Math. Ann. 320, 339–365 (2001) **Mathematische Annalen**

Digital Object Identifier (DOI) 10.1007/s002080100199

On arithmetic class invariants

A. Agboola · G. Pappas

Received June 12, 2000 / Accepted August 11, 2000 /
Published online February 5, 2001 – © Springer-Verlag 2001

1. Introduction

Let F be a number field with ring of integers O_F, and let S be a finite set of places of F. Assume that S contains the set S_∞ of archimedean places of F, and write S_f for the set of finite places contained in S. Let O_S (or O, when there is no danger of confusion) denote the ring of S_f-integers of F. Write F^c for an algebraic closure of F.

Let Y be any scheme over $\mathrm{Spec}(O)$. Suppose that G is a finite, flat commutative group scheme over Y of exponent N, and let G^D denote the Cartier dual of G. Let $\pi : X \to Y$ be a G-torsor, and write $\pi_0 : G \to Y$ for the trivial G-torsor. Then $\mathcal{O}_X$ is an $\mathcal{O}_G$-comodule, and so it is also an $\mathcal{O}_{G^D}$-module (see [12]). As an $\mathcal{O}_{G^D}$-module, $\mathcal{O}_X$ is locally free of rank one, and it therefore gives a line bundle $\mathcal{M}_\pi$ over G^D. Set $\mathcal{L}_\pi := \mathcal{M}_\pi \otimes \mathcal{M}_{\pi_0}^{-1}$. Then the map

$$\psi : H^1(Y, G) \to \mathrm{Pic}(G^D)\,; \quad [\pi] \mapsto [\mathcal{L}_\pi]$$

is a homomorphism which is often referred to as the 'class invariant homomorphism'.

Suppose now that $Y = \mathrm{Spec}(O)$, and set $G = \mathrm{Spec}(\mathfrak{B})$, $G^D = \mathrm{Spec}(\mathfrak{A})$, and $X = \mathrm{Spec}(\mathfrak{C})$. Then the algebra $\mathfrak{C}$ is a twisted form of $\mathfrak{B}$, and the homomorphism ψ measures the Galois module structure of this twisted form (see [8]). The class invariant homomorphism was first introduced by W. Waterhouse (see [33], but also [15], exposé VII) and was later further developed in the context of Galois module theory by M. J. Taylor (see [31], [32]). Taylor originally considered group schemes given by torsion points on abelian varieties with complex multiplication;

A. Agboola
Department of Mathematics, Harvard University, Cambridge, MA 02138, USA
Permanent Address: Department of Mathematics, University of California, Santa Barbara, CA 93106, USA (e-mail: agboola@math.ucsb.edu)

G. Pappas
Department of Mathematics, Michigan State University, East Lansing, MI 48824, USA
(e-mail: pappas@math.msu.edu)

the corresponding torsors are obtained by dividing points in the Mordell-Weil groups of these abelian varieties. In [30], it was shown that, for elliptic curves with complex multiplication, the class invariant homomorphism vanishes on the classes of torsors obtained by dividing torsion points of order coprime to 6. This implies the existence of Galois generators for certain rings of integers of abelian extensions of imaginary quadratic fields. This vanishing result was extended to all elliptic curves in [3] and [22]. The class invariant homomorphism for torsors that are obtained by dividing points on abelian varieties has subsequently been studied in greater generality (see for example [2], [5], [23]).

The main goal of this paper is to introduce and study an arithmetic (i.e. 'Arakelov') refinement of the class invariant homomorphism and to study its values on torsors obtained by dividing points on abelian varieties. Assume as above that we have $Y = \mathrm{Spec}(O)$. We shall show that the line bundle $\mathcal{L}_\pi$ associated to the torsor π carries canonical metrics at all of the places in S; in particular it carries canonical hermitian metrics at all archimedean places in S. As a result of this, we shall see that the homomorphism $\psi : H^1(\mathrm{Spec}(O), G) \to \mathrm{Pic}(G^D)$ lifts to a homomorphism

$$\hat{\psi} : H^1(\mathrm{Spec}(O), G) \to \widehat{\mathrm{Pic}}(G^D),$$

where $\widehat{\mathrm{Pic}}(G^D)$ is the Picard group of isomorphism classes of line bundles on G^D endowed with metrics at all places in S. In particular, if $S = S_\infty$, then $\widehat{\mathrm{Pic}}(G^D)$ is just the Arakelov Picard group of the one-dimensional scheme G^D.

Now let $\widetilde{G^D}$ denote the normalisation of G^D. By composing ψ and $\hat{\psi}$ with the natural pullback maps $\mathrm{Pic}(G^D) \to \mathrm{Pic}(\widetilde{G^D})$ and $\widehat{\mathrm{Pic}}(G^D) \to \widehat{\mathrm{Pic}}(\widetilde{G^D})$, we obtain homomorphisms

$$\varphi : H^1(\mathrm{Spec}(O), G) \to \mathrm{Pic}(\widetilde{G^D}) \quad \text{and} \quad \hat{\varphi} : H^1(\mathrm{Spec}(O), G) \to \widehat{\mathrm{Pic}}(\widetilde{G^D}).$$

We show that if the generic fibre of G^D is a constant group scheme (i.e. G^D is 'generically constant'), then the kernel of $\hat{\varphi}$ is very small (see Theorem 4.1).

In the remainder of the paper, we apply our results to study torsors that are obtained by dividing points on abelian varieties. Let E be an abelian scheme of dimension d over O, and write E^D for its dual. For each integer N, let $[N] : E \to E$ denote the multiplication-by-N map on E, and write $E[N]$ for the O-group scheme of N-torsion on E. The Cartier dual of $E[N]$ may be identified with the O-group scheme $E^D[N]$ of N-torsion on E^D. We write $\widetilde{E^D[N]}$ for the normalisation of $E^D[N]$.

Suppose that $P : \mathrm{Spec}(O) \to E$ is an O-valued point of E. Then we may form the following fibre product:

$$\begin{tikzcd}
{[N]^{-1}(P) := \mathrm{Spec}(O) \times_{E,[N]} E} \arrow[r] \arrow[d] & E \arrow[d, "{[N]}"] \\
\mathrm{Spec}(O) \arrow[r, "P"] & E.
\end{tikzcd}$$

Since $[N] : E \to E$ is an $E[N]$-torsor, $[N]^{-1}(P)$ is also an $E[N]$-torsor and it is determined up to isomorphism by the image of P modulo $[N]\cdot E(O)$. In fact, $[N]^{-1}(P)$ is just the $E[N]$-torsor given by the image of P under the natural injection

$$\frac{E(O)}{[N]\cdot E(O)} \hookrightarrow H^1(\mathrm{Spec}(O), E[N])$$

afforded by Kummer theory on E. Let $\mathcal{L}_{[N]^{-1}(P)}$ denote the line bundle on $E^D[N]$ that is associated to $[N]^{-1}(P)$. By our earlier results, $\mathcal{L}_{[N]^{-1}(P)}$ carries a canonical metric at all places in S. Let $\overline{\mathcal{L}}_{[N]^{-1}(P)}$ denote the corresponding metrised line bundle. Then since $E(O) \simeq E(F)$, we obtain a map

$$\hat{\psi}_N : \frac{E(F)}{[N]\cdot E(F)} \to \widehat{\mathrm{Pic}}(E^D[N]) ; \quad [P] \mapsto [\overline{\mathcal{L}}_{[N]^{-1}(P)}]$$

which is a group homomorphism. By composing $\hat{\psi}_N$ with the natural pullback homomorphism $\widehat{\mathrm{Pic}}(E^D[N]) \to \widehat{\mathrm{Pic}}(\widetilde{E^D[N]})$, we obtain a homomorphism

$$\hat{\varphi}_N : \frac{E(F)}{[N]\cdot E(F)} \to \widehat{\mathrm{Pic}}(\widetilde{E^D[N]}).$$

The class $\hat{\psi}(P)$ may be described in terms of the restriction of metrised line bundles on E^D to subgroup schemes of torsion points. Let $\mathcal{L}(P)$ denote the rigidified line bundle on E^D that corresponds to the point P via the duality between E and E^D. Then, at each place in S, $\mathcal{L}(P)$ carries a natural 'Néron metric' which arises via a canonical splitting of the extension of E^D by $\mathbf{G}_m$ which corresponds to P (see [17], [19], [20]). Write $\overline{\mathcal{L}}(P)$ for the line bundle $\mathcal{L}(P)$ endowed with these metrics. We show the following result.

Theorem 1.1. *With the above notation, we have* $\hat{\psi}_N(P) = (\overline{\mathcal{L}}(P) \mid_{E^D[N]})$ *in* $\widehat{Pic}(E^D[N])$.

In order to describe our main result on the arithmetic class invariants for abelian varieties, we have to introduce some further notation. Let l be a prime number. Then, for each positive integer n, the inclusion map $E^D[l^{n-1}] \to E^D[l^n]$ induces pullback homomorphisms $\widehat{\mathrm{Pic}}(E^D[l^n]) \to \widehat{\mathrm{Pic}}(E^D[l^{n-1}])$ and $\widehat{\mathrm{Pic}}(\widetilde{E^D[l^n]}) \to \widehat{\mathrm{Pic}}(\widetilde{E^D[l^{n-1}]})$. These homomorphisms are compatible with the corresponding maps $\hat{\psi}$ and $\hat{\varphi}$. Hence, we may pass to inverse limits to obtain homomorphisms

$$\hat{\Psi}_l := \varprojlim \hat{\psi}_{l^n} : E(F)\otimes_{\mathbf{Z}} \mathbf{Z}_l \to \varprojlim \widehat{\mathrm{Pic}}(E^D[l^n])$$

and

$$\hat{\Phi}_l := \varprojlim \hat{\varphi}_{l^n} : E(F)\otimes_{\mathbf{Z}} \mathbf{Z}_l \to \varprojlim \widehat{\mathrm{Pic}}(\widetilde{E^D[l^n]}).$$

Let $\mathrm{disc}(F/\mathbf{Q})$ denote the discriminant of $F/\mathbf{Q}$. The following result shows that, for almost all primes l, the class invariants $\hat{\varphi}_{l^n}(P)$ (and therefore also $\hat{\psi}_{l^n}(P)$) determine P when P is not a torsion point of order coprime to l.

Theorem 1.2. *Assume that none of the places of F that lie above l are contained in S. Suppose also that l does not divide $6 \cdot \mathrm{disc}(F/\mathbf{Q})$. Then $\hat{\Phi}_l$ is injective.*

The main ingredients of the proof of this theorem are results of Serre and Bogomolov concerning the l-adic representation attached to E (see [7], [25], [26], [27]), and a result of Fontaine which essentially gives an integral comparison theorem between the crystalline and étale cohomology of the l-divisible group scheme of E (see [14]).

We remark that Theorem 1.2 is currently the only known general injectivity result about class invariants that applies to all abelian varieties defined over number fields. For example, apart from certain cases involving elliptic curves, it is not known whether the invariants $\psi_{l^n}(P)$ (as n varies) determine P if P is a point of infinite order (see the remarks at the end of Sect. 5 of this paper).

In the final section of the paper we show that a natural pairing $<, >_{\mathrm{arith}}$ constructed using the arithmetic class invariant homomorphism on Mordell-Weil groups coincides with a certain height pairing constructed by Mazur and Tate (see [19]). This enables us to give a new interpretation of the Mazur-Tate circle and ideal class pairings in terms of Galois module structure invariants attached to torsors of finite group schemes.

