin{aligned} \mathcal{M}(D_\lambda, E_\mu) = {} & \mathrm{Norm}_{E^+/(\mathbb{Z}/p^2)}(\mathcal{O}_C(D_\lambda)) \otimes \mathrm{Norm}_{E^-/(\mathbb{Z}/p^2)}(\mathcal{O}_C(D_\lambda))^{-1} \\ & \otimes \bigotimes_{i=1}^{g} \left(b_{g+i,\mu_i}^* \mathcal{O}_C(D_\lambda) \otimes b_{g+i}^* \mathcal{O}_C(D_\lambda)^{-1}\right). \end{aligned} \tag{6.6.4}$$

For each $i \in \{1, \ldots, g\}$, $c \in C\left(\mathbb{Z}/p^2\right)$ 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 $c \in C\left(\mathbb{Z}/p^2\right)$ and each $\lambda \in \mathbb{F}_p^g$,

$$c^* \left(x_{D,c}^{-1} \cdot \prod_{i=1}^{g} \frac{x_i(c,0)}{x_i(c,\lambda_i)} \right) \text{ generates } c^*\mathcal{O}_C(D_\lambda). \tag{6.6.5}$$

We write $E^\pm = E^{0,\pm} + \cdots + E^{g,\pm}$ so that $E^{0,\pm}$ is disjoint from $\left\{\overline{b}_1, \ldots, \overline{b}_g\right\}$ 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 neighbourhood of $E^+ \cup E^-$. Then for each λ in $\mathbb{F}_p^g$,

$$\mathrm{Norm}_{E^{0,\pm}/(\mathbb{Z}/p^2)}\left(x_{D,E}^{-1}\right) \otimes \bigotimes_{i=1}^{g} \mathrm{Norm}_{E^{i,\pm}/(\mathbb{Z}/p^2)}\left(x_{D,E}^{-1} \cdot \frac{x_{b_i}}{x_{b_i} - \lambda_i p}\right) \tag{6.6.6}$$

generates $\mathrm{Norm}_{E^\pm/(\mathbb{Z}/p^2)}(\mathcal{O}_C(D_\lambda))$. By expressions (6.6.4)–(6.6.6), we see that for λ and μ in $\mathbb{F}_p^g$,

$$\begin{aligned} s_{D,E}(\lambda,\mu) := {} & \mathrm{Norm}_{E^{0,+}/(\mathbb{Z}/p^2)}\left(x_{D,E}^{-1}\right) \otimes \bigotimes_{i=1}^{g} \mathrm{Norm}_{E^{i,+}/(\mathbb{Z}/p^2)}\left(x_{D,E}^{-1} \cdot \frac{x_{b_i}}{x_{b_i} - \lambda_i p}\right) \\ & \otimes \mathrm{Norm}_{E^{0,-}/(\mathbb{Z}/p^2)}\left(x_{D,E}^{-1}\right)^{-1} \otimes \bigotimes_{i=1}^{g} \mathrm{Norm}_{E^{i,-}/(\mathbb{Z}/p^2)}\left(x_{D,E}^{-1} \cdot \frac{x_{b_i}}{x_{b_i} - \lambda_i p}\right)^{-1} \\ & \otimes \bigotimes_{i=1}^{g} \left(b_{g+i,\mu_i}^* \left(x_{D,b_{g+i}}^{-1} \cdot \prod_{j=1}^{g} \frac{x_j\left(b_{g+i,\mu_i}, 0\right)}{x_j\left(b_{g+i,\mu_i}, \lambda_j\right)} \right) \right. \\ & \left. \otimes b_{g+i}^* \left(x_{D,b_{g+i}}^{-1} \cdot \prod_{j=1}^{g} \frac{x_j\left(b_{g+i}, 0\right)}{x_j\left(b_{g+i}, \lambda_j\right)} \right)^{-1} \right) \end{aligned} \tag{6.6.7}$$

generates the free rank 1 $\mathbb{Z}/p^2$-module $\mathcal{M}(D_\lambda, E_\mu)$. The fibre $\mathcal{M}^\times\left(\overline{D}, \overline{E}\right)$ over $\left(\overline{D}, \overline{E}\right)$ in $(J \times J)(\mathbb{F}_p)$ is an $\mathbb{F}_p^\times$-torsor containing $\overline{s_{D,E}(0,0)}$ and 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 the fact that $\left(\mathbb{Z}/p^2\right)^\times = \mathbb{F}_p^\times \times (1+p\mathbb{F}_p)$, we conclude the following lemma:

Lemma 6.6.8. *With the assumptions and definitions from the start of §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*

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

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

$$\frac{x_c^2}{(x_c-\lambda p)(x_c-\mu p)} = \frac{x_c^2}{x_c^2-\lambda p x_c-\mu p x_c} = \frac{x_c}{x_c-(\lambda+\mu)p}; \tag{6.6.9}$$

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

$$(c_\lambda-c)+(c_\mu-c)=c_{\lambda+\mu}-c. \tag{6.6.10}$$

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

$$\begin{aligned} D_\lambda^0 &:= (b_{1,\lambda_1}-b_1)+\cdots+\left(b_{g,\lambda_g}-b_g\right), \\ E_\lambda^0 &:= (b_{g+1,\lambda_1}-b_{g+1})+\cdots+\left(b_{2g,\lambda_g}-b_{2g}\right), \end{aligned} \tag{6.6.11}$$

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 (6.6.7), applied with $(D,0)$ and $(0,E)$, $x_{0,E}=1$ and, for every $c\in C(\mathbb{F}_p)$, $x_{0,c}=1$, gives for all λ,μ in $\mathbb{F}_p^g$ the elements

$$s_{D,0}(\lambda,\mu)\in\mathcal{M}^\times\left(D_\lambda,E_\mu^0\right), \qquad s_{0,E}(\lambda,\mu)\in\mathcal{M}^\times\left(D_\lambda^0,E_\mu\right). \tag{6.6.12}$$

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

Lemma 6.6.13. *With the assumptions and definitions from the start of §6.6, we have, for all $\lambda,\lambda_1,\lambda_2,\mu,\mu_1,\mu_2$ in $\mathbb{F}_p^g$,*

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

Consequently, for all $\tau_1,\tau_2\in\mathbb{F}_p$ and $\xi_1,\xi_2\in\mathbb{F}_p^\times$, we have

$$\begin{aligned} \xi_1(1+\tau_1 p)\cdot s_{D,0}(\lambda,\mu_1)+_2\xi_2(1+\tau_2 p)\cdot s_{D,E}(\lambda,\mu_2) &= \xi_1(1+\tau_1 p)\xi_2(1+\tau_2 p)\cdot s_{D,E}(\lambda,\mu_1+\mu_2) \\ &= \xi_1\xi_2(1+(\tau_1+\tau_2)p)\cdot s_{D,E}(\lambda,\mu_1+\mu_2), \\ \xi_1(1+\tau_1 p)\cdot s_{0,E}(\lambda_1,\mu)+_1\xi_2(1+\tau_2 p)\cdot s_{D,E}(\lambda_2,\mu) &= \xi_1\xi_2(1+(\tau_1+\tau_2)p)\cdot s_{D,E}(\lambda_1+\lambda_2,\mu). \end{aligned} \tag{6.6.14}$$

Proof. This follows from equations (6.6.9) and (6.6.10), together with the equivalence of equations (6.3.7) and (6.3.8) and of equations (6.3.9) and (6.3.10) (in Proposition 6.3.2). □

We end this section with one more lemma:

Lemma 6.6.15. *The parametrisation in Lemma 6.6.8 is the inverse of a bijection given by parameters on $\mathcal{M}^\times$ analogously to definition (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 formula (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 $\left(C^{2g}\right)(\mathbb{F}_p)$ and induces a bijection between $\mathcal{Q}^\times\left(\mathbb{Z}/p^2\right)_{\overline{b}}$ and $\mathcal{M}^\times\left(\mathbb{Z}/p^2\right)_{\left(\overline{D},\overline{E}\right)}$. In particular, we can interpret $s_{D,E}(\lambda,\mu)$ as a section of $\mathcal{Q}\left(b_{1,\lambda_1},\dots b_{2g,\mu_g}\right)$ and interpret the parametrisation in Lemma 6.6.8 as a parametrisation of $Q^\times\left(\mathbb{Z}/p^2\right)_{\overline{\xi s_{D,E}(0,0)}}$. It is then enough to prove that the parametrisation in Lemma 6.6.8 is the inverse of a bijection given by parameters on $\mathcal{Q}^\times$. From the definition of c_ν for $c \in C\left(\mathbb{Z}/p^2\right)$ and $\nu \in \mathbb{F}_p$, the maps $\lambda_i\, \mu_i\colon C^{2g}\left(\mathbb{Z}/p^2\right)_{\overline{b}} \to \mathbb{F}_p$ are given by parameters in $\mathcal{O}_{C^{2g},\overline{b}}$ divided by p. In order to see that the coordinate $\tau\colon \mathcal{Q}^\times\left(\mathbb{Z}/p^2\right)_{\xi s_{D,E}(0,0)} \to \mathbb{F}_p$ is also 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 trivialising $\mathcal{Q}|_U$ such that $s_{D,E}(\lambda,\mu) = s\left(b_{1,\lambda_1},\dots,b_{2g,\mu_g}\right)$. Remark 6.3.12 and formula (6.5.1) give

