CLASS INVARIANTS AND p-ADIC HEIGHTS

A. AGBOOLA

ABSTRACT. Let F be a number field with ring of integers O_F, and let E/O_F be an abelian scheme of arbitrary dimension. In this paper, we study the class invariant homomoprhisms on E with respect to powers of a prime p of ordinary reduction of E. Our main result implies that if the p-adic Birch and Swinnerton-Dyer conjecture holds for E, then the kernels of these homomorphisms are of bounded order. It follows from this that (under the same hypotheses), if $\mathcal{L} \in \mathrm{Pic}^0(E)$ is a (rigidified) line bundle on E, then $\mathcal{L}$ is determined up to torsion by its restriction to the p-divisible group scheme of E/O_F.

CONTENTS

1. INTRODUCTION

Let F be a number field with ring of integers O_F. Suppose that E/O_F is an abelian scheme of dimension d, and that $p > 2$ is a rational prime. In this paper we shall study the Galois structure of torsors that are constructed by dividing points of infinite order on E by powers of p, and, when p is a prime

Date: Preliminary version of December 28, 2014.

1991 *Mathematics Subject Classification.* 11Gxx, 11Rxx.

of ordinary reduction of E, we shall show that this is closely related to the non-degeneracy of the p-adic height pairing on E.

The class invariant homomorphsim may be described as follows. Let Y be any scheme over $\mathrm{Spec}(O_F)$. Suppose that G is a finite, flat, commmutative group scheme over Y, and write G^D for its Cartier dual. Let $\pi : X \to Y$ be a G-torsor, and write $\pi_0 : G \to Y$ for the trivial G-torsor. Then the structure sheaf $\mathcal{O}_X$ of X is an $\mathcal{O}_G$-comodule, and so it is also an $\mathcal{O}_{G^D}$-module (see e.g. [15]). As an $\mathcal{O}_{G^D}$-module, the structure sheaf $\mathcal{O}_X$ is locally free of rank one, and so it gives a line bundle $\mathcal{M}_\pi$ on G^*. Set

$$\mathcal{L}_\pi := \mathcal{M}_\pi \otimes \mathcal{M}_{\pi_0}^{-1}.$$

Then the map

$$\psi : H^1(Y, G) \to \mathrm{Pic}(G^*), \qquad [\pi] \mapsto [\mathcal{L}_\pi]; \tag{1.1}$$

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

The detailed study of this homomorphism (which was first introduced by W. Waterhouse in [29]) first arose in the subject of arithmetic Galois module theory in the following way. If we write $G^D = \mathrm{Spec}(B)$, $G = \mathrm{Spec}(A)$, and $X = \mathrm{Spec}(C)$, then C is a twisted form of B, and the map ψ yields an invariant that measures the Galois module structure of this twisted form. This was first exploited by M. Taylor in [26] where he considered the case in which G is a torsion subgroup scheme of an abelian variety with complex multplication. In this situation, the torsors that one obtains arise via dividing points on these varieties, and they are closely related to rings of integers in abelian extensions of F. In the case of elliptic curves, it was shown that the torsors obtained by dividing torsion points were free over $\mathcal{O}_{G^D}$, thereby yielding an integral version of the Krönecker Júgendtraum. Let us also remark that a

striking feature of the class invariant homomorphism is that it arises in a wide variety of different settings in arithmetic geometry, ranging from Iwasawa theory (see [3], [9])) to the Arakelov theory of arithmetic varieties (see [7], [8])) to the study of equivariant Euler characteristics of structure sheaves of arithmetic surfaces (see [20]).

Suppose now that $Q : \mathrm{Spec}(O_F) \to E$ is an O_F-valued point of E, and consider the following fibre product:

$$\begin{array}{ccc} [p^n]^{-1}(Q) := \mathrm{Spec}(O_F) \times_{E,[p^n]} E & \longrightarrow & E \\ \downarrow & & \downarrow{\scriptstyle [p^n]} \\ \mathrm{Spec}(O_F) & \xrightarrow{Q} & E. \end{array}$$