Acknowledgements. We are very grateful to D. Bertrand, Ph. Cassou-Nogués, A. J. de Jong, B. Erez, M. Larsen, K. Ribet and M. J. Taylor for helpful conversations. The first author was partially supported by NSF grant no. DMS-9700937. He would like to thank the Université de Bordeaux I and Harvard University for their hospitality while part of this work was carried out. The second author was partially supported by NSF grant no. DMS-9970378 and by a Sloan Research Fellowship.

Notation. If K is any field, then K^c denotes an algebraic closure of K.

If K is a number field, and v is any place of K, then we write K_v for the local completion of K at v and $O_{K,v}$ (or O_v when there is no danger of confusion) for the ring of integers of K_v. For any O_K-module M, we set $M_v := M \otimes_{O_K} O_{K,v}$.

If v is a non-archimedean place of K and ϖ_v denotes a uniformising parameter of $O_{K,v}$, then we suppose that v is normalised so that $v(\varpi_v) = 1$. If q_v is the cardinality of the residue field of K_v, then for each $\alpha \in K_v$ we set $|\alpha|_v = q_v^{-v(\alpha)}$.

2. Torsors and canonical metrics

Let $\pi : X \to \mathrm{Spec}(O)$ be a G-torsor, and let $\mathcal{L}_\pi$ denote its associated G^D-line bundle. In this section, we shall explain how to endow $\mathcal{L}_\pi$ with canonical metrics at all places contained in S. (In fact, the construction will show that $\mathcal{L}_\pi$ carries a canonical metric at all places of F.) This will then enable us to construct the homomorphism $\hat{\psi}$ and the pairing $<, >_{\mathrm{arith}}$.

For each place $v \in S$, we fix an algebraic closure F_v^c of the field F_v and we let $\sigma_v : F \hookrightarrow F_v^c$ denote the corresponding embedding. We also write $| \cdot |_v$ for the unique extension to F_v^c of the v-adic absolute value $| \cdot |_v$ on F_v.

Suppose that V is any scheme over $\mathrm{Spec}(O)$. A metrised line bundle $\overline{\mathcal{L}}$ on V is a pair $(\overline{\mathcal{L}}, || \cdot ||)$ which consists of a line bundle $\mathcal{L}$ on V together with a family $|| \cdot || = \{|| \cdot ||_v\}_{v \in S}$ of metrics on the line bundles $L \otimes_{F,\sigma_v} F_v^c$. (Here L denotes the restriction of $\mathcal{L}$ to the generic fibre of V.) We require that each metric $|| \cdot ||_v$ take values in $\mathbf{R}_{\geq 0}$ and satisfy

$$||a \cdot x||_v = |a|_v \cdot ||x||_v$$

for all $a \in F_v^c$ and $x \in L \otimes_{F,\sigma_v} F_v^c$. We also require that each $|| \cdot ||_v$ is invariant under the action of $\mathrm{Gal}(F_v^c/F_v)$.

The set of isomorphism classes of metrised line bundles on V forms a group (with the group operation being given by tensor product) which we denote by $\widehat{\mathrm{Pic}}(V)$. The identity element of this group is the isomorphism class of the structure sheaf $\mathcal{O}_V$ of V endowed with the trivial metric $| \cdot |_v$ at all places v in S.

We next recall (see [33], [15], exposé VII, or [23]) that there is a canonical isomorphism

$$H^1(\mathrm{Spec}(O), G) \simeq \mathrm{Ext}^1(G^D, \mathbf{G}_m). \tag{2.1}$$

In particular one can associate a canonical central extension

$$1 \to \mathbf{G}_m \to G(\pi) \to G^D \to 1 \tag{2.2}$$

to the torsor π which is such that the corresponding line bundle over G^D is equal to $\mathcal{L}_\pi$. (This construction is explained in detail in [33].) Let L_π denote the restriction of $\mathcal{L}_\pi$ to the generic fibre of G^D.

Now suppose that v is a place in S, and consider the extension

$$1 \to \mathbf{G}_m(F_v^c) \to G(\pi)(F_v^c) \to G^D(F_v^c) \to 1$$

over F_v^c. Since $G(\pi)$ is the complement of the zero section in $\mathcal{L}_\pi$, it follows that each metric on the fibres of $G(\pi)(F_v^c)$ above $G^D(F_v^c)$ uniquely determines a metric on the line bundle $L_\pi \otimes_{F,\sigma_v} F_v^c$. In order to specify a canonical metric on $G(\pi)(F_v^c)$, we appeal to the following result.

Proposition 2.1. *Let K be any locally compact field. Suppose that H_1 is a commutative, locally compact group over K, and let H_2 be a closed subgroup of H_1 which is such that H_1/H_2 is compact. Then any continuous homomorphism $\lambda : H_2(K) \to \mathbf{R}$ has a unique extension to a continuous homomorphism $\tilde{\lambda} : H_1(K) \to \mathbf{R}$.*

Proof. A proof of this result is given in [17], Chapter 11, Lemma 6.1. □

Proposition 2.1 implies that, for each finite extension K of F_v, there is a unique continuous homomorphism $v_\pi^K : G(\pi)(K) \to \mathbf{R}$ which is such that $v_\pi^K(z) = \log |z|_v$ for all $z \in K^* \subset G(\pi)(K)$. If $F_v \subseteq K \subseteq L$ with $[L : F_v] < \infty$, then the uniqueness assertion of Proposition 2.1 implies that $v_\pi^L|_{G(\pi)(K)} = v_\pi^K$. Hence, by passing to the direct limit over all finite extensions of F_v, we see that there is a unique homomorphism

$$v_\pi : G(\pi)(F_v^c) \to \mathbf{R}$$

which is such that $v_\pi(z) = \log |z|_v$ for all $z \in (F_v^c)^* \subset G(\pi)(F_v^c)$. We define

$$|| \cdot ||_v : G(\pi)(F_v^c) \to \mathbf{R}_{>0} \tag{2.3}$$

by setting $||x||_v = \exp(v_\pi(x))$ for all $x \in G(\pi)(F_v^c)$. Then, if $z \in F_v^c$, we have that $||z.x||_v = |z|_v ||x||_v$, and so it follows that $|| \cdot ||_v$ defines a metric on each fibre of $G(\pi)(F_v^c)$ lying above $G^D(F_v^c)$. It is easy to see that $|| \cdot ||_v$ is invariant under the action of $\mathrm{Gal}(F_v^c/F_v)$. We use the same symbol $|| \cdot ||_v$ for the induced metric on the line bundle $L_\pi \otimes_{F,\sigma_v} F_v^c$. The metrics $\{|| \cdot ||_v\}_{v \in S}$ are the canonical metrics associated to $\mathcal{L}_\pi$, and we write $\overline{\mathcal{L}}_\pi$ for the corresponding metrised line bundle on G^D.

Now suppose that $\pi' : X' \to \mathrm{Spec}(O)$ is another G-torsor, and write π'' for the compositum of π and π'. The product $G(\pi) \cdot G(\pi')$ of the extensions $G(\pi)$ and $G(\pi')$ is given by the following pullback diagram:

$$\begin{tikzcd}
G(\pi) \cdot G(\pi') \arrow[r] \arrow[d] & G(\pi) \overset{\mathbf{G}_m}{\times} G(\pi') \arrow[d] \\
G^D \arrow[r, "\Delta"] & G^D \times G^D,
\end{tikzcd}$$

where Δ denotes the diagonal map. It follows from the construction of the extension (2.2) (see [33]) that there are canonical isomorphisms

$$G(\pi'') \simeq G(\pi) \cdot G(\pi') \quad \text{and} \quad \mathcal{L}_{\pi''} \simeq \mathcal{L}_\pi \otimes \mathcal{L}_{\pi'}. \tag{2.4}$$

The uniqueness assertion of Proposition 2.1 implies that for each $v \in S$, the homomorphism $v_{\pi''} : G(\pi'')(F_v^c) \to \mathbf{R}$ is induced by the homomorphism $v_\pi \otimes v_{\pi'} : G(\pi)(F_v^c) \times G(\pi')(F_v^c) \to \mathbf{R}$ which is defined by $(v_\pi \otimes v_{\pi'})(x, x') = v_\pi(x) + v_{\pi'}(x')$ for $x \in G(\pi)(F_v^c)$ and $x' \in G(\pi')(F_v^c)$. This in turn implies that (2.4) induces an isometry

$$\overline{\mathcal{L}}_{\pi''} \simeq \overline{\mathcal{L}}_\pi \otimes \overline{\mathcal{L}}_{\pi'}$$

of metrised line bundles on G^D. We therefore obtain the following result.

Theorem 2.2. *With the above notation, the map*

$$\hat{\psi} : H^1(Spec(O), G) \to \widehat{Pic}(G^D)\, ; \quad [\pi] \mapsto [\overline{\mathcal{L}}_\pi]$$

is a group homomorphism which lifts the homomorphism ψ. □

Remark 2.3. An alternative (and somewhat more explicit) description of the canonical metrics $\{|| \cdot ||_v\}_{v \in S}$ on $\mathcal{L}_\pi$ may be given as follows. Recall that $\pi_0 : G \to \mathrm{Spec}(O)$ denotes the trivial G-torsor over O, and that N is the exponent of G. We observe that there are canonical isomorphisms

$$G(\pi)^N \simeq G(\pi^N) \simeq G(\pi_0) \simeq G^D \times \mathbf{G}_m$$

of extensions. It follows via functoriality that these isomorphisms induce a canonical isometry

$$\xi_\pi : \overline{\mathcal{L}}_\pi^{\otimes N} \xrightarrow{\sim} \overline{\mathcal{O}}_{G^D} \tag{2.5}$$

of metrised line bundles on G^D. Hence, if $v \in S$ and s is a section of $L_\pi \otimes_{F, \sigma_v} F_v^c$, then

$$||s||_v = |\xi_\pi(s^{\otimes N})|_v^{1/N}$$

We therefore see that the metric $|| \cdot ||_v$ is the pullback via ξ_π of the Nth root of the trivial metric on $\mathcal{O}_{G^D}$. □

Suppose that G^D is generically constant, and recall that $\widetilde{G^D}$ denotes the normalisation of G^D. Then it follows that

$$\mathcal{O}_{\widetilde{G^D}} = \mathrm{Map}(G^D(F), O), \tag{2.6}$$

and so we have

$$\widehat{\mathrm{Pic}}(\widetilde{G^D}) \simeq \mathrm{Map}(G^D(F), \widehat{\mathrm{Pic}}(O)),$$
$$\mathrm{Pic}(\widetilde{G^D}) \simeq \mathrm{Map}(G^D(F), \mathrm{Pic}(O)).$$

We define

$$< , >_{\mathrm{arith}}: H^1(\mathrm{Spec}(O), G) \times G^D(F) \to \widehat{\mathrm{Pic}}(O) \tag{2.7}$$

to be the pairing which is induced by the homomorphism

$$\hat{\varphi} : H^1(\mathrm{Spec}(O), G) \to \widehat{\mathrm{Pic}}(\widetilde{G^D}) \simeq \mathrm{Map}(G^D(F), \widehat{\mathrm{Pic}}(O)). \tag{2.8}$$

Thus, if $R \in G(F)$, then we extend R to an O-valued point $R : \mathrm{Spec}(O) \to G^D$ of G^D, and we have

$$< [\pi], R >_{\mathrm{arith}} = [R^* \overline{\mathcal{L}}_\pi]. \tag{2.9}$$

We write

$$<\,,\,>_{\mathrm{class}}\colon H^1(\mathrm{Spec}(O), G) \times G^D(F) \to \mathrm{Pic}(O) \tag{2.10}$$

for the pairing that is induced by composing $<\,,\,>_{\mathrm{arith}}$ with the natural map

$$\widehat{\mathrm{Pic}}(\widetilde{G^D}) \to \mathrm{Pic}(\widetilde{G^D}) \tag{2.11}$$

given by forgetting metrics. It follows immediately from the definitions that this is the same as the pairing induced by the homomorphism

$$\varphi : H^1(\mathrm{Spec}(O), G) \to \mathrm{Pic}(\widetilde{G^D}) \simeq \mathrm{Map}(G^D(F), \mathrm{Pic}(O)). \tag{2.12}$$

We refer to $<\,,\,>_{\mathrm{class}}$ as the 'ideal class pairing'.