$$\begin{aligned}\mathcal{Q} = &\bigotimes_{i,j=1}^{g} \left((\pi_i,\pi_{g+j})^* \mathcal{O}_{C\times C}(\Delta)\right)\\ &\otimes \bigotimes_{i=1}^{g} \left(\pi_i^*\mathcal{O}_C\left(E-(b_{g+1}+\cdots+b_{2g})\right)\otimes \pi_{g+i}^*\mathcal{O}_C\left(D-(b_1+\cdots+b_g)\right)\right)\\ &\otimes \mathrm{Norm}_{E/\mathbb{Z}/p^2}\left(\mathcal{O}_C\left(D-(b_1+\cdots+b_g)\right)\right)\otimes \bigotimes_{i=1}^{g} b_{g+i}^*\mathcal{O}_C\left(D-(b_1+\cdots+b_g)\right)^{-1},\end{aligned} \tag{6.6.16}$$

where $\Delta \subset C \times C$ is the diagonal and π_i is the ith 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 trivialising $\mathcal{Q}|_U$ such that $s_{D,E}(\lambda,\mu) = s\left(b_{1,\lambda_1},\dots,b_{2g,\mu_g}\right)$ by trivialising each factor of the tensor product in a neighbourhood 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 neighbourhood of (c_1,c_2) if $c_1 \neq c_2$, or by the section $x_{\Delta,c_1,c_2} := \pi_1^* x_{c_1} - \pi_2^* x_{c_2}$ in a neighbourhood 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 that there is a neighbourhood U of (b_i,b_{g+j}) such that $x_{\Delta,b_i,b_{g+j}}^{-1}$ generates $\mathcal{O}_{C\times C}(\Delta)|_U$. For each $\lambda,\mu \in \mathbb{F}_p^g$, the point $\left(b_{i,\lambda_i},b_{g+j,\mu_j}\right)$ lies in $U\left(\mathbb{Z}/p^2\right)$ and the canonical isomorphism $\left(b_{i,\lambda_i},b_{g+j,\mu_j}\right)^* \mathcal{O}_{C\times C}(\Delta) = b_{g+j,\mu_j}^* \mathcal{O}\left(b_{i,\lambda_i}\right)$ sends the generating section $\left(b_{i,\lambda_i},b_{j,\mu_j}\right)^* x_{\Delta,c_1,c_2}^{-1}$ to $b_{j,\mu_j}^* x_i\left(b_{g+j},\lambda_i\right)^{-1}$, which is a factor in definition (6.6.7). This gives a section $s_{i,j}$ trivialising $\left((\pi_i,\pi_{g+j})^* \mathcal{O}_{C\times C}(\Delta)\right)$ in a neighbourhood of b. With similar choices we can find sections trivialising the other factors in equation (6.6.16) in a neighbourhood of b, and tensoring all such sections we get a section s such that $s_{D,E}(\lambda,\mu) = s\left(b_{1,\lambda_1},\dots,b_{2g,\mu_g}\right)$. □

6.7. Extension of the Poincaré biextension over Néron models

Let C over $\mathbb{Z}$ be a curve as in §2 and 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 fibrewise connected component of 0. On $\left(J\times_{\mathbb{Z}_q} J\right)_{\mathbb{Q}_q}$ we have $\mathcal{M}$ as in Proposition 6.3.2, rigidified at $0\times J_{\mathbb{Q}_q}$ and at $J_{\mathbb{Q}_q}\times 0$.

Proposition 6.7.1. *The invertible $\mathcal{O}$-module $\mathcal{M}$ on $\left(J\times_{\mathbb{Z}_q} J\right)_{\mathbb{Q}_q}$, 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 $\left(J\times_{\mathbb{Z}_q} J^0\right)_{\mathbb{Q}_q}$ 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 $\left(J\times_{\mathbb{Z}_q} J^0\right)_{\mathbb{F}_q}$. 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 $\mathcal{M}|_{J_{\mathbb{Q}_q}\times 0}$, and 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 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 $\mathbb{Q}_q$, which 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 its required properties follow in the same way. We have now shown that $\widetilde{\mathcal{M}}^\times$ extends the biextension $\mathcal{M}^\times$. □

6.8. Explicit description of the extended Poincaré bundle

Let C over $\mathbb{Z}$ be a curve as in §2 and let q be a prime number that divides n. We also write C for $C_{\mathbb{Z}_q}$. By [22, 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 [28, Equations (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 $\mathrm{Gal}\left(\overline{\mathbb{F}}_q/\mathbb{F}_q\right)$ on the set of irreducible components of $C_{\overline{\mathbb{F}}_q}$ is nontrivial, then $\mathrm{Pic}_{C/\mathbb{Z}_q}$ is not representable by a $\mathbb{Z}_q$-scheme, only by an algebraic space over $\mathbb{Z}_q$ [28, Proposition 5.5]. Therefore, in order not to be annoyed by such inconveniences, we pass to $S:=\mathrm{Spec}\left(\mathbb{Z}_q^{\mathrm{unr}}\right)$, 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 $\left(\mathcal{L}^{\mathrm{univ}},\mathrm{rig}\right)$ [28, Proposition 5.5 and §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 0 on the fibres of $C\to S$. It contains the open part $\mathrm{Pic}^{0}_{C/S}$ where $\mathcal{L}^{\mathrm{univ}}$ has degree 0 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 [28]. It is contained in $\mathrm{Pic}^{[0]}_{C/S}$. By [28, Proposition 5.2], E is represented by an étale S-group scheme.

By [28, Theorem 8.1.4] or [9, 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

$$C_{\overline{\mathbb{F}}_q}=\sum_{i\in I} m_i C_i. \tag{6.8.1}$$

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

$$\mathrm{mdeg}(\mathcal{L})\colon I\to\mathbb{Z},\qquad i\mapsto \deg_{C_i}\left(\mathcal{L}|_{C_i}\right), \tag{6.8.2}$$

and the total degree is then

$$\deg(\mathcal{L})=\sum_{i\in I} m_i \deg_{C_i}\left(\mathcal{L}|_{C_i}\right). \tag{6.8.3}$$

The multidegree induces a surjective morphism of groups

$$\mathrm{mdeg}\colon \mathrm{Pic}_{C/S}(S)\to\mathbb{Z}^I. \tag{6.8.4}$$

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 $\mathrm{H}^1\left(C_{\overline{\mathbb{F}}_q},\mathcal{L}\right)=0$ 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 push-forward $\mathcal{E}$ 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 $\mathcal{O}_{C\times_S V}\left(D^{\mathrm{univ}}\right)\otimes_{\mathcal{O}_V} b^*\mathcal{O}_{C\times_S V}\left(-D^{\mathrm{univ}}\right)$ with its tautological rigidification at b; in a diagram,

$$\begin{tikzcd}\mathcal{L}^{\mathrm{univ}}\otimes\mathcal{L}_0 \arrow[r, equal] & \mathcal{O}_{C\times_S V}\left(D^{\mathrm{univ}}\right)\otimes_{\mathcal{O}_V} b^*\mathcal{O}_{C\times_S V}\left(-D^{\mathrm{univ}}\right).\end{tikzcd} \tag{6.8.5}$$

Then for T an S-scheme, $\Sigma_{\mathcal{L}_0}$ sends a T-point D on C_T to $\mathcal{O}_{C_T}(D) \otimes_{\mathcal{O}_T} b^*\mathcal{O}_{C_T}(-D) \otimes_{\mathcal{O}_C} \mathcal{L}_0^{-1}$ 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 $\mathrm{Pic}^{[0]}_{C/S} \times_S v_0$:

$$\mathcal{N}_{q,d}\colon \left(\mathrm{Pic}^{[0]}_{C/S} \times_S V\right)(T) \ni (\mathcal{L},\mathrm{rig},D) \longmapsto \mathrm{Norm}_{D/T}(\mathcal{L}) \otimes_{\mathcal{O}_T} \mathrm{Norm}_{D_0/T}(\mathcal{L})^{-1}. \tag{6.8.6}$$

Any global regular function on the integral scheme $\mathrm{Pic}^{[0]}_{C/S} \times_S V$ is constant on the generic fibre and 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 [25, 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 6.8.7. *In the situation of §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 rigidifications at $J \times 0$ and $\mathrm{Pic}^{[0]}_{C/\mathbb{Z}_q^{\mathrm{unr}}} \times v_0$. In a diagram:*

$$\begin{tikzcd}
P^{\times} \arrow[d] & \mathcal{M}^{\times} \arrow[l] \arrow[d] & \mathcal{N}_{q,d}^{\times} \arrow[l] \arrow[d] \\
J \times_{\mathbb{Z}_q^{\mathrm{unr}}} J^{\vee,0} & J \times_{\mathbb{Z}_q^{\mathrm{unr}}} J^0 \arrow[l, "\mathrm{id}\times j_b^{*,-1}"'] & \mathrm{Pic}^{[0]}_{C/\mathbb{Z}_q^{\mathrm{unr}}} \times_{\mathbb{Z}_q^{\mathrm{unr}}} V. \arrow[l, "\mathrm{quot}\times\Sigma_{\mathcal{L}_0}"']
\end{tikzcd} \tag{6.8.8}$$

For T any $\mathbb{Z}_q^{\mathrm{unr}}$-scheme, 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

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

Proof. The scheme $\mathrm{Pic}^{[0]}_{C/\mathbb{Z}_q^{\mathrm{unr}}} \times_{\mathbb{Z}_q^{\mathrm{unr}}} V$ is smooth over $\mathbb{Z}_q^{\mathrm{unr}}$ and hence regular, and connected and hence integral; and since $V_{\overline{\mathbb{F}}_q}$ is irreducible, the irreducible components of $\left(\mathrm{Pic}^{[0]}_{C/\mathbb{Z}_q^{\mathrm{unr}}} \times_{\mathbb{Z}_q^{\mathrm{unr}}} V\right)_{\overline{\mathbb{F}}_q}$ are the $P^i \times_{\overline{\mathbb{F}}_q} V_{\overline{\mathbb{F}}_q}$, with P^i the irreducible components of $\left(\mathrm{Pic}^{[0]}_{C/\mathbb{Z}_q^{\mathrm{unr}}}\right)_{\overline{\mathbb{F}}_q}$, with i in $\pi_0\left(\left(\mathrm{Pic}^{[0]}_{C/\mathbb{Z}_q^{\mathrm{unr}}}\right)_{\overline{\mathbb{F}}_q}\right)$ – 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 prove the first claim. Both $\mathcal{N}_{q,d}$ and the pullback of $\mathcal{M}$ are rigidified on $\mathrm{Pic}^{[0]}_{C/\mathbb{Z}_q^{\mathrm{unr}}} \times v_0$. After inverting q, we will give 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 $\left(\mathrm{Pic}^{[0]}_{C/\mathbb{Z}_q^{\mathrm{unr}}} \times_{\mathbb{Z}_q^{\mathrm{unr}}} V\right)_{\overline{\mathbb{F}}_q}$, such that α is an isomorphism from $\mathcal{N}_{q,d}(D_\alpha)$ to the pullback of $\mathcal{M}$. Let i be in $\pi_0\left(\left(\mathrm{Pic}^{[0]}_{C/\mathbb{Z}_q^{\mathrm{unr}}}\right)_{\overline{\mathbb{F}}_q}\right)$ and let x be in $\mathrm{Pic}^{[0]}_{C/\mathbb{Z}_q^{\mathrm{unr}}}\left(\mathbb{Z}_q^{\mathrm{unr}}\right)$ 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 0. Hence D_α is 0.