Then $[p^n] : E \to E$ is an $E[p^n]$-torsor, and so $[p^n]^{-1}(Q)$ is also an $E[p^n]$-torsor which is given by the image of Q under the natural injection

$$\frac{E(O_F)}{[p^n] \cdot E(O_F)} \hookrightarrow H^1(O_F, E[p^n])$$

afforded by Kummer theory on E. Let E^D be the dual abelian scheme of E; then $E^D[p^n]$ may be identified with the Cartier dual of $E[p^n]$. Since $E(O_F) \simeq E(F)$, we obtain a homomorphism

$$\frac{E(F)}{[p^n]E(F)} \hookrightarrow H^1(O_F, E[p^n]) \xrightarrow{\psi_{p^n}} \mathrm{Pic}(E^D[p^n]).$$

Let $\mathcal{L}_{[p^n]^{-1}Q}$ denote the line bundle on $E^D[p^n]$ associated to $[p^n]^{-1}(Q)$ by Waterhouse's construction, and write $\mathcal{L}(Q)$ for the rigidified line bundle on E^D associated to Q via the duality between E and E^D. It is shown in [1] that

$$\mathcal{L}(Q)_{[p^n]^{-1}Q} = \mathcal{L}(Q) \mid_{E^D[p^n]},$$

and so

$$\psi_{p^n}(Q) = (\mathcal{L}(Q) \mid_{E^D[p^n]})$$

in $\mathrm{Pic}(E[p^n])$. In other words, the class $\psi(Q)$ for $Q \in E(F)$ may be described in terms of the restriction of line bundles on E^D to torsion subgroup schemes of E^D.

In order to describe our main result, we must introduce some further notation. We first observe that the inclusion maps $E^D[p^n] \hookrightarrow E^D[p^{n+1}]$ induce pullback maps $\mathrm{Pic}(E^D[p^{n+1}]) \to \mathrm{Pic}(E^D[p^n])$, and that these maps are compatible with the corresponding homomorphisms ψ_{p^n} and $\psi_{p^{n+1}}$. We may therefore pass to inverse limits to obtain a homomorphism

$$\Psi := \varprojlim_n \psi_{p^n} : \varprojlim H^1(O_F, E[p^n]) \to \varprojlim \mathrm{Pic}(E^D[p^n]).$$

If we write T for the p-adic Tate module of E, then we may identify $\varprojlim H^1(O_F, E[p^n])$ with $H^1_f(F, T)$, and so we obtain a homomorphism

$$\Psi : H^1_f(F, T) \to \varprojlim \mathrm{Pic}(E^D[p^n]).$$

Conjecture A. *The homomorphism Ψ is injective modulo torsion.* □

If Conjecture A is true, then it follows that each rigidified line bundle $\mathcal{L}(Q)$ on E^D is determined up to torsion by its restriction to torsion subgroup schemes of E^D (and in fact is determined up to torsion by its restriction to the p-divisible group scheme of E^D). Equivalently, it follows that a point $Q \in E(F)$ is determined modulo torsion by the Galois structure of the torsors obtained by dividing Q by powers of a fixed ordinary prime p. The only currently known results concerning Conjecture A are as follows. Conjecture A is known to be true (subject to certain technical hypotheses) when E/O_F is a CM elliptic curve, and $p > 2$ is a prime of ordinary reduction of E (see [9]). If we consider metrised line bundles on E, then a suitable Arakelov-type analogue of Conjecture A is also known to be true for arbitrary E/O_F (see [7]). We also remark that a geometric analogue of Conjecture A holds in the setting of CM abelian varieties over global function fields (see [2]).

In this paper we shall show that Conjecture A is implied by the p-adic Birch and Swinnerton-Dyer conjecture for E when p is a prime of ordinary reduction for E, thereby giving a affirmative answer to a question first raised by the author in [1] (see [1, Question 2]). Suppose now therefore, that p is ordinary for E. Let T^* denote the p-adic Tate module of E^D, and write

$$\langle\ ,\ \rangle : H^1_f(F,T) \times H^1_f(F,T^*) \to \mathbf{Q}_p \tag{1.2}$$

for the p-adic height pairing constructed by Perrin-Riou in [21]. The p-adic Birch and Swinnerton-Dyer conjecture for E asserts, in part, that the pairing $\langle\ ,\ \rangle$ is non-degenerate modulo torsion. The following result thus implies that if the p-adic Birch and Swinnerton-Dyer conjecture holds for E, then Ψ is injective modulo torsion.

Theorem B. *Suppose that $x \in H^1_f(F,T)$ and that $\Psi(x) = 0$. Then*

$$\langle x, y\rangle = 0$$

for all $y \in H^1_f(F,T^*)$.

Hence, if x is of infinite order and $\langle\ ,\ \rangle$ is non-degenerate, then $\Psi(x) \neq 0$.