Let $\mathcal{C}(\widetilde{G^D})$ denote the kernel of the natural map (2.11), and write $\mathcal{C}(O)$ for the subgroup of $\widehat{\mathrm{Pic}}(O)$ which is similarly defined. We refer to $\mathcal{C}(\widetilde{G^D})$ and $\mathcal{C}(O)$ as the 'circle groups' of $\widetilde{G^D}$ and O respectively. Then $\hat{\varphi}$ induces a homomorphism

$$\mathrm{Ker}(\varphi) \to \mathcal{C}(\widetilde{G^D}) \simeq \mathrm{Map}(G^D(F), \mathcal{C}(O)). \tag{2.13}$$

We write

$$<\,,\,>_{\mathrm{circ}}\colon \mathrm{Ker}(\varphi) \times G^D(F) \to \mathcal{C}(O) \tag{2.14}$$

for the pairing induced by (2.13), and we refer to this as the 'circle pairing'.

In Sect. 7 we shall show that the pairings defined above are related to certain pairings defined by Mazur and Tate (see [19]) in the case in which G is a torsion subgroup scheme of an abelian scheme.

Remark 2.4. An explicit description of the groups $\widehat{\mathrm{Pic}}(O)$ and $\mathcal{C}(O)$ may be given as follows.

Let $J(F)$ denote the group of ideles of F, and define

$$J_{/S}(F) := \{\alpha \in J(F) \mid \alpha_v = 1 \text{ for all places } v \text{ of } F \text{ lying above } S\}.$$

Write $\delta_1 : F^* \to J_{/S}(F)$ for the obvious natural map, and define

$$\delta_2 : F^* \to \prod_{v\in S} \mathbf{R}^*_{>0}\,; \quad a \mapsto \prod_{v\in S} |a|_v^{-1}.$$

Let

$$\delta : F^* \to \frac{J_{/S}(F)}{\prod_{v\notin S} O_v^*} \times \prod_{v\in S} \mathbf{R}^*_{>0}$$

be the homomorphism induced by the map $a \mapsto (\delta_1(a), \delta_2(a))$. Then it is not hard to show (cf. [9], Chapter 1, Cor. 5.5, for example) that

$$\widehat{\mathrm{Pic}}(O) \simeq \left(\frac{J_{/S}(F)}{\prod_{v\notin S} O_v^*} \times \prod_{v\in S} \mathbf{R}^*_{>0}\right) \Big/ \delta(F^*) \tag{2.15}$$

and

$$\mathcal{C}(O) \simeq \frac{\prod_{v\in S}\mathbf{R}^*_{>0}}{\delta_2(O^*)}. \tag{2.16}$$

It may also be shown (see e.g. no. 3.5.2 of [19], or [9]) that there is a (non-canonical) isomorphism $\mathcal{C}(O) \simeq \mathbf{R} \times (\mathbf{R}/\mathbf{Z})^{|S|-1}$, i.e. $\mathcal{C}(O)$ is isomorphic to a direct product of a real line and $|S|-1$ circles. This is the motivation for our choice of terminology with regard to the circle group.

3. Kummer theory

Our main aim in this section is to apply Kummer theory in order to study torsors over $\mathrm{Spec}(F)$. Throughout this section, we will assume that our base scheme Y is equal to $\mathrm{Spec}(F)$.

Suppose therefore that G is a group scheme over $\mathrm{Spec}(F)$, and let $\pi : X \to \mathrm{Spec}(F)$ be a G-torsor. Write $G^D = \mathrm{Spec}(A)$, and let $\mathcal{L}_\pi$ denote the line bundle on G^D associated to π. Since $\mathrm{Pic}(G^D) = 0$, we may choose a trivialisation $\phi_\pi : A \to \mathcal{L}_\pi$, and this induces a trivialisation

$$\phi_\pi^N : A \xrightarrow{\sim} \mathcal{L}_\pi^{\otimes N}.$$

Now since $\mathcal{L}_\pi$ is associated to a G^D-torsor, there is a canonical trivialisation

$$\xi_\pi : \mathcal{L}_\pi^{\otimes N} \xrightarrow{\sim} A \tag{3.1}$$

(cf. (2.5)). Then the isomorphism $\xi_\pi \circ \phi_\pi^N : A \xrightarrow{\sim} A$ is multiplication by an element $a_\pi \in A^*$. It is not hard to check that changing ϕ_π or replacing X by an isomorphic G-torsor alters a_π by multiplying it by an element of A^{*N}. Also, if $\pi' : X' \to \mathrm{Spec}(F)$ is another G-torsor, then since there is a canonical isomorphism $\mathcal{L}_{\pi\cdot\pi'} \simeq \mathcal{L}_\pi \otimes \mathcal{L}_{\pi'}$, it follows that we have the equality $\overline{a}_{\pi\cdot\pi'} = \overline{a}_\pi \cdot \overline{a}_{\pi'}$ in $A^*/(A^*)^N$. We thus have the following result.

Proposition 3.1. *The map $\eta_F : H^1(\mathit{Spec}(F), G) \to A^*/(A^*)^N$ given by $[\pi] \to \overline{a}_\pi$ is a homomorphism.* □

Now suppose that G^D is a constant group scheme over $\mathrm{Spec}(F)$. Then

$$A^*/(A^*)^N \simeq \mathrm{Map}(G^D(F), F^*/(F^*)^N).$$

For each element $R : \mathrm{Spec}(F) \to G^D$ in $G^D(F)$, write $\chi_R : G \to \mu_N$ for the corresponding character of G. Then χ_R induces a homomorphism (which we denote by the same symbol)

$$\chi_R : H^1(\mathrm{Spec}(F), G) \to H^1(\mathrm{Spec}(F), \mu_N)\,; \quad [\pi] \to [\pi(\chi_R)]$$

We write

$$\mathrm{ev}_R : A^*/(A^*)^N \simeq \mathrm{Map}(G^D(F), F^*/(F^*)^N) \to F^*/(F^*)^N$$

for the map $a \mapsto a(R)$ given by 'evaluation at R'. The following result shows that the homomorphism η_F may be described in terms of Kummer theory.

Proposition 3.2. *Let the hypotheses and notation be as above. Then the following diagram is commutative:*

$$\begin{tikzcd} H^1(Spec(F), G) \arrow[r, "\chi_R"] \arrow[d, "\eta_F"'] & H^1(Spec(F), \mu_N) \\ A^*/(A^*)^N \arrow[r, "ev_R"] & F^*/(F^*)^N. \arrow[u, "\text{Kummer}"'] \end{tikzcd} \tag{3.2}$$

(Here the right-hand vertical arrow is the natural isomorphism afforded by Kummer theory.)

Proof. Let $\chi_R^D : \mu_N^D = \mathbf{Z}/N\mathbf{Z} \to G^D$ denote the homomorphism induced by χ_R via Cartier duality, and write $\mathbf{1} : \mathrm{Spec}(F) \to \mathbf{Z}/N\mathbf{Z}$ for the F-valued point of $\mathbf{Z}/N\mathbf{Z}$ corresponding to the character of μ_N given by the identity map $\mathrm{Id} : \mu_N \to \mu_N$. Then we have that $R = \chi_R^D \circ \mathbf{1}$. Now the extension of $\mu_N^D = \mathbf{Z}/N\mathbf{Z}$ by $\mathbf{G}_m$ corresponding to the μ_N-torsor $\pi(\chi_R)$ is canonically isomorphic to the pullback via χ_R^D of the extension of G^D by $\mathbf{G}_m$ corresponding to the G-torsor π. Hence if $\mathcal{L}_{\pi(\chi_R)}$ denotes the line bundle on μ_N^D associated to $\pi(\chi_R)$, then there is a natural isomorphism

$$(\chi_R^D)^*\mathcal{L}_\pi \simeq \mathcal{L}_{\pi(\chi_R)}.$$

We therefore deduce that there is a canonical isomorphism $R^*\mathcal{L}_\pi \simeq \mathbf{1}^*\mathcal{L}_{\pi(\chi_R)}$ of line bundles on $\mathrm{Spec}(F)$. Hence it follows from the definitions of a_π and $a_{\pi(\chi_R)}$ that we have the equality $\overline{a}_\pi(R) = \overline{a}_{\pi(\chi_R)}(\mathbf{1})$ in $F^*/(F^*)^N$. Thus, to prove the proposition, it suffices to show that if $\tau : V \to \mathrm{Spec}(F)$ is any μ_N-torsor, then τ is represented in $H^1(\mathrm{Spec}(F), \mu_N) \simeq F^*/(F^*)^N$ by the element $a_\tau(\mathbf{1}) \in F^*$. This follows from the standard proof of the main statement of Kummer theory. □

Corollary 3.3. *Suppose that G^D is a constant group scheme over $Spec(F)$. Then the homomorphism η_F is injective.*

Proof. Since G^D is a direct sum of cyclic constant group schemes, we may assume without loss of generality that $G^D \simeq \mathbf{Z}/N\mathbf{Z}$ and $G \simeq \mu_N$. Suppose that π is a G-torsor which is such that $\eta_F(\pi) = 0$. Then Proposition 3.2 implies that $\chi_R(\pi) = 0$ for all $R \in G^D(F)$. Hence π is a trivial torsor. □

Corollary 3.4. *Suppose that G^D is a constant group scheme over Spec(F). Then the image of η_F is equal to*

$$Hom(G^D(F), F^*/(F^*)^N) \subset Map(G^D(F), F^*/(F^*)^N) \simeq A^*/(A^*)^N.$$

Proof. In order to prove this result, it suffices to consider the case in which $G^D \simeq \mathbf{Z}/N\mathbf{Z}$ and $G \simeq \mu_N$. Suppose that R and R' are elements of $G^D(F)$. Then (using additive notation for the group law in $G^D(F)$)

$$\chi_{R+R'} = \chi_R \cdot \chi_{R'},$$

and this implies that $\eta_F(\pi) \in \mathrm{Hom}(G^D(F), F^*/(F^*)^N)$.