Let us now give, over $\left(\mathrm{Pic}^{[0]}_{C/\mathbb{Z}_q^{\mathrm{unr}}} \times_{\mathbb{Z}_q^{\mathrm{unr}}} V\right)_{\mathbb{Q}_q^{\mathrm{unr}}}$, an isomorphism α from $\mathcal{N}_{q,d}$ to the pullback of $\mathcal{M}$. Note that $\left(\mathrm{Pic}^{[0]}_{C/\mathbb{Z}_q^{\mathrm{unr}}}\right)_{\mathbb{Q}_q^{\mathrm{unr}}} = J_{\mathbb{Q}_q^{\mathrm{unr}}}$ 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, using Proposition 6.3.2 and definition (6.8.6) we have the following isomorphisms (functorial in T), respecting the rigidifications at $v = v_0$:

$$\begin{aligned}\mathcal{M}(x, \Sigma_{\mathcal{L}_0}(v)) &= \mathcal{M}(x, \Sigma(v) - \Sigma(v_0)) = \mathcal{M}(x, \Sigma(v)) \otimes \mathcal{M}(x, \Sigma(v_0))^{-1} \\ &= \mathrm{Norm}_{D/T}(\mathcal{L}) \otimes_{\mathcal{O}_T} \mathrm{Norm}_{D_0/T}(\mathcal{L})^{-1} = \mathcal{N}_{q,d}(x,v).\end{aligned} \tag{6.8.9}$$

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 6.3.2. □

6.9. Integral points of the extended Poincaré torsor

Let C over $\mathbb{Z}$ be a curve as in §2. Given a point $(x,y) \in \left(J \times J^0\right)(\mathbb{Z})$, 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 0 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, 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 6.3.2 with $S = \mathrm{Spec}(\mathbb{Z}[1/n])$ gives

$$\mathcal{M}(x,y)[1/n] = \left(\mathrm{Norm}_{D^+/\mathbb{Z}}(\mathcal{L}) \otimes_{\mathbb{Z}} \mathrm{Norm}_{D^-/\mathbb{Z}}(\mathcal{L})^{-1}\right)[1/n], \tag{6.9.1}$$

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

$$\mathcal{M}(x,y) = \left(\prod_{q|n} q^{e_q}\right) \cdot \left(\mathrm{Norm}_{D^+/\mathbb{Z}}(\mathcal{L}) \otimes_{\mathbb{Z}} \mathrm{Norm}_{D^-/\mathbb{Z}}(\mathcal{L})^{-1}\right). \tag{6.9.2}$$

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 $C_{i,q}$ $(i \in I_q)$ be 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 6.9.3. *The integers in equation* (6.9.2) *are given by*

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

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 $\mathbb{Z}$ and 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 a 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

$$\operatorname{div}(f_q) = \left(D_q^+ - D_q^-\right) - (D+V) = \left(D_q^+ + D^-\right) - \left(D^+ + D_q^-\right) - V. \tag{6.9.4}$$

This linear equivalence, restricted to $\mathbb{Q}_q$, gives, via the definition in (6.4.7), the isomorphism

$$\varphi\colon \operatorname{Norm}_{(D^+ + D_q^-)/\mathbb{Q}_q}(\mathcal{L}) \longrightarrow \operatorname{Norm}_{(D_q^+ + D^-)/\mathbb{Q}_q}(\mathcal{L}). \tag{6.9.5}$$

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

$$\varphi\otimes\mathrm{id}\colon \operatorname{Norm}_{D^+/\mathbb{Q}_q}(\mathcal{L})\otimes\operatorname{Norm}_{D^-/\mathbb{Q}_q}(\mathcal{L})^{-1} \longrightarrow \operatorname{Norm}_{D_q^+/\mathbb{Q}_q}(\mathcal{L})\otimes\operatorname{Norm}_{D_q^-/\mathbb{Q}_q}(\mathcal{L})^{-1} \tag{6.9.6}$$

using the identifications

$$\begin{aligned}\operatorname{Norm}_{D^+/\mathbb{Q}_q}(\mathcal{L})\otimes\operatorname{Norm}_{D^-/\mathbb{Q}_q}(\mathcal{L})^{-1} &= \operatorname{Norm}_{\left(D^+ + D_q^-\right)/\mathbb{Q}_q}(\mathcal{L})\otimes\operatorname{Norm}_{\left(D^- + D_q^-\right)/\mathbb{Q}_q}(\mathcal{L})^{-1},\\ \operatorname{Norm}_{D_q^+/\mathbb{Q}_q}(\mathcal{L})\otimes\operatorname{Norm}_{D_q^-/\mathbb{Q}_q}(\mathcal{L})^{-1} &= \operatorname{Norm}_{\left(D_q^+ + D^-\right)/\mathbb{Q}_q}(\mathcal{L})\otimes\operatorname{Norm}_{\left(D^- + D_q^-\right)/\mathbb{Q}_q}(\mathcal{L})^{-1}.\end{aligned} \tag{6.9.7}$$

Using the same method as we used to get the rational section f_q of $\mathcal{O}_C(D+V)$, we get a rational section l of $\mathcal{L}$ with the support of $\operatorname{div}(l)$ 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 6.8.7 and the choice of l,

$$\mathcal{M}(x,y)_{\mathbb{Z}_q} = \operatorname{Norm}_{D_q^+/\mathbb{Z}_q}(\mathcal{L})\otimes\operatorname{Norm}_{D_q^-/\mathbb{Z}_q}(\mathcal{L})^{-1} = \mathbb{Z}_q\cdot\operatorname{Norm}_{D_q^+/\mathbb{Z}_q}(l)\otimes\operatorname{Norm}_{D_q^-/\mathbb{Z}_q}(l)^{-1} \tag{6.9.8}$$

and

$$\operatorname{Norm}_{D^+/\mathbb{Z}_q}(\mathcal{L})\otimes\operatorname{Norm}_{D^-/\mathbb{Z}_q}(\mathcal{L})^{-1} = \mathbb{Z}_q\cdot\operatorname{Norm}_{D^+/\mathbb{Z}_q}(l)\otimes\operatorname{Norm}_{D^-/\mathbb{Z}_q}(l)^{-1}. \tag{6.9.9}$$

By definition (6.4.4), we have that $\varphi\otimes\mathrm{id}$ maps

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

to

$$f_q(\mathrm{div}(l))^{-1} \cdot \mathrm{Norm}_{D_q^+/\mathbb{Q}_q}(l) \otimes \mathrm{Norm}_{D_q^-/\mathbb{Q}_q}(l)^{-1}. \tag{6.9.10}$$

Comparing with equation (6.9.2), we conclude that

$$e_q = v_q\left(f_q(\mathrm{div}(l))\right). \tag{6.9.11}$$

We write $\mathrm{div}(l) = \sum_j n_j D_j$ as a sum of prime divisors. These D_j are finite over $\mathbb{Z}_q$ and 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, both $f_q^{m_{s(j),q}}$ 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 neighbourhood of D_j. Then we have

$$\begin{aligned} v_q\left(f_q\left(D_j\right)\right) &= \frac{v_q\left(f_q^{m_{s(j),q}}\left(D_j\right)\right)}{m_{s(j),q}} = \frac{v_q\left(q^{-V_{s(j),q}}\left(D_j\right)\right)}{m_{s(j),q}} = \frac{v_q\left(\mathrm{Norm}_{D_j/\mathbb{Z}_q}\left(q^{-V_{s(j),q}}\right)\right)}{m_{s(j),q}} \\ &= \frac{-V_{s(j),q}\deg_{\mathbb{Z}_q}\left(D_j\right)}{m_{s(j),q}} = \frac{-V_{s(j),q}\cdot\left(D_j\cdot C_{\mathbb{F}_q}\right)}{m_{s(j),q}} = \frac{-V_{s(j),q}\cdot\left(D_j\cdot m_{s(j),q}C_{s(j),q}\right)}{m_{s(j),q}} \\ &= -V_{s(j),q}\left(D_j\cdot C_{s(j)}\right) = -V_q\cdot D_j. \end{aligned} \tag{6.9.12}$$

We get

$$\begin{aligned} e_q = v_q\left(f_q(\mathrm{div}(l))\right) = -V_q\cdot\mathrm{div}(l) = -\sum_{i\in I_q} V_{i,q}(C_i\cdot\mathrm{div}(l)) \\ = -\sum_{i\in I_q} V_{i,q}\deg_{\mathbb{F}_q}\left(\mathcal{L}|_{C_{i,q}}\right). \end{aligned} \tag{6.9.13}$$

□

7. Description of the map from the curve to the torsor

The situation is as in §2. The aim of this section is to give descriptions of all the morphisms in diagram (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 making computations when applying Theorem 4.12. The main point is that each $\mathrm{tr}_{c_i}\circ f_i$ is described in diagram (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 7.8 describes $\left(\widetilde{j_b}\right)_i\colon C_{\mathbb{Z}[1/n]}\to T_i$. For finding the required line bundles, see [12].