The proof of Theorem B involves a careful analysis of the p-adic height pairing $\langle\ ,\ \rangle$ in terms of resolvends.

An outline of the contents of this paper is as follows. In Section 2 we recall a number of facts that we require concerning class invariants and the description of cohomology groups in terms of resolvends. (The reader may find a more complete treatment of much of this material in terms of relative algebraic K-theory in [5].) In Section 3 we recall Perrin-Riou's definition of the p-adic height pairing 1.2. In Section 4, establish the existence of an exact sequence that plays a key role in the proof of Theorem B. Finally, in Section 5, by analysing the p-adic height pairing in terms of resolvends, we prove Theorem B.

Acknowledgements. This paper was written while I was visiting the Université de Bordeaux I as an ALGANT scholar. I am very grateful to the ALGANT consortium for financial support, and to my colleagues in Bordeaux for their wonderful hospitality during my visit.

Notation. Throughout this paper, we assume that p is an odd prime.

For any field L, we write L^c for an algebraic closure of L, and we set $\Omega_L := \mathrm{Gal}(L^c/L)$. If L is either a number field or a local field, then we write O_L for its ring of integers.

If L is a number field and v is a finite place of L, then we write L_v for the local completion of L at v. We fix an algebraic closure L_v^c of L_v and we identify Ω_{L_v} with a subgroup of Ω_L. If P is any O_L-module, then we shall usually write write $P_v := P \otimes_{O_L} O_{L_v}$.

If R and S are rings with $R \subseteq S$, and if A is any R-algebra, then we often write A_S for $A \otimes_R S$.

2. Resolvends and Cohomology Groups

Let R be an integral domain of characteristic zero with field of fractions L. We write L^c for an algebraic closure of L, and R^c for the integral closure of R in L^c. (We allow the possibility that $R = L$, in which case we set $R^c = L^c$.) Let $G = \mathrm{Spec}(B)$ be a finite, flat, commutative group scheme over $\mathrm{Spec}(R)$ of exponent N, and let $G^D = \mathrm{Spec}(A)$ denote its Cartier dual. We set $\Gamma := G(L^c)$ and $\Gamma^* := G^D(L^c)$. In this section we shall explain how the cohomology group $H^1(R, G) := H^1(\mathrm{Spec}(R), G)$ may be described in terms of certain resolvends in A_{L^c}.

Recall that there is a canonical isomorphism

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

(see [29], [16, éxposé VII], or [20]). This implies that given any G-torsor $\pi : X \to \mathrm{Spec}(R)$, we can associate to it a canonical commutative extension

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

The scheme $G(\pi)$ is a $\mathbf{G}_m$-torsor over G^D, and its associated G^D-line bundle is equal to $\mathcal{L}_\pi$. (This construction is explained in detail by Waterhouse in [29].)

Over $\mathrm{Spec}(R^c)$, the G-torsors π_0 and π become isomorphic, i.e. there is an isomorphism

$$X \times_{\mathrm{Spec}(R)} \mathrm{Spec}(R^c) \simeq G \times_{\mathrm{Spec}(R)} \mathrm{Spec}(R^c) \tag{2.2}$$

of schemes with G-action. (This isomorphism is not unique: it is only well-defined up to the action of an element of $G(R^c)$.) Hence, via the functoriality of Waterhouse's construction in [29], the isomorphism (2.2) induces an isomorphism

$$\xi_\pi : \mathcal{L}_\pi \otimes_R R^c \xrightarrow{\sim} A_{R^c}.$$

We shall refer to ξ_π as a *splitting isomorphism* for π. The class invariant map associated to G is

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

Now suppose that $\psi(\pi) = 0$. Then $\mathcal{L}_\pi$ is a free A-module, and so we may choose a trivialisation $s_\pi : A \xrightarrow{\sim} \mathcal{L}_\pi$. Consider the composition

$$A_{R^c} \xrightarrow{s_\pi \otimes_R R^c} \mathcal{L}_\pi \otimes_R R^c \xrightarrow{\xi_\pi} A_{R^c}.$$

This is an isomorphism of A_{R^c}-modules, and so it is just multiplication by an element $\mathbf{r}(s_\pi)$ of $A_{R^c}^\times$. We refer to $\mathbf{r}(s_\pi)$ as a *resolvend* of s_π or as a *resolvend associated to* π. (This terminology is due to L. McCulloh, [18].) Note that $\mathbf{r}(s_\pi)$ depends upon the choice of ξ_π as well as upon s_π. We shall usually not make the dependence of $\mathbf{r}(s_\pi)$ upon ξ_π explicit.