Since

$$\mathrm{Hom}(G^D(F), F^*/(F^*)^N) \simeq F^*/(F^*)^N \simeq H^1(\mathrm{Spec}(F), \mu_N),$$

we see that the image of η_F is equal to $\mathrm{Hom}(G^D(F), F^*/(F^*)^N)$ by applying Proposition 3.2 with any R which is such that χ_R is an isomorphism. □

4. Cyclotomic extensions

In this section we shall apply Proposition 3.2 to give a criterion that will enable us to detect elements lying in the kernel of $\hat{\varphi}$.

Let G be a group scheme over Spec(O) which is such that G^D is generically constant. We write $G_{/F}$ and $G^D_{/F}$ for the generic fibres of G and G^D respectively. Set $G^D = \mathrm{Spec}(\mathfrak{A})$ and $G^D_{/F} = \mathrm{Spec}(A)$. Then

$$A = (\mathfrak{A}) \otimes_O F \simeq \mathrm{Map}(G^D(F), F).$$

If $\widetilde{G^D}$ denotes the normalisation of G^D, then we have $\mathcal{O}_{\widetilde{G^D}} = \mathrm{Map}(G^D(F), O)$.

Let $\pi : X \to \mathrm{Spec}(O)$ be a G-torsor, and let $\pi_F : X_{/F} \to \mathrm{Spec}(F)$ be its generic fibre. We shall view π_F as a $G_{/F}$-torsor. Suppose that $\mu(F)$ is the group of all roots of unity in F, and write $L := F(\mu(F)^{1/N})$ for the field obtained by adjoining all Nth roots of all elements in $\mu(F)$ to F. We have the following result.

Theorem 4.1. *Let the hypotheses and notation be as above, and suppose in addition that $\hat{\varphi}(\pi) = 0$. Then the torsor π_F becomes trivial over the field L.*

Proof. Write $e : \widetilde{G^D} \to G^D$ for the obvious natural map. Since $\hat{\varphi}(\pi) = 0$, we may choose an isometry $\tilde{\phi}_\pi : \overline{\mathcal{O}}_{\widetilde{G^D}} \xrightarrow{\sim} e^*\overline{\mathcal{L}}_\pi$, and this induces an isometry

$$\tilde{\phi}_\pi^N : \overline{\mathcal{O}}_{\widetilde{G^D}} \xrightarrow{\sim} e^*\overline{\mathcal{L}}_\pi^{\otimes N}.$$

Next we note that the canonical isometry (2.5) of metrised line bundles on G^D induces an isometry

$$\tilde{\xi}_\pi : e^*\overline{\mathcal{L}}_\pi^{\otimes N} \xrightarrow{\sim} \overline{\mathcal{O}}_{\widetilde{G^D}}.$$

The composition $\tilde{\xi}_\pi \circ \tilde{\phi}_\pi^N : \overline{\mathcal{O}}_{\widetilde{G^D}} \xrightarrow{\sim} \overline{\mathcal{O}}_{\widetilde{G^D}}$ is multiplication by an element $a_\pi \in \mathcal{O}^*_{\widetilde{G^D}}$. Since this composition is an isometry, it follows that $a_\pi(R) \in O^*$ and $|a_\pi(R)|_v = 1$ for all $R \in G^D(F)$ and all places $v \in S$. As S contains all infinite places of F, this implies that $a_\pi(R)$ is a root of unity for all $R \in G^D(F)$.

Now consider the $G_{/F}$-torsor π_F. It follows from the definition of the map η_F given at the begining of Sect. 3 that we have

$$\eta_F(\pi_F) = \overline{a}_\pi \in A^*/(A^*)^N.$$

Hence Proposition 3.2 implies that for each $R \in G^D(F)$, the element $a_\pi(R) \in F^*$ is a Kummer representative in $H^1(\mathrm{Spec}(F), \mu_N)$ of the torsor $\pi_F(\chi_R)$. Therefore $\pi_F(\chi_R)$ becomes trivial over the field $F(a_\pi(R)^{1/N}) \subseteq L$. We therefore deduce that if

$$\mathrm{Res} : H^1(\mathrm{Spec}(F), G^D_{/F}) \to H^1(\mathrm{Spec}(L), G^D_{/L})$$

denotes the restriction homomorphism on cohomology, then $\eta_L(\mathrm{Res}(\pi_F)) = 0$. Hence Corollary 3.3 implies that $\mathrm{Res}(\pi_F) = 0$, as claimed. □

5. Arithmetic class invariants attached to abelian varieties

In this section we shall discuss arithmetic class invariants arising via the division of points on abelian varieties O.

Let E be an abelian scheme of dimension d over $\mathrm{Spec}(O)$, and write E^D for the dual abelian scheme. Let $\mathcal{P}$ denote the Poincaré line bundle on $E \times_O E^D$. For each O-valued point $P : \mathrm{Spec}(O) \to E$ of E, we set

$$\mathcal{L}(P) := (P \times_O \mathrm{Id})^*(\mathcal{P}).$$

Then $\mathcal{L}(P)$ is a rigidified line bundle on E^D, and it corresponds to the point P under the duality between E and E^D. For each place v in S, we may endow $\mathcal{L}(P) \otimes_{F,\sigma_v} F_v^c$ with a metric in the following way.

Since the $\mathbf{G}_m$-torsor associated to $\mathcal{P}$ supports the structure of a biextension on $E \times_O E^D$, it follows that there exists a commutative extension

$$1 \to \mathbf{G}_m \to \mathcal{G}(P) \to E^D \to 1 \tag{5.1}$$

which is such that the total space $\mathcal{G}(P)$ is equal to the complement of the zero section in $\mathcal{L}(P)$. Then, just as in the case of G-torsors described in Sect. 2, it follows from Proposition 2.1 that there exists a unique homomorphism

$$v_P : \mathcal{G}(P)(F_v^c) \to \mathbf{R}$$

which is such that $v_P(z) = \log|z|_v$ for all $z \in (F_v)^{c*} \subset \mathcal{G}(P)(F_v^c)$. Hence the map

$$||\cdot||_v := \exp \circ v_P : \mathcal{G}(P)(F_v^c) \to \mathbf{R}_{>0}$$

induces a metric $||\cdot||_v$ on $\mathcal{L}(P) \otimes_{F,\sigma_v} F_v^c$, and this metric is invariant under the action of $\mathrm{Gal}(F_v^c/F_v)$. We refer to $||\cdot||_v$ as the Néron metric at v on $\mathcal{L}(P)$. We write $\overline{\mathcal{L}}(P)$ for the metrised line bundle on E^D which is obtained by endowing $\mathcal{L}$ with the Néron metric at all places $v \in S$.

Now let

$$1 \to \mathbf{G}_m \to \mathcal{G}_N(P) \to E^D[N] \to 1$$

denote the extension of $E^D[N]$ by $\mathbf{G}_m$ that is obtained by pulling back (5.1) along the inclusion map $E^D[N] \to E^D$. This corresponds to an $E[N]$-torsor $\pi_N(P) : X_N(P) \to \mathrm{Spec}(O)$ via the isomorphism (2.1). Let $\overline{\mathcal{L}}_{\pi_N(P)}$ be the metrised line bundle on $E^D[N]$ associated to $\pi_N(P)$, as described in Sect. 2. Then it follows from the definitions that there is a natural isometry

$$\overline{\mathcal{L}}_{\pi_N(P)} \simeq \overline{\mathcal{L}}(P)|_{E^D[N]}.$$

Recall from the introduction that there is an $E[N]$-torsor $[N]^{-1}(P)$ which is obtained by dividing the point P by N. We have the following result.

Theorem 5.1. *There is an isometry*

$$\overline{\mathcal{L}}_{[N]^{-1}(P)} \simeq \overline{\mathcal{L}}(P)|_{E^D[N]} \tag{5.2}$$

of metrised line bundles on $E^D[N]$.

Proof. As $\overline{\mathcal{L}}_{[N]^{-1}(P)}$ and $\overline{\mathcal{L}}(P)|_{E^D[N]}$ are the metrised line bundles associated to the $E[N]$-torsors $[N]^{-1}(P)$ and $X_N(P)$ respectively, in order to prove the result it suffices to show that

$$[N]^{-1}(P) \simeq X_N(P). \tag{5.3}$$

Write $[N]^{-1}(P)_{/F}$ (respectively $X_N(P)_{/F}$) for the generic fibre of $[N]^{-1}(P)$ (respectively $X_N(P)$). Since any $E[N]$-torsor over $\mathrm{Spec}(O)$ is determined by its generic fibre, (5.3) will follow if we show that

$$[N]^{-1}(P)_{/F} \simeq X_N(P)_{/F}. \tag{5.4}$$

This isomorphism (5.4) is explained in [1] (see especially (10) in the proof of Theorem 1. See also Proposition 3.1 of [24] for a detailed proof of this isomorphism.) □

Remark 5.2. Note that Theorem 1.1 is an immediate consequence of Theorem 5.1. This stregnthens results of [1] and [22], and it shows that the arithmetic class invariant homomorphism $\hat{\psi}_N$ may be interpreted in terms of restricting the metrised line bundle $\overline{\mathcal{L}}(P)$ on E^D to the torsion subgroup scheme $E^D[N]$. The reader may consult [4] for a further discussion concerning the restriction of metrised line bundles on arithmetic varieties to horizontal subschemes. □

We shall now discuss certain inverse limits. Let l be a prime number. For each positive integer n, let

$$p_n : \widehat{\mathrm{Pic}}(E^D[l^n]) \to \widehat{\mathrm{Pic}}(E^D[l^{n-1}])$$

be the pullback homomorphism induced by the inclusion map $E^D[l^{n-1}] \to E^D[l^n]$. Write

$$\mathrm{red} : \frac{E(F)}{[l^n] \cdot E(F)} \to \frac{E(F)}{[l^{n-1}] \cdot E(F)}$$

for the homomorphism given by reduction modulo l^{n-1}. The following result follows directly from Theorems 5.1 and 1.1.

Proposition 5.3. *The following diagram is commutative:*

$$\begin{tikzcd} E(F)/([l^n] \cdot E(F)) \arrow[r, "\hat{\psi}_{l^n}"] \arrow[d, "\mathrm{red}"'] & \widehat{Pic}(E^D[l^n]) \arrow[d, "p_n"] \\ E(F)/([l^{n-1}] \cdot E(F)) \arrow[r, "\hat{\psi}_{l^{n-1}}"] & \widehat{Pic}(E^D[l^{n-1}]). \end{tikzcd} \qquad (5.5)$$

□

Taking inverse limits using the diagram (5.5) yields a homomorphism

$$\hat{\Psi}_l := \varprojlim \hat{\psi}_{l^n} : E(F) \otimes_{\mathbf{Z}} \mathbf{Z}_l \to \varprojlim \widehat{\mathrm{Pic}}(E^D[l^n])).$$

By composing $\hat{\Psi}_l$ with the natural maps

$$\varprojlim \widehat{\mathrm{Pic}}(E^D[l^n]) \to \varprojlim \mathrm{Pic}(E^D[l^n]),$$

$$\varprojlim \widehat{\mathrm{Pic}}(E^D[l^n]) \to \varprojlim \widehat{\mathrm{Pic}}(\widetilde{E^D[l^n]}),$$

and

$$\varprojlim \widehat{\mathrm{Pic}}(E^D[l^n]) \to \varprojlim \mathrm{Pic}(\widetilde{E^D[l^n]}),$$

respectively, we obtain homomorphisms

$$\Psi_l : E(F) \otimes_{\mathbf{Z}} \mathbf{Z}_l \to \varprojlim \mathrm{Pic}(E^D[l^n]), \qquad (5.6)$$

$$\hat{\Phi}_l : E(F) \otimes_{\mathbf{Z}} \mathbf{Z}_l \to \varprojlim \widehat{\mathrm{Pic}}(\widetilde{E^D[l^n]}), \qquad (5.7)$$

and

$$\Phi_l : E(F) \otimes_{\mathbf{Z}} \mathbf{Z}_l \to \varprojlim \operatorname{Pic}(\widetilde{E^D[l^n]}). \tag{5.8}$$

We shall now make a few remarks concerning these maps.