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 group schemes 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 and $\mathcal{L}_\alpha$ be the pullback of $\mathcal{M}$ (see diagram (6.3.3)) to $C_{\mathbb{Q}}\times C_{\mathbb{Q}}$ via $j_b\times(\alpha\circ j_b)$, and define $T_\alpha := (\mathrm{id},\alpha)^*\mathcal{M}^\times$ on $J_{\mathbb{Q}}$:

$$\begin{tikzcd}
 & T_\alpha \arrow[rr] \arrow[d] & & \mathcal{M}^\times \arrow[dl] \\
C_{\mathbb{Q}} \arrow[r, "j_b"] \arrow[d, "\mathrm{diag}"] & J_{\mathbb{Q}} \arrow[r, "(\mathrm{id},\alpha)"] & (J\times J)_{\mathbb{Q}} & \\
(C\times C)_{\mathbb{Q}} \arrow[r, "\mathrm{id}\times j_b"] & (C\times J)_{\mathbb{Q}} \arrow[r, "\mathrm{id}\times\alpha"] & (C\times J)_{\mathbb{Q}} \arrow[u, "j_b\times\mathrm{id}"'] & \\
\mathcal{L}_\alpha^\times \arrow[u] \arrow[rrr] & & & \mathcal{L}^{\mathrm{univ},\times}. \arrow[ul] \arrow[uuu]
\end{tikzcd} \tag{7.1}$$

Then $(b,\mathrm{id})^*\mathcal{L}_\alpha = \mathcal{O}_{C_{\mathbb{Q}}}$, $\mathcal{L}_\alpha$ is of degree 0 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 (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 7.2. *In the situation of Section 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 7.2. Then $\mathrm{diag}^*\mathcal{L}=\mathcal{O}_{C_{\mathbb{Q}}}$, compatible with rigidifications at b. Let

$$\ell\in\left(\mathrm{diag}^*\mathcal{L}^\times\right)(C_{\mathbb{Q}}) \tag{7.3}$$

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:

$$\begin{tikzcd}
 & & T_{m\cdot\circ\alpha_{\mathcal{L}}} \arrow[r] \arrow[d] & \mathcal{M}^\times \arrow[d] \\
U \arrow[r] \arrow[urr, "\widetilde{j_b}"] & C^{\mathrm{sm}} \arrow[r, "j_b"] & J \arrow[r, "(\mathrm{id},m\cdot\circ\alpha_{\mathcal{L}})"] & J\times J^0.
\end{tikzcd} \tag{7.4}$$

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

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

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, through a 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

$$\begin{aligned}\mathcal{M}(\Sigma(D),\alpha_{\mathcal{L}}(\Sigma(E))) &= \mathcal{M}(\alpha_{\mathcal{L}}(\Sigma(E)),\Sigma(D))\\ &= \mathcal{M}\left(\beta_{\mathcal{L}}(b) + \sum_j (\beta_{\mathcal{L}}(y_j) - \beta_{\mathcal{L}}(b)), \sum_i j_b(x_i)\right)\\ &= \left(\bigotimes_i \mathcal{L}(x_i,b)^{\otimes(1-e)}\right) \otimes \bigotimes_{i,j} \mathcal{L}(x_i,y_j),\end{aligned} \tag{7.5.1}$$

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 multiplying ℓ by the product, over the primes q dividing n, of q^{-W_q} generates $\mathrm{diag}^*\mathcal{L}$ on U:

$$\left(\prod_{q|n} q^{-W_q}\right)\cdot\ell \in \left(\mathrm{diag}^*\mathcal{L}^\times\right)(U). \tag{7.6}$$

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

$$\mathcal{L}^m := \mathcal{L}^{\otimes m}(V) \text{ on } C \times U \tag{7.7}$$

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 the fact that $J^0_{\mathbb{F}_q}$ is geometrically connected for all $q \mid n$). Hence on U we have $j_b^*T_{m\cdot\circ\alpha_{\mathcal{L}}} = \mathrm{diag}^*\left(\mathcal{L}^{\otimes m}(V)^\times\right)$, 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 7.8. *For x and S as in Proposition 7.5, we have the following description of $\widetilde{j}_b$:*

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

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 [18], and computions in Magma show that that equation and the equations later give isomorphic curves over $\mathbb{Q}$.

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

$$V_1: y^2+y=x^6-3x^5+x^4+3x^3-x^2-x,$$
$$V_2: w^2+z^3w=1-3z+z^2+3z^3-z^4-z^5,$$

by gluing 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 also be 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, C_0 is finite of degree 2 over $\mathbb{P}^1_{\mathbb{Z}}$. Hence C_0 is proper over $\mathbb{Z}$ and is moreover smooth over $\mathbb{Z}[1/n]$ with $n=3\cdot 43$. The generic fibre 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 $P_0=(3,x-2,y-1)$ contained in V_1, and the blowup C of C_0 in P_0 is regular.

In the rest of this section we apply our geometric method to the curve C and prove that $C(\mathbb{Z})$ contains exactly 14 elements. We use the same notation as in §§2 and 4.

The fibre $C_{\mathbb{F}_{43}}$ is absolutely irreducible, whereas $C_{\mathbb{F}_3}$ is the union of two geometrically irreducible curves, a curve of genus 0 lying above the point P_0 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 §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 fibres 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

$$m=2. \tag{8.1}$$

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

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

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 $\rho = 2$.

8.2. 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 fix the base point $b = \infty$ in $C(\mathbb{Z})$. Following §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 $T = (\mathrm{id}, m \cdot \circ \alpha)^* \mathcal{M}^\times$ depends only on the scheme morphism $\alpha \colon J_{\mathbb{Q}} \to J_{\mathbb{Q}}$, which by Proposition 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 nontrivial $\mathcal{O}$-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 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

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

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

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

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

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

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 7.5, the torsor $T := T_{m \cdot \circ \alpha_{\mathcal{L}}}$ on J, for S a $\mathbb{Z}[1/n]$-scheme and x in $C(S)$, using the trivialisation given by l and l_b and with $m = 2$ as explained before equation (8.1), satisfies

$$\begin{aligned} T(j_b(x)) &= \mathcal{M}^\times(j_b(x), m\cdot\alpha_{\mathcal{L}}(j_b(x))) = \mathcal{M}^\times\left(j_b(x), (\mathrm{id},x)^*\mathcal{L}^{\otimes m}\right) \\ &= x^*(\mathrm{id},x)^*\mathcal{L}^{\otimes m,\times} \otimes b^*(\mathrm{id},x)^*\mathcal{L}^{\otimes -m,\times} \\ &= \mathcal{L}^{\otimes m,\times}(x,x) \otimes \mathcal{L}^{\otimes m,\times}(b,x)^{-1} = \mathcal{L}^{\otimes m,\times}(x,x) = \mathcal{O}_S^\times. \end{aligned} \tag{8.2.1}$$

Using Proposition 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 fibres $C \times U_1 \to U_1$, hence in order to compute $\widetilde{j_{b,1}}$ we must take $V = 0$ in definition (7.7), giving $V_3 = V_{43} = 0$. Hence for S and x as in equation (8.2.1), assuming moreover that 2 is invertible on S,

$$\begin{aligned} \widetilde{j_{b,1}}(x) &= l^2 \otimes l_b^{-2} = \frac{1}{4}(x^*1) \otimes (b^*1)^{-1} \text{ in} \\ T(j_b(x)) &= x^*(\mathrm{id},x)^*\mathcal{L}^{\otimes m,\times} \otimes b^*(\mathrm{id},x)^*\mathcal{L}^{\otimes -m,\times} \\ &= x^*\mathcal{O}_{C_S}(\eta(x) - \infty_-)^\times \otimes b^*\mathcal{O}_{C_S}(\eta(x) - \infty_-)^\times, \end{aligned} \tag{8.2.2}$$

where the last equality 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 fibres $C \times U_0 \to U_0$ of characteristic not 3; a fibre of characteristic 3 has degree 2 over K_0 and degree -2 over K_1. Hence to compute $\widetilde{j_{b,0}}$ we take $V = K_0 \times (K_0 \cap U_0)$ in definition (7.7), giving $V_{43} = 0$, $V_3 = 1$. Hence for S and x as in equation (8.2.1), assuming moreover that 2 is invertible on S,

$$\begin{aligned} \widetilde{j_{b,0}}(x) &= \frac{1}{3} l^2 \otimes l_b^{-2} = \frac{1}{12}(x^*1) \otimes (b^*1)^{-1} \text{ in} \\ T(j_b(x)) &= x^*(\mathrm{id},x)^*\mathcal{L}^{\otimes m,\times} \otimes b^*(\mathrm{id},x)^*\mathcal{L}^{\otimes -m,\times} \\ &= x^*\mathcal{O}_{C_S}(\eta(x) - \infty_-)^\times \otimes b^*\mathcal{O}_{C_S}(\eta(x) - \infty_-)^\times, \end{aligned} \tag{8.2.3}$$

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

8.3. Some integral points on the biextension

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

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

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

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

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 6.9.3, we have

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

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, $2f(G_1)$ already has multidegree 0 over 43, so $e_{43}=0$. If we look at $C_{\mathbb{F}_3}$, $2f(G_1)$ does not have multidegree 0, while $2f(G_1)+K_0$ has multidegree 0; hence, by Proposition 6.9.3,