Definition 2.1. Let A and R be as above. Define

$$\mathbf{H}(A) := \left\{ \alpha \in A_{R^c}^{\times} \,\middle|\, \alpha^{\omega}\alpha^{-1} \in \Gamma \text{ for all } \omega \in \Omega_L. \right\};$$
$$H(A) := \frac{\mathbf{H}(A)}{\Gamma \cdot A^{\times}}.$$

□

If $\omega \in \Omega_L$, then $\xi_{\pi}^{\omega} = g_{\omega}\xi_{\pi}$, where $g_{\omega} \in \Gamma$. Since $s_{\pi}^{\omega} = s_{\pi}$, we deduce that $\mathbf{r}(s_{\pi})^{\omega} = g_{\omega}\mathbf{r}(s_{\pi})$, that is, $\mathbf{r}(s_{\pi}) \in \mathbf{H}(A)$. It is easy to see that changing s_{π} alters $\mathbf{r}(s_{\pi})$ via multiplication by an element of $A^{\times}$, while changing ξ_{π} alters $\mathbf{r}(s_{\pi})$ via multiplication by an element of Γ. Hence the image $r(\pi)$ of $\mathbf{r}(s_{\pi})$ in $H(A)$ depends only upon the isomorphism class of the torsor π.

The following result, in the case in which G is a constant group scheme, is equivalent to certain results of L. McCulloh (see [18, Sections 1 and 2]; note, however that McCulloh formulates his results in a rather different way from that described here). McCulloh's methods were generalised by N. Byott to the case of arbitrary G (see [12, Lemma 1.11 and Sections 2 and 3]) using techniques from the theory of Hopf algebras. The proofs of McCulloh and Byott proceed via analysing the Ω_L-cohomology of the exact sequence

$$1 \to \Gamma \to A_{R^c}^{\times} \to A_{R^c}^{\times}/\Gamma \to 1$$

of Ω_L-modules. We give a different approach using a method that involves combining the functoriality of Waterhouse's construction with the theory of descent. I am very grateful to Brian Conrad for a helpful discussion concerning the proof below of the following result.

Theorem 2.2. *Let G be a finite, flat commutative group scheme over $\mathrm{Spec}(R)$, and let $G^D = \mathrm{Spec}(A)$ be the Cartier dual of G. Then the map*

$$\Upsilon_R : \mathrm{Ker}(\psi) \to H(A); \qquad [\pi] \mapsto r(\pi)$$

is an isomorphism.

Proof. We first show that Υ_R is a homomorphism. Suppose that

$$\pi_1 : X_1 \to \mathrm{Spec}(R), \quad \pi_2 : X_2 \to \mathrm{Spec}(R)$$

are G-torsors satisfying $\psi(\pi_1) = \psi(\pi_2) = 0$. For $i = 1, 2$, let

$$\xi_{\pi_i} : \mathcal{L}_{\pi_i} \otimes_R R^c \xrightarrow{\sim} A_{R^c}$$

be a splitting isomorphism for π_i, and suppose that

$$s_{\pi_i} : A \xrightarrow{\sim} \mathcal{L}_{\pi_i}$$

is a trivialisation of $\mathcal{L}_{\pi_i}$. Set $\pi_3 := \pi_1 \cdot \pi_2$. Then it follows via the functoriality of Waterhouse's construction that there is a natural isomorphism

$$\mathcal{L}_{\pi_3} \simeq \mathcal{L}_{\pi_1} \otimes_A \mathcal{L}_{\pi_2}.$$

Thus, if we set

$$s_{\pi_3} := s_{\pi_1} \otimes s_{\pi_2} : A \simeq A \otimes_A A \xrightarrow{\sim} \mathcal{L}_{\pi_1} \otimes_A \mathcal{L}_{\pi_2},$$
$$\xi_{\pi_3} := \xi_{\pi_1} \otimes \xi_{\pi_2} : (\mathcal{L}_{\pi_1} \otimes_A \mathcal{L}_{\pi_2}) \otimes_R R^c \xrightarrow{\sim} A_{R^c} \otimes_{A_{R^c}} A_{R^c} \simeq A_{R^c},$$

then we have that $\mathbf{r}(s_{\pi_3}) = \mathbf{r}(s_{\pi_1})\mathbf{r}(s_{\pi_2})$, where, for each i, the resolvend $\mathbf{r}(s_{\pi_i})$ is defined using the splitting isomorphism ξ_{π_i}. This implies that

$$r(\pi_3) = r(\pi_1)r(\pi_2),$$

as required.