(1) If E is an elliptic curve, and $l > 3$, then it is shown in [30], [2], and [22] that all l-power torsion points in $E(F)$ lie in the kernel of Ψ_l. If $l \leq 3$, then this is no longer true in general (see [6], [11]).

(2) Suppose that E is an elliptic curve with complex multiplication, and that l is a prime of ordinary reduction. Then it is shown in [5] that (subject to certain technical hypotheses) the map Ψ_l is injective modulo torsion. On the other hand, the kernel of Φ_l is infinite in general (see [1], [5]), and it may be described in terms of the l-adic height pairing on E.

(3) It follows from Theorem 6.4 below that $\hat{\Phi}_l$ and $\hat{\Psi}_l$ are injective modulo torsion for all abelian schemes E and all primes l. It seems reasonable to expect that the same is true for Ψ_l (but not for Φ_l).

6. Proof of Theorem 1.2

In this section, we shall prove Theorem 1.2.

Throughout this section (unless explicitly stated otherwise), we assume that l is a prime number satisfying the hypotheses of Theorem 1.2. We shall write E_{l^n} and $E_{l^n}^D$ for the groups $E[l^n](F^c)$ and $E^D[l^n](F^c)$ respectively.

Fix compatible identifications $E_{l^n} \simeq (\mathbf{Z}/l^n\mathbf{Z})^{2d}$, $n > 0$ which give

$$E_{l^\infty} := \varinjlim{}_n E_{l^n} \simeq (\mathbf{Q}_l/\mathbf{Z}_l)^{2d}, \quad T_l(E) := \varprojlim{}_n E_{l^n} \simeq \mathbf{Z}_l^{2d}.$$

We shall use the l-adic representation

$$\rho : \operatorname{Gal}(F^c/F) \to \operatorname{Aut}_{\mathbf{Z}_l}(T_l(E)) \simeq \operatorname{GL}(2d, \mathbf{Z}_l).$$

The composition $\det \cdot \rho$ is equal to ϵ^d, where

$$\epsilon : \operatorname{Gal}(F^c/F) \to \mathbf{Z}_l^*$$

is the l-adic cyclotomic character. We shall also use the Galois representations

$$\rho_n : \operatorname{Gal}(F^c/F) \to \operatorname{Aut}_{\mathbf{Z}_l}(E_{l^n}) \simeq \operatorname{GL}(2d, \mathbf{Z}/l^n\mathbf{Z}).$$

Let K_n denote the fixed field of $\operatorname{Ker}(\rho_n)$; this is the extension of F that is obtained by adjoining the coordinates of points in E_{l^n} to F. Write $F_n := K_n(\mu_{l^n})$. Then it follows from the existence of the Weil pairing on E that the points of $E_{l^n}^D$ are rational over F_n. We set $K_\infty := \cup_n K_n$ and $F_\infty := \cup_n F_n$.

Our main strategy for proving Theorem 1.2 may be described as follows. Suppose that $P \in E(F) \otimes_{\mathbf{Z}} \mathbf{Z}_l$ lies in the kernel of $\hat{\Phi}_l$. For each integer $n > 0$, choose $P_n \in E(F)$ so that

$$P_n \otimes 1 \equiv P \mod l^n[E(F) \otimes_{\mathbf{Z}} \mathbf{Z}_l]$$

Then Theorem 4.1 implies that for every integer $n > 0$, the extension $L_n(P) := F_n(\frac{1}{l^n}P_n)$ of F_n is obtained by adjoining to F_n an l^nth root of a root of unity in F_n. The field $L_n(P)$ is independent of the choices of P_n and $\frac{1}{l^n}P_n$. Thus, for all $n > 0$, we have

$$F \subseteq F_n \subseteq L_n(P) \subseteq F_{2n}. \tag{6.1}$$

We shall prove the Theorem 1.2 by establishing the following result, which is itself of some independent interest.

Theorem 6.1. *Suppose that $P \in E(F) \otimes_{\mathbf{Z}} \mathbf{Z}_l$. Then, for all sufficiently large n, the extension $L_n(P)/F_n$ is not a cyclotomic extension.*

We shall require the following lemma.

Lemma 6.2. $K_\infty = F_\infty$.

Proof. We first observe that plainly $K_\infty \subset F_\infty$.

Let $\beta : E \to E^D$ be a polarisation of E which is defined over F. The l-primary part of the kernel of β is a finite, flat, commutative group scheme H. Suppose that H is of exponent l^N. Then, for $n >> 0$, β induces an injection $E[l^n]/H \to E^D[l^n]$, and so we may view $E[l^n]/H$ as being a subscheme of $E^D[l^n]$.

The points of the group scheme $E[l^n]/H$ are rational over the field K_n. Since H is of exponent l^N, not all points of $E[l^n]/H$ are killed by l^{n-N-1}, and so it follows that there is some point of $E[l^n]/H$ which is of exact order l^{n-N}.

Now composing the Weil pairing

$$E[l^{n-N}] \times E^D[l^n] \to \mu_{l^{n-N}}$$

with the natural map $E[l^n] \to E[l^n]/H \subset E^D[l^n]$ gives a pairing

$$E[l^{n-N}] \times E[l^n] \to E[l^{n-N}] \times E^D[l^n] \to \mu_{l^{n-N}}.$$

We therefore deduce that for $n >> 0$, we have $\mu_{l^{n-N}} \subset K_n$. This implies that $F_\infty \subset K_\infty$, and so it follows that $F_\infty = K_\infty$ as asserted. □

Let $\mu(F_n)$ denote the group of all roots of unity in F_n, and write $M_n := F_n(\mu(F_n)^{1/l^n})$ for the field obtained by adjoining all l^nth roots of all elements in $\mu(F_n)$ to F_n. Set $M_\infty := \cup_n M_n$. Then, since $\mu_{l^n} \subset F_n$, it follows that $M_\infty = F_\infty$

and so Lemma 6.2 implies that $M_\infty = K_\infty$. Consider the restriction homomorphism

$$\mathrm{Res} : H^1(F, T_l(E)) \to H^1(K_\infty, T_l(E)) = H^1(M_\infty, T_l(E)).$$

The restriction-inflation sequence implies that the kernel of this homomorphism is equal to $H^1(\mathrm{Gal}(K_\infty/F), T_l(E))$. This is a finite group (see [26], Corollary to Theorem 2).

Proposition 6.3. *Let l be any prime, and suppose that $P \in E(F) \otimes_{\mathbf{Z}} \mathbf{Z}_l$ is of infinite order. Then Theorem 6.1 holds for the element P, and so $\hat{\Phi}_l(P) \neq 0$.*

Proof. We shall argue via contradiction. Suppose that Theorem 6.1 does not hold for P, and hence that $\hat{\Phi}_l(P) = 0$. Let $[P] \in H^1(F, T_l(E))$ denote the image of P under the natural injective map

$$E(F) \otimes_{\mathbf{Z}} \mathbf{Z}_l \to H^1(F, T_l(E))$$

arising from Kummer theory on E. For each integer $n > 0$, let $[P_n]$ denote the image of $[P]$ in $H^1(F, E_{l^n})$.

We now observe that $L_n(P)$ is the smallest extension of F_n which trivialises the image of $[P_n]$ in $H^1(F_n, E_{l^n})$. Since, by our initial assumption, $L_n(P) \subseteq F_{2n}$ (see (6.1)), it follows that the image of $[P_n]$ in $H^1(F_\infty, E_{l^n})$ is trivial for all $n > 0$. This in turn implies that $\mathrm{Res}([P]) = 0$, which is a contradiction, since Res has finite kernel.

Thus $L_n(P)/F_n$ is not a cyclotomic extension if n is sufficiently large, and hence $\hat{\Phi}_l(P) \neq 0$. □

The following result is an immediate corollary of the proof of Proposition 6.3.

Theorem 6.4. *The map $\hat{\Phi}_l$ (and therefore also $\hat{\Psi}_l$) is injective modulo torsion for* all *primes l.* □

We now consider the case in which $P \in E(F) \otimes_{\mathbf{Z}} \mathbf{Z}_l$ is a non-trivial torsion point. Since P is torsion, it follows that in fact $P \in E(F)$. It is sufficient to show that if $l \cdot P = 0$, then $\hat{\Phi}_l(P) \neq 0$.

Assume therefore $P \in E(F)$ with $l \cdot P = 0$ and $P \neq 0$. We shall again argue via contradiction. Suppose that $\hat{\Phi}_l(P) = 0$ and hence that Theorem 6.1 does not hold for the point P. Set $F' := F(\mu_{l^\infty})$. Then it follows from (6.1) that for all $n > 0$,

$$L_n(P) \subset M_n \subset F_n F'.$$

Let ρ' and ρ'_n denote the restrictions of ρ and ρ_n respectively to the subgroup $\mathrm{Gal}(F^c/F')$ of $\mathrm{Gal}(F^c/F)$. Write F'_n for the extension of F' which is fixed by $\Gamma'_n := \mathrm{Ker}(\rho'_n)$. Consider the field

$$L'_n(P) := L_n(P) F'_n.$$

Our assumption that Theorem 6.1 does not hold for the point P implies that

$$L_n'(P) = F_n' \tag{6.2}$$

for all $n > 0$. This will lead to the desired contradiction.

We shall use the following facts about the Galois representation ρ (see [7]):

A. Let $\mathfrak{G}$ denote the algebraic group over $\mathbf{Q}_l$ which is given by the Zariski closure of $\mathrm{Im}(\rho)$ in $\mathrm{GL}(2d, \mathbf{Q}_l)$. Then $\mathrm{Im}(\rho)$ is open with respect to the l-adic topology on $\mathfrak{G}(\mathbf{Q}_l)$.

B. The algebraic group $\mathfrak{G}/\mathbf{Q}_l$ contains the diagonal torus of homotheties $\mathbf{G}_m$.

For simplicity of notation, we shall often write T instead of $T_l(E)$ in what follows.

Let $\mathfrak{G}'$ denote the algebraic subgroup of $\mathfrak{G}$ consisting of elements with determinant 1.