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

Notice that over $\mathbb{Z}\left[\frac{1}{2}\right]$ 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 blowup), and thus $\beta^{*}\mathcal{O}_C(\gamma-\alpha)$ and $\delta^{*}\mathcal{O}_C(\gamma-\alpha)$ are generated by $\beta^{*}1$ and $\delta^{*}1$ over $\mathbb{Z}\left[\frac{1}{2}\right]$. 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

$$\begin{aligned}&\mathcal{M}(G_1,m\cdot f(G_1)) = 3^{-1}\cdot(\delta^{*}2)^2\otimes\left(\beta^{*}2^{-1}\right)^{-2}\cdot\mathbb{Z} = 2^4\cdot 3^{-1}\cdot(\delta^{*}1)^2\otimes(\beta^{*}1)\cdot\mathbb{Z},\\ &Q_{1,1} := \pm 2^4\cdot 3^{-1}\cdot(\delta^{*}1)^2\otimes(\beta^{*}1)^{-2}\quad \text{generates } \mathcal{M}_{G_1,m\cdot f(G_1)}.\end{aligned}$$

With analogous computations, we see that

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

8.4. Some residue disks of the biextension

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

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

we use Lemma 6.6.8 to give parameters on the residue disks in $\mathcal{M}^{\times}\left(\mathbb{Z}/p^2\right)_{\overline{D},\overline{E}}$ and $T\left(\mathbb{Z}/p^2\right)_{\overline{D}}$, with $\overline{D},\overline{E}$ the images of D,E in $\mathrm{Div}\left(C_{\mathbb{F}_p}\right)$.

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 $h^0\left(C_{\mathbb{F}_p}, b_1+b_2\right) = h^0\left(C_{\mathbb{F}_p}, b_3+b_4\right)=1$. As in formula (6.6.2), we define $x_\alpha = x-1$, $x_\infty = z$, $x_\beta = x$, $x_{D,\beta}=x_{D,\infty_-}=1$ and $x_{D,\infty}=z^{-1}$. 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 mod p and such that $x_Q(Q_a) = ap \in \mathbb{Z}/p^2$. We have the bijections

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

Following definition (6.6.7), for $\lambda,\mu \in \mathbb{F}_p^2$ we define

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

which – by Proposition 6.3.2 and Remark 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 $\left(\mathbb{Z}/p^2\right)^\times = \mathbb{F}_p^\times \times (1+p\mathbb{F}_p)$, for each $\xi \in \mathbb{F}_p^\times$ we parametrise the residue disk of $\xi \cdot s_{D,E}(0,0)$ using the bijection in Lemma 6.6.8:

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

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

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

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 $\left(\overline{D},\overline{E}\right)$, and we have the following bijection induced by parameters in $\xi\cdot s_{D,E}(0,0)$:

$$\mathbb{F}_p^3 \longrightarrow T(\mathbb{Z}_p)_{\xi s_{D,E}(0,0)}, \qquad (\lambda_1,\lambda_2,\tau) \longmapsto (1+\tau p)\cdot\xi\cdot s_{D,E}((\lambda_1,\lambda_2),(-2\lambda_1,-2\lambda_2)). \quad (8.4.1)$$

If we apply equations (8.2.2) and (8.2.3) to $Q = \alpha_\lambda$ and use the symmetry of the Poincaré torsor explained in Proposition 6.3.2 and made explicit in Lemma 6.5.4, we obtain the following description of $\widetilde{j_{b,i}}$ on $C\left(\mathbb{Z}/p^2\right)_{\alpha_{\mathbb{F}_p}}$ when $p \neq 2$:

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

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

$$\widetilde{j_{b,1}}(\alpha_\lambda) = -(1+p)\cdot s_{D,E}((\lambda,0),(-2\lambda,0)), \qquad \widetilde{j_{b,0}}(Q) = 18\cdot(1+2p)\cdot s_{D,E}((\lambda,0),(-2\lambda,0)). \quad (8.4.2)$$

Since it is useful for computing the map $\kappa_{\mathbb{Z}}$ in the residue disks of $T\left(\mathbb{Z}/p^2\right)$ projecting to $\overline{D}$, we also apply Lemma 6.6.8 to the residue disks of $\mathcal{M}^\times\left(\mathbb{Z}/p^2\right)$ lying over $\left(\overline{D},0\right)$, $\left(0,\overline{E}\right)$ and $(0,0)$. Hence for $\lambda,\mu \in \mathbb{F}_p^2$ we define the divisors on $C_{\mathbb{Z}/p^2}$

$$D_\lambda^0 := \alpha_{\lambda_1} - \alpha + \infty_{\lambda_2} - \infty, \qquad E_\mu^0 := \beta_{\mu_1} - \beta + \infty_{\mu_2} - \infty,$$

and the sections

$$s_{D,0}(\lambda,\mu) := \left(\beta^*_{\mu_1}1\right)\otimes\left(\infty^*_{\mu_2}\frac{z^2}{z-\lambda_2 p}\right)\otimes(\beta^*1)^{-1}\otimes\left(\infty^*\frac{z^2}{z-\lambda_2 p}\right)^{-1} \quad \text{in } \mathcal{M}^\times\left(D_\lambda,E^0_\mu\right)\left(\mathbb{Z}/p^2\right),$$

$$s_{0,E}(\lambda,\mu) := (\beta^*1)\otimes\left(\beta^*_{\mu_1}1\right)\otimes\left(\infty^*_{\mu_2}\frac{z}{z-\lambda_2 p}\right)\otimes\left(\infty^*\frac{z}{z-\lambda_2 p}\right)^{-1}\otimes(\infty^*_-1)^{-2} \quad \text{in } \mathcal{M}^\times\left(D^0_\lambda,E_\mu\right)\left(\mathbb{Z}/p^2\right),$$

$$s_{0,0}(\lambda,\mu) := \left(\beta^*_{\mu_1}1\right)\otimes\left(\infty^*_{\mu_2}\frac{z}{z-\lambda_2 p}\right)\otimes(\beta^*1)^{-1}\otimes\left(\infty^*\frac{z}{z-\lambda_2 p}\right)^{-1} \quad \text{in } \mathcal{M}^\times\left(D^0_\lambda,E^0_\mu\right)\left(\mathbb{Z}/p^2\right).$$

8.5. Geometry mod p^2 of integral points

From now on, $p=5$. Let $\overline{\alpha}\in C\left(\mathbb{Z}/p^2\right)$ be the image of $\alpha\in C(\mathbb{Z})$. In this subsection we compute the composition $\overline{\kappa}\colon \mathbb{Z}^2\to T\left(\mathbb{Z}/p^2\right)_{\widetilde{j_{b,1}(\overline{\alpha})}}$ of the map $\kappa_{\mathbb{Z}}\colon\mathbb{Z}^2\to T(\mathbb{Z}_p)_{\widetilde{j_{b,1}(\overline{\alpha})}}$ in formula (4.9) and the reduction map $T(\mathbb{Z}_p)_{\widetilde{j_{b,1}(\overline{\alpha})}}\to T\left(\mathbb{Z}/p^2\right)_{\widetilde{j_{b,1}(\overline{\alpha})}}$. 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 parametrisation (8.4.1), 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

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

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

$$\tilde{t} := Q^{6}_{1,0}\otimes Q^{3}_{2,0}\otimes Q^{6\cdot6}_{1,1}\otimes Q^{6\cdot3}_{1,2}\otimes Q^{3\cdot6}_{2,1}\otimes Q^{3\cdot3}_{2,2} \text{ in } \mathcal{M}^\times\left(\widetilde{D_1},m\cdot\left(D_0+\eta_*\widetilde{G_t}\right)\right)(\mathbb{Z})$$

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

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

Let $\widetilde{G_{t,2}}$ be the divisor $m\left(D_0+\eta_*\left(\widetilde{G_t}\right)\right)$ representing $(m\cdot\circ\mathrm{tr}_c\circ f)\left(\widetilde{G_t}\right)\in J^0(\mathbb{Z})$. Following formula (4.1) for $i,j\in\{1,2\}$, we define

$$\begin{tikzcd}
P_{i,j} := \displaystyle\bigotimes_{m,l=1}^{2} Q_{l,m}^{e_{i,l}\cdot e_{j,m}} \arrow[d, mapsto] & R_{i,\tilde{t}} := \displaystyle\bigotimes_{l=1}^{2} Q_{l,0}^{e_{i,l}}\otimes\bigotimes_{m,l=1}^{2} Q_{l,m}^{e_{i,l}\cdot e_{0,m}} \arrow[d, mapsto] & S_{\tilde{t},j} := \displaystyle\bigotimes_{m,l=1}^{2} Q_{l,m}^{e_{0,l}\cdot e_{j,m}} \arrow[d, mapsto] \\
\left(\widetilde{G_i},f\left(m\widetilde{G_j}\right)\right), & \left(\widetilde{G_i},\widetilde{G_{t,2}}\right), & \left(\widetilde{G_t},f\left(m\widetilde{G_j}\right)\right).
\end{tikzcd}$$