We now show that Υ_R is surjective. For any scheme $S \to \mathrm{Spec}(R)$, write $\mathrm{Map}_S(G^D, \mathbf{G}_m)$ for the set of scheme morphisms

$$G^D \times_{\mathrm{Spec}(R)} S \to \mathbf{G}_m \times_{\mathrm{Spec}(R)} S.$$

Since G^D is affine, the functor $S \mapsto \mathrm{Map}_S(G^D, \mathbf{G}_m)$ is representable by an affine group scheme over R, which we denote by $\mathcal{M}(G^D, \mathbf{G}_m)$. The group

scheme G (which represents the functor $S \mapsto \mathrm{Hom}_S(G^D, \mathbf{G}_m)$) is a closed subgroup scheme of $\mathcal{M}(G^D, \mathbf{G}_m)$.

Suppose that $\alpha \in \mathbf{H}(A)$. Then we may view α as being a $\mathrm{Spec}(R^c)$-valued point of $\mathcal{M}(G^D, \mathbf{G}_m)$. Let

$$G_\alpha := \alpha \cdot [G \times_{\mathrm{Spec}(R)} \mathrm{Spec}(R^c)] \tag{2.3}$$

denote the 'translation-by-α' in $\mathcal{M}(G^D, \mathbf{G}_m) \times_{\mathrm{Spec}(R)} \mathrm{Spec}(R^c)$ of $G \times_{\mathrm{Spec}(R)} \mathrm{Spec}(R^c)$. Then $G \times_{\mathrm{Spec}(R)} \mathrm{Spec}(R^c)$ acts on G_α via translation. Furthermore, translation by α induces an isomorphism

$$\Xi_\alpha : G \times_{\mathrm{Spec}(R)} \mathrm{Spec}(R^c) \xrightarrow{\sim} G_\alpha \tag{2.4}$$

of schemes with $G \times_{\mathrm{Spec}(R)} \mathrm{Spec}(R^c)$ action.

We now claim that G_α descends to $\mathrm{Spec}(R)$, i.e. that there is a scheme $\pi_\alpha : Z_\alpha \to \mathrm{Spec}(R)$ defined over R which is such that $G_\alpha = Z_\alpha \times_{\mathrm{Spec}(R)} \mathrm{Spec}(R^c)$. (We refer the reader to [11, Chapter 6] for a good account of the theory of descent.) Since R is a Dedekind domain, and G_α is flat over $\mathrm{Spec}(R^c)$, it suffices to check that the generic fibre G_{α/L^c} of G_α descends to a scheme over $\mathrm{Spec}(L)$. This in turn follows via Galois descent, and may be seen as follows. We first note that the isomorphism Ξ_α induces a bijection $\Gamma \to G_\alpha(L^c)$ of sets. Define $z_\alpha : \Omega_L \to \Gamma$ by $z(\omega) = \alpha^\omega \alpha^{-1}$; thus z_α is the Γ-valued cocycle of Ω_L associated to α. Then it is easy to check that the action of Ω_L on $G_\alpha(L^c)$ is given by

$$\Xi(g)^\omega = z_\alpha(\omega)\Xi(g^\omega)$$

for all $g \in \Gamma$ and $\omega \in \Omega_L$. This implies that G_{α/L^c} descends to $Z_{\alpha/L}$ over $\mathrm{Spec}(L)$. A similar argument also shows that $\pi_\alpha : Z_\alpha \to \mathrm{Spec}(R)$ is a G-torsor over $\mathrm{Spec}(R)$.