Proposition 6.5. *For $n >> 0$, we have*

$$\rho(\Gamma_n') = \rho(Ker(\rho_n')) = Ker(SL(T) \to SL(T/l^nT)) \cap \mathfrak{G}'(\mathbf{Q}_l).$$

Proof. Notice that since $\det(\rho) = \epsilon^d$, it follows that, for all $n > 0$, $\det(\rho)$ is trivial on the subgroup Γ_n' corresponding to F_n'. Hence it is clear that

$$\rho(\Gamma_n') \subseteq \mathrm{Ker}(\mathrm{SL}(T) \to \mathrm{SL}(T/l^nT)) \cap \mathfrak{G}'(\mathbf{Q}_l).$$

By (A) above, $\mathrm{Im}(\rho)$ is open in the l-adic topology of $\mathfrak{G}(\mathbf{Q}_l)$, and therefore $\mathrm{Im}(\rho) \cap \mathfrak{G}'(\mathbf{Q}_l)$ is open in the l-adic topology of $\mathfrak{G}'(\mathbf{Q}_l)$. We have that $\mathrm{Im}(\rho') \subset \mathfrak{G}'(\mathbf{Q}_l)$. We will show that $\mathrm{Im}(\rho')$ is open in the l-adic topology of $\mathfrak{G}'(\mathbf{Q}_l)$.

The subgroup $\mathrm{Im}(\rho')$ of $\mathfrak{G}'(\mathbf{Q}_l)$ is equal to the subgroup of $\mathrm{Im}(\rho) \cap \mathfrak{G}'(\mathbf{Q}_l)$ which consists of images $\rho(\sigma)$ of $\sigma \in \mathrm{Gal}(F^c/F)$ for which $\epsilon(\sigma) = 1$. Since every element of $\mathrm{Im}(\rho) \cap \mathfrak{G}'(\mathbf{Q}_l)$ is the image $\rho(\sigma)$ of some $\sigma \in \mathrm{Gal}(F^c/F)$ for which $\epsilon^d(\sigma) = 1$, it follows that there are a finite number of cosets (parametrised by a subset of the d-th roots of unity in $\mathbf{Z}_l^*$) of $\mathrm{Im}(\rho')$ in $\mathrm{Im}(\rho) \cap \mathfrak{G}'(\mathbf{Q}_l)$. Therefore $\mathrm{Im}(\rho')$ is l-adically open in $\mathrm{Im}(\rho) \cap \mathfrak{G}'(\mathbf{Q}_l)$, and so it is also l-adically open in $\mathfrak{G}'(\mathbf{Q}_l)$. Now since

$$\mathrm{Ker}(\mathrm{SL}(T) \to \mathrm{SL}(T/l^nT)) \cap \mathfrak{G}'(\mathbf{Q}_l)$$

for $n >> 0$ gives a fundamental system of neighbourhoods of the identity in $\mathfrak{G}'(\mathbf{Q}_l)$, we have that

$$\mathrm{Ker}(\mathrm{SL}(T) \to \mathrm{SL}(T/l^nT)) \cap \mathfrak{G}'(\mathbf{Q}_l) = \mathrm{Ker}(\mathrm{SL}(T) \to \mathrm{SL}(T/l^nT)) \cap \mathrm{Im}(\rho')$$

whenever n is sufficiently large.

The result now follows since

$$\mathrm{Ker}(\mathrm{SL}(T) \to \mathrm{SL}(T/l^nT)) \cap \mathrm{Im}(\rho') = \rho(\mathrm{Ker}(\rho'_n)) = \rho(\Gamma'_n).$$

□

We now observe that (6.2) implies that the natural action of the group $\rho(\Gamma'_n)$ on $T/l^{n+1}T$ fixes the element $\frac{1}{l^n}P$. (Note that there is no well-defined choice of $\frac{1}{l^n}P$. However, any two choices differ by an l^n-torsion point, and so, since $\rho(\Gamma'_n)$ fixes all l^n-torsion points, it makes sense to say that $\rho(\Gamma'_n)$ fixes $\frac{1}{l^n}P$.) Hence, Proposition 6.5 implies that for all sufficiently large n, the natural action of the group

$$\mathrm{Ker}(\mathrm{SL}(T) \to \mathrm{SL}(T/l^nT)) \cap \mathfrak{G}'(\mathbf{Q}_l)$$

on $T/l^{n+1}T$ also fixes the element $\frac{1}{l^n}P$.

Let λ be any prime ideal of F which divides lO_F. Let F_λ denote the local completion of F at λ. We write $\mathbf{C}_l$ for the completion of the algebraic closure F_λ^c of F_λ, and we let $\mathfrak{R}$ denote the completion of the ring of integers of F_λ^c. Then $\mathfrak{R}$ is a flat (non-noetherian) $\mathbf{Z}_l$-algebra which is a valuation ring with valuation $v : \mathfrak{R} - \{0\} \to \mathbf{Q}_{\geq 0}$, say. The field $\mathbf{C}_l$ is the fraction field of $\mathfrak{R}$. We set $T_{\mathfrak{R}} := T \otimes_{\mathbf{Z}_l} \mathfrak{R}$ and

$$\Delta_n := \mathrm{Ker}(\mathrm{SL}(T_{\mathfrak{R}}) \to \mathrm{SL}(T_{\mathfrak{R}}/l^nT_{\mathfrak{R}})) \cap \mathfrak{G}'(\mathbf{C}_l).$$

Then Δ_n acts on $T_{\mathfrak{R}}/l^{n+1}T_{\mathfrak{R}} = (T/l^{n+1}T) \otimes_{\mathbf{Z}_l} \mathfrak{R}$.

Proposition 6.6. *Assume that Theorem 6.1 does not hold for the point P, and hence that* (6.2) *is true for all $n > 0$. Then the element*

$$\frac{1}{l^n}P \otimes 1 \in (T/l^{n+1}T) \otimes_{\mathbf{Z}_l} \mathfrak{R}$$

is fixed by Δ_n for all sufficiently large n.

Proof. Let $\mathfrak{g}'$ denote the Lie algebra of $\mathfrak{G}'(\mathbf{Q}_l)$. Then $\mathfrak{g}'$ is a $\mathbf{Q}_l$-vector space which is a $\mathbf{Q}_l$-subspace of $\mathrm{End}_{\mathbf{Q}_l}(T \otimes_{\mathbf{Z}_l} \mathbf{Q}_l)$. Set

$$\gamma' := \mathfrak{g}' \cap \mathrm{End}_{\mathbf{Z}_l}(T).$$

There is an exact sequence

$$0 \to \gamma' \to \mathrm{End}_{\mathbf{Z}_l}(T) \oplus \mathfrak{g}' \to \mathrm{End}_{\mathbf{Q}_l}(T \otimes_{\mathbf{Z}_l} \mathbf{Q}_l) \tag{6.3}$$

of $\mathbf{Z}_l$-modules, and γ' is a $\mathbf{Z}_l$-lattice in $\mathfrak{g}'$. Since $\mathfrak{R}$ is flat over $\mathbf{Z}_l$, and $\mathbf{Q}_l \otimes_{\mathbf{Z}_l} \mathfrak{R} = \mathbf{C}_l$, (6.3) gives an exact sequence

$$0 \to \gamma' \otimes_{\mathbf{Z}_l} \mathfrak{R} \to \mathrm{End}_{\mathfrak{R}}(T_{\mathfrak{R}}) \oplus (\mathfrak{g}' \otimes_{\mathbf{Q}_l} \mathbf{C}_l) \to \mathrm{End}_{\mathbf{C}_l}(T \otimes_{\mathbf{Z}_l} \mathbf{C}_l). \tag{6.4}$$

Hence it follows that

$$(\mathfrak{g}' \otimes_{\mathbf{Q}_l} \mathbf{C}_l) \cap \mathrm{End}_{\mathfrak{R}}(T_{\mathfrak{R}}) = \gamma' \otimes_{\mathbf{Z}_l} \mathfrak{R}.$$

The natural map $\mathrm{End}_{\mathbf{Z}_l}(T) \to \mathrm{End}_{\mathbf{Z}_l}(T/l^n T)$ induces a Lie homomorphism

$$\tau_n : \gamma' \to \mathrm{End}_{\mathbf{Z}_l}(T/l^n T)$$

whose kernel we denote by γ_n'. It follows from Proposition 6.5 together with standard properties of the exponential on l-adic Lie groups (see for example [16] or [18]) that, for all $n >> 0$, the exponential map gives a bijection between γ_n' and the l-adic Lie group $\rho(\Gamma_n')$. We now assume that n is large enough for the exponential map to satisfy this property.

Now consider the homomorphism

$$\tau_n \otimes_{\mathbf{Z}_l} \mathfrak{R} : \gamma' \otimes_{\mathbf{Z}_l} \mathfrak{R} \to \mathrm{End}_{\mathfrak{R}}(T_{\mathfrak{R}}/l^n T_{\mathfrak{R}}).$$

The kernel of $\tau_n \otimes_{\mathbf{Z}_l} \mathfrak{R}$ is equal to $\gamma_n' \otimes_{\mathbf{Z}_l} \mathfrak{R}$. The Lie algebra of $\mathfrak{G}'(\mathbf{C}_l)$ is equal to

$$\mathfrak{g}' \otimes_{\mathbf{Q}_l} \mathbf{C}_l \subset \mathrm{End}_{\mathbf{C}_l}(T_{\mathbf{C}_l}).$$

The exponential is defined on elements of $\mathrm{End}_{\mathfrak{R}}(T_{\mathfrak{R}}) \subset \mathrm{End}_{\mathbf{C}_l}(T_{\mathbf{C}_l})$ which reduce to zero modulo $l\mathfrak{R}$, and so it is defined on $\mathrm{Ker}(\tau_n \otimes_{\mathbf{Z}_l} \mathfrak{R})$. The values of the exponential map on elements of $\mathrm{Ker}(\tau_n \otimes_{\mathbf{Z}_l} \mathfrak{R})$ belong on the one hand to $\mathfrak{G}'(\mathbf{C}_l)$ because

$$\mathrm{Ker}(\tau_n \otimes_{\mathbf{Z}_l} \mathfrak{R}) \subset \mathfrak{g}' \otimes_{\mathbf{Q}_l} \mathbf{C}_l,$$

and on the other hand to $\mathrm{Ker}(\mathrm{SL}(T_{\mathfrak{R}}) \to \mathrm{SL}(T_{\mathfrak{R}}/l^n T_{\mathfrak{R}}))$. Hence we obtain a map

$$\mathrm{Exp} : \mathrm{Ker}(\tau_n \otimes_{\mathbf{Z}_l} \mathfrak{R}) \to \Delta_n.$$

A similar argument shows that the logarithm defines a map in the other direction which is inverse to Exp. We conclude that Exp gives a bijection between

$$\mathrm{Ker}(\tau_n \otimes_{\mathbf{Z}_l} \mathfrak{R}) = \gamma_n' \otimes_{\mathbf{Z}_l} \mathfrak{R}$$

and Δ_n. Now, by our initial assumption, $\rho(\Gamma_n')$ fixes $\frac{1}{l^n}P \in T/l^{n+1}T$ and therefore, since we have chosen n to be large, γ_n' annihilates $\frac{1}{l^n}P$. We conclude that $\gamma_n' \otimes_{\mathbf{Z}_l} \mathfrak{R}$ annihilates $\frac{1}{l^n}P \otimes 1$, and therefore Δ_n fixes $\frac{1}{l^n}P \otimes 1$, as asserted.