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

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

Applying Lemma 6.4.8 and the functoriality of the norm, we compute the following:

$$
\begin{aligned}
P_{1,1} &= (1+4p)\cdot s_{0,0}((4,0),(2,0)) \quad \text{in } \mathcal{M}^\times\left(\widetilde{G_1},\widetilde{G_1}\right)(\mathbb{Z}/p^2) = \mathcal{M}^\times\left(D^0_{4,0},E^0_{2,0}\right)(\mathbb{Z}/p^2),\\
P_{1,2} &= (1+4p)\cdot s_{0,0}((4,0),(0,4)) \quad \text{in } \mathcal{M}^\times\left(\widetilde{G_1},\widetilde{G_2}\right)(\mathbb{Z}/p^2) = \mathcal{M}^\times\left(D^0_{4,0},E^0_{0,4}\right)(\mathbb{Z}/p^2),\\
P_{2,1} &= (1+4p)\cdot s_{0,0}((0,3),(2,0)) \quad \text{in } \mathcal{M}^\times\left(\widetilde{G_2},\widetilde{G_1}\right)(\mathbb{Z}/p^2) = \mathcal{M}^\times\left(D^0_{0,3},E^0_{2,0}\right)(\mathbb{Z}/p^2),\\
P_{2,2} &= (-1)\cdot(1+2p)\cdot s_{0,0}((0,3),(0,4)) \quad \text{in } \mathcal{M}^\times\left(\widetilde{G_2},\widetilde{G_2}\right)(\mathbb{Z}/p^2) = \mathcal{M}^\times\left(D^0_{0,3},E^0_{0,4}\right)(\mathbb{Z}/p^2),\\
R_{1,\tilde{t}} &= s_{0,E}((4,0),(0,4)) \quad \text{in } \mathcal{M}^\times\left(\widetilde{G_1},\widetilde{G_{t,2}}\right)(\mathbb{Z}/p^2) = \mathcal{M}^\times\left(D^0_{4,0},E_{0,4}\right)(\mathbb{Z}/p^2),\\
R_{2,\tilde{t}} &= (1+4p)\cdot s_{0,E}((0,3),(0,4)) \quad \text{in } \mathcal{M}^\times\left(\widetilde{G_2},\widetilde{G_{t,2}}\right)(\mathbb{Z}/p^2) = \mathcal{M}^\times\left(D^0_{0,3},E_{0,4}\right)(\mathbb{Z}/p^2),\\
S_{\tilde{t},1} &= s_{D,0}((0,3),(2,0)) \quad \text{in } \mathcal{M}^\times\left(\widetilde{G_t},\widetilde{G_1}\right)(\mathbb{Z}/p^2) = \mathcal{M}^\times\left(D_{0,3},E^0_{2,0}\right)(\mathbb{Z}/p^2),\\
S_{\tilde{t},2} &= (-1)(1+4p)\cdot s_{D,0}((0,3),(0,4)) \quad \text{in } \mathcal{M}^\times\left(\widetilde{G_t},\widetilde{G_2}\right)(\mathbb{Z}/p^2) = \mathcal{M}^\times\left(D_{0,3},E^0_{0,4}\right)(\mathbb{Z}/p^2),\\
\tilde{t} &= (-1)\cdot(1+2p)\cdot s_{D,E}((0,3),(0,4)) \ \text{ in } \mathcal{M}^\times(\widetilde{G_t},\widetilde{G_{t,2}})(\mathbb{Z}/p^2) = \mathcal{M}^\times(D_{0,3},E_{0,4})(\mathbb{Z}/p^2).
\end{aligned}
\tag{8.5.1}
$$

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

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

and indeed,

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

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

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

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

$$\mathcal{M}\left(\widetilde{G_t},\widetilde{G_{t,2}}\right)=\widetilde{G_{t,2}}^{*}\mathcal{O}_{C_{\mathbb{Z}/p^2}}\left(\widetilde{G_t}\right)\to\widetilde{G_{t,2}}^{*}\mathcal{O}_{C_{\mathbb{Z}/p^2}}(D_{0,3})=\mathcal{M}\left(D_{0,3},\widetilde{G_{t,2}}\right),\tag{8.5.2}$$

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

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

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

and indeed,

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

Following the recipe in §6.4 that describes map (6.4.4), we consider the 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 neighbourhood of the supports of $\widetilde{G_{t,2}}$ and $E_{0,4}$. Then

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

Hence by Lemma 6.4.8, the canonical isomorphism

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

described in equation (6.4.1) sends

$$\widetilde{G_{t,2}}^{*}l\longmapsto h_2(\operatorname{div}(l))\cdot E_{0,4}^*l=14\cdot E_{0,4}^*l,\tag{8.5.3}$$

where

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

Formulas (8.5.2) and (8.5.3) 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 $\mathcal{M}^{\times}(\mathbb{Z}_p) \to \mathcal{M}\left(\mathbb{Z}/p^2\right)$ and, respectively, $A_{\tilde{t}}, B_{\tilde{t}}, C$ and $D_{\tilde{t}}$ defined in formulas (4.2)–(4.4). Using equations (6.6.14) and (8.5.1) we get the following for n in $\mathbb{Z}^2$:

$$\begin{aligned}
\overline{A_{\tilde{t}}}(n) &= (-1)^{n_2}(1+(4n_2)t)\cdot s_{D,0}((0,3),(2n_1,4n_2)),\\
\overline{B_{\tilde{t}}}(n) &= (1+(4n_2)p)s_{0,E}((4n_1,3n_2),(0,4)),\\
\overline{C}(n) &= (-1)^{n_2^2}\left(1+\left(4n_1^2+(4+4)n_1n_2+2n_2^2\right)p\right)\cdot s_{0,0}((4n_1,3n_2),(2n_1,4n_2)),\\
\overline{D_{\tilde{t}}}(n) &= -\left(1+\left(4n_1^2+3n_1n_2+2n_2^2+3n_2+2\right)p\right)\cdot s_{D,E}((4n_1,3+3n_2),(2n_1,4+4n_2)),\\
\overline{\kappa}(n) &= -\left(1+\left(4n_1^2+3n_1n_2+2n_2^2+2n_2+2\right)p\right)\cdot s_{D,E}((n_1,3+2n_2),(3n_1,4+n_2)).
\end{aligned} \tag{8.5.4}$$

Hence, using bijection (8.4.1),

$$\overline{\kappa_1} = z_1, \qquad \overline{\kappa_2} = 3+2z_2, \qquad \overline{\kappa_3} = 4z_1^2+3z_1z_2+2z_2^2+2z_2+2. \tag{8.5.5}$$

8.6. The rational points with a specific image mod 5

By equation (8.5.4), 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 equation (8.2.3) we see that there is no point $T(\mathbb{Z})$ with reduction $\widetilde{j_{b,0}}(\overline{\alpha}) \in T(\mathbb{F}_p)$. Therefore $C(\mathbb{Z})_{\overline{\alpha}} = U_1(\mathbb{Z})_{\overline{\alpha}}$.

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 §4. The bijection (8.4.1) gives an isomorphism $\mathbb{F}_p \otimes \mathcal{O}(\widetilde{T}_t^p) = \mathbb{F}_p[\lambda_1,\lambda_2,\tau]$, and since the kernel of $\widetilde{j_{b,1}}^* : \mathbb{F}_p \otimes \mathcal{O}(\widetilde{T}_t^p)^{\wedge_p} \to \mathbb{F}_p \otimes \mathcal{O}(\widetilde{U}_u^p)^{\wedge_p}$ is generated by the images of $\overline{f_1}, \overline{f_2}$ of f_1, f_2 in $\mathbb{F}_p \otimes \mathcal{O}(\widetilde{T}_t^p)$, we can suppose that

$$\overline{f_1} = \lambda_2, \qquad \overline{f_2} = \tau - 1.$$

By equation (8.5.5) we have

$$\kappa^*\overline{f_1} = \overline{\kappa_2} = 3+2z_2, \qquad \kappa^*\overline{f_2} = \overline{\kappa_3} - 1 = 4z_1^2+3z_1z_2+2z_2^2+2z_2+1.$$

Let A be $\mathbb{Z}_p\langle z_1,z_2\rangle/(\kappa^*f_1,\kappa^*f_2)$. Then the ring

$$\overline{A} := A/pA = \mathbb{F}_p[z_1,z_2]/\left(\kappa^*\overline{f_1},\kappa^*\overline{f_2}\right) = \mathbb{F}_p[z_1,z_2]/\left(z_2-1, 4z_1^2+3z_1\right) \tag{8.6.1}$$

has dimension 2 over $\mathbb{F}_p$, and hence by Theorem 4.12 $U(\mathbb{Z})_{\overline{\alpha}}$ contains at most two points. Since both

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

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

8.7. 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 the fact 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

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

Applying our method to $\overline{\infty}$, we discover that $U_1(\mathbb{Z})_{\overline{\infty}}$ contains at most two 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 two 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

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

Using the Mordell–Weil sieve [27], we derive a contradiction: for all integers n_1, n_2, the image in $J(\mathbb{F}_7)$ of $39 G_1 + 17 G_2 + 5 n_1 \widetilde{G_1} + 5 n_2 \widetilde{G_2}$ 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 two 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 that 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 the fact 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 six 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,

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

9. Some further remarks

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 [6, 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

$$\begin{aligned}(x_1,y,z_1)+_1(x_2,y,z_2)&=(x_1+x_2,y,z_1+z_2),\\ (x,y_1,z_1)+_2(x,y_2,z_2)&=(x,y_1+y_2,z_1+z_2).\end{aligned}\tag{9.1.1}$$

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

$$Q^u(\mathbb{Z}):=\left\{\begin{pmatrix}1 & x & z\\ 0 & 1_{2g} & y\\ 0 & 0 & 1\end{pmatrix} : x\in\mathrm{M}_{1,2g}(\mathbb{Z}), y\in\mathrm{M}_{2g,1}(\mathbb{Z}), z\in\mathbb{Z}\right\},\tag{9.1.2}$$

also known as a Heisenberg group. Its action on D_τ is given in [6, (4.5.3)].

Now recall the definition of T in diagram (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 $\mathrm{M}_{g,1}(\mathbb{C})$ and 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 [6, §4.7]. Then we have

$$\pi_1(T(\mathbb{C}))=\left\{\begin{pmatrix}1_{\rho-1} & m\cdot f(y) & z\\ 0 & 1_{2g} & y\\ 0 & 0 & 1\end{pmatrix} : y\in\mathrm{M}_{2g,1}(\mathbb{Z}), z\in\mathrm{M}_{\rho-1,1}(\mathbb{Z})\right\},\tag{9.1.3}$$

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

$$\begin{aligned}\widetilde{T(\mathbb{C})}&=\{(m\cdot(c+f(v)),v,w) : v\in\mathrm{M}_{g,1}(\mathbb{C}), w\in\mathrm{M}_{\rho-1,1}(\mathbb{C})\}\\ &\subset\mathrm{M}_{\rho-1,g}(\mathbb{C})\times\mathrm{M}_{1,g}(\mathbb{C})\times\mathrm{M}_{\rho-1,1}(\mathbb{C}),\end{aligned}\tag{9.1.4}$$

with $m\cdot(c+f(v))\in\mathrm{M}_{\rho-1,g}(\mathbb{C})$ with rows the $m\cdot(\widetilde{c_i}+v^t\cdot f_{i,\mathbb{C}})$ and $\widetilde{c_i}$ 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 [6, (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 $\pi_2(J(\mathbb{C}))=0$:

$$\pi_1\left(\mathbb{C}^{\times,\rho-1},1\right)\hookrightarrow\pi_1(T(\mathbb{C}),1)\twoheadrightarrow\pi_1(J(\mathbb{C}),0).\tag{9.1.5}$$

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 know that the ith coordinate of the commutator pairing is given by $mf_i\colon \mathrm{H}_1(J(\mathbb{C}),\mathbb{Z})\to\mathrm{H}_1\left(J^\vee(\mathbb{C}),\mathbb{Z}\right)=\mathrm{H}_1(J(\mathbb{C}),\mathbb{Z})^\vee$. 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:

$$mf_i = c_1(T_i) \text{ in } \mathrm{H}^2(J(\mathbb{C}),\mathbb{Z}). \tag{9.1.6}$$

There is a central extension

$$\mathrm{H}_2(J(\mathbb{C}),\mathbb{Z}) \hookrightarrow E \twoheadrightarrow \pi_1(J(\mathbb{C}),0) \tag{9.1.7}$$

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

$$G := \pi_1(C(\mathbb{C}),b). \tag{9.1.8}$$

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:

$$[G,G]/[G,[G,G]] \hookrightarrow G/[G,[G,G]] \twoheadrightarrow G/[G,G] = G^{\mathrm{ab}} = \pi_1(J(\mathbb{C}),0). \tag{9.1.9}$$

This extension arises from formula (9.1.7) by pushout via a morphism from $\mathrm{H}_2(J(\mathbb{C}),\mathbb{Z})$ to $[G,G]/[G,[G,G]]$:

$$\begin{tikzcd}
\mathrm{H}_2(J(\mathbb{C}),\mathbb{Z}) \arrow[r, hook] \arrow[d] & E \arrow[r, two heads] \arrow[d] & G^{\mathrm{ab}} \arrow[d, equal] \\
{[G,G]/[G,[G,G]]} \arrow[r, hook] & G/[G,[G,G]] \arrow[r, two heads] & G^{\mathrm{ab}}.
\end{tikzcd} \tag{9.1.10}$$

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 diagram (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 diagram (9.1.10) factors through the pushout by the quotient of $\mathrm{H}_2(J(\mathbb{C}),\mathbb{Z})$ by $\mathrm{H}_2(C(\mathbb{C}),\mathbb{Z})$:

$$\begin{tikzcd}
\mathrm{H}_2(J(\mathbb{C}),\mathbb{Z})/\mathrm{H}_2(C(\mathbb{C}),\mathbb{Z}) \arrow[r, hook] \arrow[d, two heads] & E' \arrow[r, two heads] \arrow[d, two heads] & G^{\mathrm{ab}} \arrow[d, equal] \\
{[G,G]/[G,[G,G]]} \arrow[r, hook] & G/[G,[G,G]] \arrow[r, two heads] & G^{\mathrm{ab}}.
\end{tikzcd} \tag{9.1.11}$$

Using again the presentation of G, we can split this morphism of extensions and – using the fact 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 diagram (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 equation (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 four 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 we are dealing with $\mathrm{Hom}(J(\mathbb{C}),J^\vee(\mathbb{C}))^+$), and then $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ acts (because $\mathrm{Hom}(J(\mathbb{C}),J^\vee(\mathbb{C}))^+$ and $\mathrm{Hom}\left(J_{\overline{\mathbb{Q}}},J^\vee_{\overline{\mathbb{Q}}}\right)^+$ are equal) through the Galois group of a finite extension of $\mathbb{Q}$. Take the invariants (because we only use morphisms f_i defined over $\mathbb{Q}$). 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

$$\begin{tikzcd}
\mathrm{H}_2(J(\mathbb{C}),\mathbb{Z}(-1))/\mathrm{H}_2(C(\mathbb{C}),\mathbb{Z}(-1)) \arrow[r, hook] \arrow[d] & G/[G,[G,G]] \arrow[r, two heads] \arrow[d] & G^{\mathrm{ab}} \arrow[d, equal] \\
\left((\mathrm{H}_2(J(\mathbb{C}),\mathbb{Z}(-1))/\mathrm{H}_2(C(\mathbb{C}),\mathbb{Z}(-1)))_{(0,0)}\right)_{\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)} \arrow[r, hook] & \pi_1(T(\mathbb{C}),1) \arrow[r, two heads] & G^{\mathrm{ab}},
\end{tikzcd} \tag{9.1.12}$$

where the subscript $(0,0)$ means the largest quotient of type $(0,0)$, the subscript $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ means coinvariants modulo torsion and 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 $\widetilde{j_b}\colon C(\mathbb{C}) \to T(\mathbb{C})$.

9.2. Finiteness of rational points

In this section we re-prove Faltings' finiteness result [16] in the special case where the base field is $\mathbb{Q}$ and $r < g+\rho-1$. This was already done in [4, 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.

9.2.1. 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 neighbourhood of a in A, and 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; similarly, the formal completion of A at a is denoted by $A^{a,\infty}$, and so on. 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 such 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 first and second coordinates and $+_2$ by addition on the first and third coordinates). 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 $A \times B$:

$$\begin{tikzcd} & E \arrow[d] \\ A^{0,1} \times B^{0,1} \arrow[ur, "\tilde{e}"] \arrow[r] & A \times B, \end{tikzcd}$$

with $\tilde{e}(0,0) = e$ in $E(k)$. Note that

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

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 $A^{0,0} \times B^{0,1}$, 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 $A^{0,0} \times B^{0,1}$. In geometric terms, $\tilde{e}$ (which we assume 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 $B^{0,1}$:

$$\left((T_G(0) \oplus T_A(0)) \otimes_k \mathbb{G}_{\mathrm{a}}^{0,\infty}\right)_{B^{0,1}} \lhook\joinrel\twoheadrightarrow E^{0,\infty}_{B^{0,1}}.$$

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 pullback to $A^{0,\infty}$ of $E \to A$ then gives an isomorphism of formal groups over $A^{0,\infty}$:

$$\begin{tikzcd} G^{0,\infty} \times B^{0,\infty} \times A^{0,\infty} \arrow[r, equal] & \left(G^{0,\infty} \times B^{0,\infty}\right)_{A^{0,\infty}} \arrow[r, hook, two heads] & E^{0,\infty}_{A^{0,\infty}/A^{0,\infty}} \arrow[r, equal] & E^{0,\infty}, \end{tikzcd}$$

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

$$\begin{tikzcd}
 & E_b \arrow[d] \\
A^{a,1}\times\{b\} \arrow[ur, "\tilde{e}_1"] \arrow[r] & A\times\{b\},
\end{tikzcd}$$

with $\tilde{e}_1(a,b) = e$ in $E(k)$. The exponentials for the group laws of E_b and A then give a section

$$\begin{tikzcd}
 & E_b \arrow[d] \\
A^{a,\infty}\times\{b\} \arrow[ur, "\tilde{e}_1^\infty"] \arrow[r] & A\times\{b\},
\end{tikzcd}$$

which 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 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 $(a,0)$, giving 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 $E^{(0,b),\infty} \to E^{e,\infty}$, and hence by composition a second 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 §9.2.3 we will use the fact that these isomorphisms transport all additions that occur in definition (4.4) to additions in $E^{0,\infty}$ and therefore to additions in the trivial formal biextension.

9.2.2. Zariski density of the curve in formally trivial coordinates. Let C be as in the beginning of §2 and 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 equation (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 $\widetilde{C(\mathbb{C})}$ and consequently 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 $\widetilde{j}_b(C_{\mathbb{C}}^{c,\infty})$ vanishes on $T_{\mathbb{C}}^{t,\infty}$. 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.

9.2.3. The p-adic closure in good formal coordinates. We stay in the situation of §2, but we denote $G := \mathbb{G}_{\mathrm{m}}^{\rho-1}$, $A := J$, $B := J^{\vee,0\rho-1}$ 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 §9.2.1 and Lemma 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 §9.2.1 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 §4. As explained at the end of §9.2.1, 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, as in §4, that for $i,j \in \{1,\ldots,r\}$ we have x_i in $A(\mathbb{Z}_p)_{\overline{0}}$, y_j in $B(\mathbb{Z}_p)_{\overline{0}}$, $e_{i,j}$ in $E(\mathbb{Z}_p)_{\overline{0}}$ over (x_i,y_j), 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:

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

Then a straightforward computation shows that the image of $D(n)$ as defined in definition (4.4) is

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

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.