This completes the proof of the Proposition. □

We now continue with the proof of Theorem 1.2. Consider the canonical Hodge-Tate decomposition

$$T \otimes_{\mathbf{Z}_l} \mathbf{C}_l := V_{\mathbf{C}_l} = V(0) \oplus V(1),$$

with each $V(i)$ $(i = 0, 1)$ a $\mathbf{C}_l$-subspace of $V_{\mathbf{C}_l}$ of dimension d. By [14] (Proposition 11 on p. 406; see also 5.10 and 5.11), there are $\mathcal{R}$-lattices $\Lambda(i)$ $(i = 0, 1)$ in $V(i)$, and an element $\alpha \in \mathcal{R}$ of valuation $v(\alpha) = (l-1)^{-1}$ such that

$$\alpha(\Lambda(0) \oplus \Lambda(1)) \subset T \otimes_{\mathbf{Z}_l} \mathcal{R} \subset \Lambda(0) \oplus \Lambda(1).$$

(Using the terminology of [14], $\Lambda(0) = t^*_{H'}(O_{\mathbf{C}_l})$ and $\Lambda(1) = t_H(T_l(\Omega))$, where H stands for the l-divisible group of the abelian scheme E over O_{F_λ}. The stated property of α follows from [14], Corollary to Theorem 3 (see 4.10). Note that here we are using our assumption that $F/\mathbf{Q}$ is unramified at l.)

Set

$$\Lambda := \Lambda(0) \oplus \Lambda(1). \tag{6.5}$$

This grading defines a cocharacter

$$\Upsilon : \mathbf{G}_{m/\mathcal{R}} \to \mathrm{GL}(\Lambda)$$

which when basechanged to $\mathbf{C}_l$ produces the Hodge cocharacter

$$\Upsilon_{\mathbf{C}_l} : \mathbf{C}_l^* \to \mathrm{GL}(V_{\mathbf{C}_l}) = \mathrm{GL}(T \otimes_{\mathbf{Z}_l} \mathbf{C}_l).$$

It follows from the canonicity of the Hodge-Tate decomposition and Tannakian equivalence that the image of the Hodge cocharacter is contained in $\mathfrak{G}(\mathbf{C}_l)$ (cf. [27], 1.4). We therefore see that

$$\Upsilon(\mathbf{G}_{m/\mathcal{R}})) = \Upsilon_{\mathbf{C}_l}(\mathcal{R}^*) \subset \mathrm{GL}(\Lambda) \cap \mathfrak{G}(\mathbf{C}_l).$$

On the other hand, (B) above implies that we have $\mathrm{diag}(\mathbf{C}_l^*) \subset \mathfrak{G}(\mathbf{C}_l)$. This implies that

$$\mathrm{diag}(\mathcal{R}^*) \subset \mathrm{GL}(\Lambda) \cap \mathfrak{G}(\mathbf{C}_l).$$

Hence there is a homomorphism

$$\mathcal{R}^* \times \mathcal{R}^* \to \mathrm{GL}(\Lambda) \cap \mathfrak{G}(\mathbf{C}_l)$$

defined by $(r_1, r_2) \mapsto \Upsilon(r_1) \cdot \mathrm{diag}(r_2)$. Since $\det(\Upsilon(r_1) \cdot \mathrm{diag}(r_2)) = r_1^d r_2^{2d}$, it follows that there exists an injective homomorphism

$$\kappa : \mathcal{R}^* \to \mathrm{SL}(\Lambda) \cap \mathfrak{G}'(\mathbf{C}_l)$$

which is defined by $r \mapsto \Upsilon(r)^2 \cdot \mathrm{diag}(r^{-1})$.

Let $\mathcal{R}^*_{l^n\alpha}$ denote the subgroup of $\mathcal{R}^*$ consisting of those elements r which satisfy $r \equiv 1 \mod \alpha l^n \mathcal{R}$.

Lemma 6.7. *We have that*

$$\kappa(\mathfrak{R}^*_{l^n\alpha}) \subset \Delta_n = Ker(SL(T_{\mathfrak{R}}) \to SL(T_{\mathfrak{R}}/l^n T_{\mathfrak{R}})) \cap \mathfrak{G}'(\mathbf{C}_l). \tag{6.6}$$

Proof. Write $r = 1 + \alpha l^n r'$ and $r^{-1} = 1 + \alpha l^n r''$, with $r', r'' \in \mathfrak{R}$. It is easy to see that $v(r') = v(r'')$. Now choose a basis $e_i(0), e_i(1)$ $(i = 1, ..., g)$ of Λ which respects the decomposition (6.5). With respect to this basis, we can write

$$\kappa(r) = I + \alpha l^n M(r), \tag{6.7}$$

where $M(r) = \mathrm{diag}(r'', \dots, r'', r', \dots, r')$ is a diagonal matrix with coefficients in $\mathfrak{R}$. We have that

$$\alpha l^n T_{\mathfrak{R}} \subset \alpha l^n \Lambda = l^n(\alpha\Lambda) \subset l^n T_{\mathfrak{R}}.$$

Therefore $\kappa(r)$ preserves $T_{\mathfrak{R}}$ and is congruent to the identity modulo $l^n T_{\mathfrak{R}}$. This shows that $\kappa(r) \in \Delta_n$, and so (6.6) holds as asserted. □

Proposition 6.8. *Suppose that $r \in \mathfrak{R}^*_{l^n\alpha}$ is such that*

$$\kappa(r)\left(\frac{1}{l^n}P \otimes 1\right) = \frac{1}{l^n}P \otimes 1 \tag{6.8}$$

in $T_{\mathfrak{R}}/l^{n+1}T_{\mathfrak{R}}$. Then

$$r \equiv 1 \mod l^{n+1}\alpha^{-1}\mathfrak{R}. \tag{6.9}$$

Proof. Lift $\frac{1}{l^n}P \in T/l^{n+1}T$ to an element $\tilde{P}_n$ of T. Then (6.7) and (6.8) imply that

$$\alpha l^n M(r)(\tilde{P}_n \otimes 1) \in l^{n+1}T_{\mathfrak{R}},$$

which gives

$$M(r)(\tilde{P}_n \otimes 1) \in l\alpha^{-1}T_{\mathfrak{R}}.$$

Since $P \neq 0$, we have that $\frac{1}{l^n}P \otimes 1$ is an element of an $\mathfrak{R}/l^{n+1}\mathfrak{R}$-basis of $T_{\mathfrak{R}}/l^{n+1}T_{\mathfrak{R}}$, and $\tilde{P}_n \otimes 1$ is an element of an $\mathfrak{R}$-basis of $T_{\mathfrak{R}}$. Hence, since

$$\alpha\Lambda \subset T_{\mathfrak{R}} \subset \Lambda,$$

it follows that $\tilde{P}_n \otimes 1$ is an element of an $\mathfrak{R}$-basis of Λ multiplied by an element $\beta \in \mathfrak{R}$ with $v(\alpha) \geq v(\beta) \geq 0$. Therefore, with respect to the basis $e_i(0)$, $e_i(1)$, we may write

$$\tilde{P}_n \otimes 1 = \beta \cdot (x_1, \dots, x_d, x_{d+1}, \dots, x_{2d}),$$

where at least one of the coordinates x_i is a unit (i.e. satisfies $v(x_i) = 0$). From

$$\operatorname{diag}(r'', \dots, r'', r', \dots, r')(\tilde{P}_n \otimes 1) \in l\alpha^{-1} T_{\mathfrak{R}} \subset l\alpha^{-1}\Lambda,$$

we now obtain that

$$(r''x_1, \dots, r''x_d, r'x_{d+1}, \dots, r'x_{2d}) \in l\alpha^{-1}\beta^{-1}\Lambda \in l\alpha^{-2}\Lambda.$$

As $v(r') = v(r'')$, we can write $r'' = r'u$, where u is a unit in $\mathfrak{R}$. Setting $x_i' = x_i u$ for $i = 1, \dots, d$, we obtain

$$(x_i', \dots, x_d', x_{d+1}, \dots, x_{2d}) \in l\alpha^{-2}r'^{-1}\Lambda.$$

Since at least one of the x_i or x_i' is a unit, we conclude that $v(l\alpha^{-2}r'^{-1}) \leq 0$, and so

$$v(r') = v(r'') \geq v(l\alpha^{-2}).$$

Hence it follows that $r \equiv 1 \mod l^{n+1}\alpha^{-1}\mathfrak{R}$ as claimed. □

Lemma 6.7 and Proposition 6.8 imply that if r is any element of $\mathfrak{R}^*_{l^n\alpha}$ (i.e. $r \equiv 1 \mod l^n\alpha\mathfrak{R}$) which is not congruent to 1 modulo $l^{n+1}\alpha^{-1}\mathfrak{R}$, then $\kappa(r)$ is a non-trivial element of Δ_n which does not fix the element $\frac{1}{l^n}P \otimes 1 \in T_{\mathfrak{R}}/l^{n+1}T_{\mathfrak{R}}$. Since $v(\alpha) = (l-1)^{-1}$ and $l > 3$, such elements r do exist. This contradicts Proposition 6.6. We therefore deduce that in fact Theorem 6.1 holds for the point P. Hence $\hat{\Phi}_l(P) \neq 0$.

This completes the proof of Theorem 1.2.

7. Class invariants and Mazur-Tate pairings

In this section we shall explain the relationship between the pairings constructed at the end of Sect. 2 and a refinement of the canonical height pairing on abelian varieties constructed by Mazur and Tate in [19]. A good reference for background concerning this material is [9] (see also [10]).

We retain the notation established at the begining of Sect. 5. Throughout this section we shall assume that $S = S_\infty$, and so O is the ring of integers of F. If X is any scheme over $\operatorname{Spec}(O)$, then we shall write $X_{/F}$ for the generic fibre of X.

Write $\operatorname{Div}^0(E^D_{/F})$ for the group of divisors on $E^D_{/F}$ that are rational over F and algebraically equivalent to zero. Let $Z_0(E^D_{/F})$ denote the group of zero-cycles on $E^D_{/F}$ of degree zero which are of the form

$$Z = \sum_i n_i(Q_i)$$

with each Q_i rational over F. If $\overline{\mathcal{L}}$ is any metrised line bundle on E^D, then the metrised line bundle $Z^*\overline{\mathcal{L}}$ on $\mathrm{Spec}(O)$ is defined by

$$Z^*\overline{\mathcal{L}} := \bigotimes_i Q_i^*\overline{\mathcal{L}}^{\otimes n_i}.$$

(Here we have identified each point Q_i on $E^D_{/F}$ with its Zariski closure on E^D.)

Suppose that $Z \in Z_0(E^D_{/F})$ and $D_1 \in \mathrm{Div}^0(E^D_{/F})$ have disjoint supports, and let v be any place of F. Then the Néron symbol $< Z, D_1 >_v$ may be described as follows (see [17], Chapter 11, Theorem 6.2). Let $P : \mathrm{Spec}(F) \to E_{/F}$ be the point on $E_{/F}$ corresponding to D_1 under the duality between E and E^D. We may identify P with the corresponding $\mathrm{Spec}(O)$-valued point of E. Choose any rational section

$$s_{D_1} : E^D \to \mathcal{G}(P)$$

of (5.1) such that the generic fibre of the divisor of s_{D_1} is equal to D_1. Then s_{D_1} induces a map (which we denote by the same symbol)

$$s_{D_1} : E^D(F_v^c) \to \mathcal{G}(P)(F_v^c).$$

The Néron symbol $< Z, D_1 >_v$ is then equal to

$$< Z, D_1 >_v = -v_P \circ s_{D_1}(Z), \tag{7.1}$$

where we extend s_{D_1} to $Z_0(E^D_{/F})$ via linearity. It may be shown that this is independent of the choice of s_{D_1}.