9.2.4. 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 §4.10. By construction, $\kappa\left(\mathbb{Z}_p^r\right)$ 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 $\kappa\left(\mathbb{Z}_p^r\right)$ 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 nonzero 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 therefore zero on a nonempty open smaller disk. Via a ring morphism $\mathbb{Z}_p \to \mathbb{C}$, this contradicts the conclusion of §9.2.2.

9.3. The relation with p-adic heights

We want to compare the approach to quadratic Chabauty in this article to the one in [4] 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 [4]? Before we do this, we note that the Poincaré biextension has played a role in Arakelov theory and the theory of p-adic heights for a long time [23, 25, 32]. Moreover, [8] gives a detailed description of 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 $\mathcal{M}^\times$ on $(J\times J)_{\mathbb{Q}_p}$ via diagram (6.3.3), and we use the description of $\mathcal{M}^\times$ given in equation (6.3.13).

Let $\mathcal{D}$ be the subset $\mathrm{Div}^0\left(C_{\mathbb{Q}_p}\right)\times\mathrm{Div}^0\left(C_{\mathbb{Q}_p}\right)$ made of pairs of divisors (D_1,D_2) having disjoint support. Let $\log\colon \mathbb{Q}_p^\times\to\mathbb{Q}_p$ be a group morphism extending the formal logarithm on $1+p\mathbb{Z}_p$ and let W be an isotropic complement of $\Omega^1_{C_{\mathbb{Q}_p}/\mathbb{Q}_p}\left(C_{\mathbb{Q}_p}\right)$ in $\mathrm{H}^1_{\mathrm{dR}}(C_{\mathbb{Q}_p}/\mathbb{Q}_p)$. With these choices made, Coleman and Gross [11, (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 $\mathrm{Div}\left(C_{\mathbb{Q}_p}\right)$ of the same degree, every E in $\mathrm{Div}^0\left(C_{\mathbb{Q}_p}\right)$ 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

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

be sent to

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

That this depends only on the linear equivalence classes of D_1-D_2 and E follows from formula (6.4.4), plus (see [11, Proposition 5.2]) the facts that h_p is biadditive and symmetric and that, for any nonzero rational function f on $C_{\mathbb{Q}_p}$ and any D in $\mathrm{Div}^0\left(C_{\mathbb{Q}_p}\right)$ 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 [7, 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 $\Omega^1_{C_{\mathbb{Q}_p}/\mathbb{Q}_p}\left(C_{\mathbb{Q}_p}\right)$. 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 5.1.1. We define

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

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 equation (9.1.1). As $p > 2$, Ψ induces a homeomorphism, given by power series, from each residue polydisk to its image. 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 suffices to describe, for each i in $\{1,\dots,\rho-1\}$, $\widetilde{j_{b,i}}\colon C \to T_i$, 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 §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 trivialises $\mathcal{L}$ 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 diag^*D are both equal to the zero divisor on $C_{\mathbb{Z}_p}$, and 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 7.5 and 7.8, there exists a unique $\lambda \in \mathbb{Q}_p^\times$ such that for each $d \in C(\mathbb{Z}_p)_c$,

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

Since x_j is the jth coordinate of $\log_J$ and z is the pullback of ψ, we deduce that

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

and by [4, Proof of Theorem 1.2] and [5, Lemma 5.5], the function $d \mapsto h_p\left(d - b, D|_{\{d\}\times C}\right)$ is a sum of double Coleman integrals.

It should now be easy to exactly interpret the cohomological approach geometrically, 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 $T(\mathbb{Z})$. Computations can be made in the geometric context of this article or, as in [5], in terms of the étale fundamental group of C. The connection between these is then given by p-adic local systems on T.

Acknowledgments This project started with an idea of the first author in December 2017. From then on the authors worked together it. §8 is due entirely to the second author. §9 was written in July and August 2020. We thank Steffen Müller, Netan Dogra, Jennifer Balakrishnan, Kamal Khuri-Makdisi, Jan Vonk, Barry Mazur and Gerd Faltings for discussions and correspondence, Michael Stoll for suggesting the title, Pim Spelier for his master's thesis [32] and Sachi Hashimoto for the cartoon guide [19]. Finally, we thank the referee for their very thorough work and for having us increase the number of propositions and lemmas, so that hopefully this article has become easier to parse and to digest.

References

[1] M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra* (Addison–Wesley Publishing Co., Reading, MA, 1969)

[2] J. Balakrishnan, A. Besser, F. Bianchi and J. S. Müller, 'Explicit quadratic Chabauty over number fields', Preprint, 2019, https://arxiv.org/abs/1910.04653.

[3] J. Balakrishnan, F. Bianchi, V. Cantoral-Farfán, M. Çiperiani and A. Etropolski, Chabauty–Coleman experiments for genus 3 hyperelliptic curves, in *Research Directions in Number Theory*, Association for Women in Mathematics Series, **19**, pp. 67–90 (Springer, New York, US, 2019).

[4] J. Balakrishnan and N. Dogra, Quadratic Chabauty and rational points, I: p-adic heights, *Duke Math. J.* **167**(11) (2018), 1981–2038. With an appendix by J. S. Müller.

[5] J. Balakrishnan, N. Dogra, J. S. Müller, J. Tuitman and J. Vonk, Explicit Chabauty-Kim for the split Cartan modular curve of level 13, *Ann. of Math. (2)* **189**(3) (2019), 885–944.

[6] D. Bertrand and B. Edixhoven, 'Pink's conjecture on unlikely intersections and families of semi-abelian varieties', *J. Éc. polytech. Math.* **7** (2020), 711–742, https://jep.centre-mersenne.org/item/JEP_2020__7__711_0/.

[7] A. Besser, p-adic Arakelov theory, *J. Number Theory* **111**(2) (2005), 318—371.

[8] A. Betts, 'The motivic anabelian geometry of local heights on abelian varieties', Preprint, (2017), https://arxiv.org/abs/1706.04850.

[9] S. Bosch, W. Lütkebohmert and M. Raynaud, *Néron Models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), 21 (Springer-Verlag, Berlin, 1990).

[10] C. Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité (French)*, *C. R. Acad. Sci. Paris* **212** (1941), 882–885.

[11] R. Coleman and G. Gross, p-adic heights on curves: Algebraic number theory, *Adv. Stud. Pure Math.* 17 (1989), 73 –81.

[12] E. Costa, N. Mascot, J. Sijsling and J. Voight, Rigorous computation of the endomorphism ring of a Jacobian, *Math. Comp.* **88**(317) (2019), 1303–1339.

[13] P. Coupek, D. Lilienfeldt, L. Xiao and Z. Yao, *'Geometric quadratic Chabauty over number fields*', Unpublished notes, 2020, http://www.math.mcgill.ca/lilien/Chabauty-Part1.pdf.

[14] N. Dogra, 'Unlikely intersections and the Chabauty-Kim method over number fields', Preprint, 2019, https://arxiv.org/abs/1903.05032.

[15] B. Edixhoven, 'Geometric quadratic Chabauty', *Lectures at the Arizona Winter School*, 2020, http://swc.math.arizona.edu/index.html.

[16] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. Math.* **73**(3) (1983), 349–366.

[17] V. Flynn, A flexible method for applying Chabauty's theorem, *Compos. Math.* **105**(1) (1997), 79–94.

[18] Y. Hasegawa, Table of quotient curves of modular curves $X_0(N)$ with genus 2, *Proc. Japan Acad. Ser. A Math. Sci.* **71**(10) (1995), 235–239.

[19] S. Hashimoto, 'Cartoon guide to finding $\mathbb{Q}$-points with geometric quadratic Chabauty', Unpublished notes, 2020, https://github.com/sachihashimoto/cartoon-guide-gqc.

[20] T. Honda, On the theory of commutative formal groups, *J. Math. Soc. Japan* **22**(2) (1970), 213–246, https://projecteuclid.org/euclid.jmsj/1259942752.

[21] N. Katz and B. Mazur, *Arithmetic Moduli of Elliptic Curves*, Annals of Mathematics Studies, **108** (Princeton University Press, Princeton, NJ, 1985).

[22] Q. Liu, *Algebraic Geometry and Arithmetic Curves*, *Oxford Graduate Texts in Mathematics*, **6** (Oxford University Press, Oxford, UK, 2002).

[23] B. Mazur and J. Tate, Canonical height pairings via biextensions, in *Arithmetic and Geometry, Vol. I*, Progress in Mathematics, 35, pp. 195–237 (Birkhäuser Boston, Boston, MA, 1983).

[24] W. McCallum and B. Poonen, *The method of Chabauty and Coleman*, in *Explicit Methods in Number Theory*, Panoramas et Synthèses, **36**, pp. 99–117 (Société mathématique de France, Paris, 2012).

[25] L. Moret-Bailly, Métriques permises, in *Seminar on Arithmetic Bundles: The Mordell Conjecture (Paris,* 1983/*84)*, Astérisque, 127, pp. 29–87 (Soc. Math. France, Paris, 1985), http://www.numdam.org/article/AST_1985__127__29_0.pdf.

[26] L. Moret-Bailly, Pinceaux de variétés abéliennes, *Astérisque* 129 (1985).

[27] S. Müller, Applying the Mordell-Weil sieve, Appendix to [4].

[28] M. Raynaud, Spécialisation du foncteur de Picard, *Publ. Math. Inst. Hautes Études Sci.* **38** (1970), 27–76.

[29] 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.

[30] P. Spelier, *A Geometric Approach to Linear Chabauty*, Master's thesis , Universiteit Leiden, 2020.

[31] M. Stoll, 'Finite coverings and rational points', Oberwolfach lecture, 2005, http://www.mathe2.uni-bayreuth.de/stoll/workshop2005/oberwolfach2005.pdf.

[32] Y. Zarhin, Neron coupling and quasicharacters, *Izv. Akad. Nauk SSSR Ser. Mat.* **36** (1972), 497–509.