If v is a non-archimedean place of F and ϖ_v is a local uniformiser of F at v, then it may be shown that

$$< Z, D_1 >_v = i_v(Z, D_1) \log |\varpi_v|_v, \tag{7.2}$$

where $i_v(Z, D_1)$ denotes the intersection multiplicity of D_1 and Z at v (see [17], Chapter 11, §5).

For each place v of F, write

$$\lambda_v(Z, D_1) = \begin{cases} \varpi_v^{\mathrm{i}_v(Z,D_1)}, & \text{if } v \nmid \infty; \\ \exp(< Z, D_1 >_v), & \text{if } v \mid \infty. \end{cases} \tag{7.3}$$

Then we may view $\prod_v \lambda_v(Z, D_1)$ as being an element of $J_{/S}(F) \times \prod_{v \in S}(F_v^c)^*$. Hence, via the isomorphism (2.15), we obtain an element $[\prod_v \lambda_v(Z, D_1)] \in \widehat{\mathrm{Pic}}(O)$. By using the section s_{D_1} to compute $Z^*\overline{\mathcal{L}}(P)$, we see from (7.2), (7.3) and the definition of the Néron metrics on $\overline{\mathcal{L}}(P)$ (see Sect. 5) that we have

$$[Z^*\overline{\mathcal{L}}(P)] = \left[\prod_v \lambda_v(Z, D_1)\right] \tag{7.4}$$

in $\widehat{\mathrm{Pic}}(O)$.

We shall now recall the definition of the Mazur-Tate pairing

$$b_{\mathrm{MT}} : E(F) \times E^D(F) \to \widehat{\mathrm{Pic}}(O) \tag{7.5}$$

(cf. [9], [10], or [19]).

Suppose that $P \in E(F)$ and $Q \in E^D(F)$. It may be shown that we may choose $D_P \in \mathrm{Div}^0(E^D_{/F})$ and $Z_Q \in Z_0(E^D_{/F})$ satisfying the following properties:

(1) The divisor D_P corresponds to the point P under the duality between E and E^D;

(2) If $Z_Q = \sum_i n_i(Q_i)$, then $\sum_i [n_i]Q_i = Q$;

(3) D_P and Z_Q have disjoint supports.

Then we define

$$b_{\mathrm{MT}}(P, Q) = \left[\prod_v \lambda_v(Z_Q, D_P)\right] \in \widehat{\mathrm{Pic}}(O).$$

It may be shown that $b_{\mathrm{MT}}(P, Q)$ is independent of all choices made in its definition.

It will be helpful to express the definition of the pairing b_{MT} in terms of metrised line bundles as follows. Let $Z_Q = (Q) - (\underline{O})$. We may then choose D_P to satisfy conditions (1) and (3) above. As $\underline{O}^*\overline{\mathcal{L}}(P)$ is the trivial line bundle, it follows from (7.4) that we have

$$b_{\mathrm{MT}}(P, Q) = [Q^*\overline{\mathcal{L}}(P)][\underline{O}^*\overline{\mathcal{L}}(P)]^{-1} = [Q^*\overline{\mathcal{L}}(P)]. \tag{7.6}$$

Now suppose that N is a positive integer, and that $E^D[N]$ is generically constant. Write $E^D_N = E^D[N](F)$. Then we have a pairing

$$<,>_{\mathrm{arith}}: H^1(\mathrm{Spec}(O), E[N]) \times E^D_N \to \widehat{\mathrm{Pic}}(O)$$

as defined in (2.7). The following result shows that the pairing

$$b_{\mathrm{MT}} : E(F) \times E^D_N \to \widehat{\mathrm{Pic}}(O)$$

induced by (7.5) has an interpretation in terms of the Galois module structure of $E[N]$-torsors.

Theorem 7.1. *Suppose that $P \in E(F)$ and $R \in E^D_N$. Then*

$$b_{\mathrm{MT}}(P, R) =< [N]^{-1}(P), R >_{\mathrm{arith}} .$$

Proof. This just follows from unwinding the definitions, using (7.6), Theorem 5.1, and (2.9). We have

$$b_{\mathrm{MT}}(P, R) = [R^*\overline{\mathcal{L}}(P)] = [R^*\overline{\mathcal{L}}_{[N]^{-1}(P)}] =< [N]^{-1}(P), R >_{\mathrm{arith}} .$$

□

Mazur and Tate have used (7.5) to construct two further pairings that are of interest. These may be described as follows.

By composing b_{MT} with the natural surjection $\widehat{\mathrm{Pic}}(O) \to \mathrm{Pic}(O)$, we obtain a pairing

$$b_{\mathrm{class}} : E(F) \times E^D(F) \to \mathrm{Pic}(O). \tag{7.7}$$

The pairing b_{class} is called the Mazur-Tate ideal class pairing. It has been extensively studied by G. Call (see [9], [10]).

To define the second pairing, we set

$$E(F) \times_{\mathrm{circ}} E^D(F) := \{(P, Q) \in E(F) \times E^D(F) \mid b_{\mathrm{class}}(P, Q) = 0\}.$$

Then if $(P, Q) \in E(F) \times_{\mathrm{circ}} E^D(F)$, we have that $b_{\mathrm{MT}}(P, Q) \in \mathcal{C}(O)$. We write

$$b_{\mathrm{circ}} : E(F) \times_{\mathrm{circ}} E^D(F) \to \mathcal{C}(O)$$

for the restriction of b_{MT} to $E(F) \times_{\mathrm{circ}} E^D(F)$, and we refer to b_{circ} as the Mazur-Tate circle pairing.

Set

$$E(F) \times_{\mathrm{circ}} E^D_N := (E(F) \times E^D_N) \cap (E(F) \times_{\mathrm{circ}} E^D(F)).$$

The following result is an immediate corollary of Theorem 7.1. It gives a new interpretation of the Mazur-Tate pairings in terms of the Galois structure of $E[N]$-torsors.

Corollary 7.2. *Suppose that $R \in E^D_N$ and $P \in E(F)$. Then*

$$b_{\mathrm{class}}(P, R) =< [N]^{-1}(P), R >_{\mathrm{class}} .$$

If $\varphi([N]^{-1}(P)) = 0$, then $(P, R) \in E(F) \times_{\mathrm{circ}} E^D_N$ for all $R \in E^D_N$, and we have

$$b_{\mathrm{circ}}(P, R) =< [N]^{-1}(P), R >_{\mathrm{circ}} .$$

□

References

1. A. Agboola, A geometric interpretation of the class invariant homomorphism, Journal des Théorie des Nombres de Bordeaux, **8** (1994), 273–280
2. A. Agboola, Iwasawa theory of elliptic curves and Galois module structure, Duke Math. J., **71**, (1993), 441–462
3. A. Agboola, Torsion points on elliptic curves and Galois module structure, Invent. Math., **123**, (1996), 105–122
4. A. Agboola, G. Pappas, Line bundles, rational points, and ideal classes, preprint
5. A. Agboola, M. J. Taylor, Class invariants of Mordell-Weil groups, Crelle, **447**, (1994), 23–61
6. W. Bley, M. Klebel, An infinite family of elliptic curves and Galois module structure, preprint

7. F. A. Bogomolov, Sur l'algébricité des représentations l-adiques, C. R. Acad. Sci. Paris, **290**, (1980), 701–703
8. N. Byott, M. J. Taylor, Hopf orders and Galois module structure, In: Group rings and class-groups, K. W. Roggenkamp, M. J. Taylor (eds), Birkhäuser, 1992, pp. 153–210
9. G. Call, Local heights on families of abelian varieties, Harvard University Ph.D. Thesis, (1986)
10. G. Call, Variation of local heights on an algebraic family of abelian varieties, In: Théorie des nombres (Quebec, PQ 1987), J.-M. De Koninck, C. Levesque (eds), de Gruyter, (1989), pp. 72–96
11. Ph. Cassou-Noguès, A. Jehanne, Espaces homogènes principaux et points de 2-division de courbes elliptiques, preprint
12. T. Chinburg, B. Erez, G. Pappas, M. J. Taylor, Tame actions for group schemes: integrals and slices, Duke Math. Journal, **82**, (1996), 269–308
13. E. B. Dynkin, Normed Lie algebras and analytic groups (Russian), Uspehi Metm. Nauk (N.S.) **5** (1950) no. 1(35), 135–186. Translation in: AMS Translations, (1953), no. 97
14. J-M. Fontaine, Formes différentielles et modules de Tate des variétés abéliennes sur les corps locaux, Invent. Math. **65**, (1981/82), no. 3, 379–409
15. A. Grothendieck et al., Groupes de monodromie en géometrie algébrique, Lecture Notes in Mathematics, Vol. 288, Springer-Verlag, Berlin-New York, 1970
16. R. Hooke, Linear p-adic groups and their Lie algebras, Ann. of Math. (2) **43**, (1942), 641–655
17. S. Lang, Fundamentals of diophantine geometry, Springer, 1983
18. M. Lazard, Groupes analytiques p-adiques, Publications Mathématiques IHES, **26**, (1965)
19. B. Mazur, J. Tate, Canonical height pairings via biextensions. In: Arithmetic and Geometry vol. 1, M. Artin, J. Tate (eds), Birkhäuser, 1983, pp. 195–237
20. L. Moret-Bailly, Pinceaux de variétés abéliennes Astérisque **129**, (1985)
21. D. Mumford, Abelian varieties, Oxford University Press, 1970
22. G. Pappas, On torsion line bundles and torsion points on abelian varieties, Duke Math. J., **91** (1998), 215–224
23. G. Pappas, Galois modules and the theorem of the cube, Invent. Math., **133** (1998), 193–225
24. K. Ribet, Kummer theory on extensions of abelian varieties by tori, Duke Math. J., **49** (1979), 745–761
25. J-P. Serre, Sur les groupes de congruence des variétés abéliennes I, Izv. Akad. Nauk. SSR, **28** (1964), 3–18 (or Collected Papers, Vol. II, 62)
26. J-P. Serre, Sur les groupes de congruence des variétés abéliennes II, Izv. Akad. Nauk. SSR, **35** (1975), 731–735 (or Collected Papers, Vol. II, 89)
27. J-P. Serre, Groupes algébriques associés aux modules de Hodge-Tate, Journées arithmetiques de Rennes, Astérisque **65**, (1979), 155–188 (or Collected Papers Vol. III, 119)
28. J-P. Serre, Lie algebras and Lie groups, second edition, Lecture Notes in Mathematics 1500, Springer-Verlag, Berlin, 1992
29. J. Silverman, The arithmetic of elliptic curves, Springer, 1986
30. A. Srivastav, M. J. Taylor, Elliptic curves with complex multiplication and Galois module structure, Invent. Math., **99**, (1990), 165–184
31. M. J. Taylor, Mordell-Weil groups and the Galois module structure of rings of integers, Ill. J. Math. **32** (1988), 428–452
32. M. J. Taylor, Relative Galois module structure of rings of integers and elliptic functions II, Ann. Math. (2) **121**, (1985), no. 3, 519–535
33. W. Waterhouse, Principal homogeneous spaces and group scheme extensions, AMS Transactions **153**, (1971), 181-189