We shall now show that $\psi(\pi_\alpha) = 0$. Let

$$\xi_{\pi_\alpha} : \mathcal{L}_{\pi_\alpha} \otimes_R R^c \xrightarrow{\sim} A_{R^c}$$

denote the splitting isomorphism of π_α induced by Ξ_α. Define an isomorphism

$$\sigma_\alpha : A_{R^c} \xrightarrow{\sim} \mathcal{L}_{\pi_\alpha} \otimes_R R^c$$

by

$$\sigma_\alpha(a) = \xi_{\pi_\alpha}^{-1}(\alpha a) = \alpha \xi_{\pi_\alpha}^{-1}(a)$$

for all $a \in A_{R^c}$. In order to show that $\psi(\pi_\alpha) = 0$, it suffices to show that σ_α descends to an isomorphism $\sigma'_\alpha : A \xrightarrow{\sim} \mathcal{L}_{\pi_\alpha}$ over R. This will in turn follow if we show that

$$\sigma_\alpha^\omega(a) = \sigma_\alpha(a)$$

for all $\omega \in \Omega_L$ and all $\alpha \in A_{R^c}$. To check this last equality, we simply observe that

$$\begin{aligned}
\sigma_\alpha^\omega(a) = \omega[\sigma_\alpha(a^{\omega^{-1}})] &= \omega[\alpha \xi_{\pi_\alpha}^{-1}(a^{\omega^{-1}})] \\
&= \omega[\alpha z_\alpha(\omega^{-1}) \xi_{\pi_\alpha}^{-1}(a)^{\omega^{-1}}] \\
&= \omega[\alpha^{\omega^{-1}} \xi_{\pi_\alpha}^{-1}(a)^{\omega^{-1}}] \\
&= \alpha \xi_{\pi_\alpha}^{-1}(a) \\
&= \sigma_\alpha(a).
\end{aligned}$$

Hence $\psi(\pi_\alpha) = 0$ as asserted.

To complete the proof of the surjectivity of Υ_R, we note that it follows from the definition of σ_α that we have $\mathbf{r}(\sigma'_\alpha) = \alpha$. Hence $r(\pi_\alpha) = [\alpha] \in H(A)$, and so Υ_R is surjective as claimed.

We now show that Υ_R is injective. Suppose that $\alpha, \beta \in \mathbf{H}(A)$ with $[\alpha] = [\beta] \in H(A)$. Then it is easy to check that the isomorphism

$$\Xi_\beta \circ \Xi_\alpha^{-1} : G_\alpha \xrightarrow{\sim} G_\beta$$

induces an isomorphism $G_\alpha(L^c) \xrightarrow{\sim} G_\beta(L^c)$ of Ω_L-modules. This implies that the G-torsors $\pi_\alpha : Z_\alpha \to \mathrm{Spec}(R)$ and $\pi_\beta : Z_\beta \to \mathrm{Spec}(R)$ are isomorphic. This completes the proof of the theorem. □

Remark 2.3. It is not hard to check that (using the notation established in the proof of Theorem 2.2) the map $\Omega_L \to \Gamma$ defined by $\omega \mapsto \mathbf{r}(s_\pi)^\omega \mathbf{r}(s_\pi)^{-1}$ is an Ω_L-cocycle representing the image of π under the natural map $H^1(R, G) \to H^1(L, G)$. □

Recall that N denotes the exponent of G. The following result follows immediately from Theorem 2.2.

Corollary 2.4. *The map* $[\pi] \mapsto \mathbf{r}(s_\pi)^N$ *induces a homomorphism*

$$\eta_R : \mathrm{Ker}(\psi) \to \frac{A^\times}{(A^\times)^N}.$$

□

If R is a local ring, then $\mathrm{Pic}(G^D) = 0$, and so $\mathrm{Ker}(\psi) = H^1(R, G)$. The following result is a direct corollary of Theorem 2.2. It gives a description of the flat cohomology of G over $\mathrm{Spec}(R)$ in terms of resolvends. We remark that a rather different (but related) idelic description of torsors of G over a Dedekind domain has been given by M. Taylor (see [28],[13, Chapter 3, §4]) and by N. Byott (see [12, §3]).

Corollary 2.5. *Suppose that R is a local ring whose field of fractions is of characteristic zero. Then there is an isomorphism*

$$\Upsilon_R : H^1(R, G) \xrightarrow{\sim} H(A)$$

□

Remark 2.6. For each $\gamma^* \in \Gamma^*$, write $L[\gamma^*]$ for the smallest extension of L whose absolute Galois group fixes γ^*. Let $\Gamma^*\backslash\Omega_L$ denote a set of representatives of Ω_L-orbits of Γ^*. Then, via an argument virtually identical to that given in [3, Lemma 3.3], it may be shown that the Wedderburn decomposition of the L-algebra A_L is given by

$$A_L \simeq (L^c\Gamma)^{\Omega_L} \simeq \prod_{\gamma^* \in \Omega_L\backslash\Gamma^*} L[\gamma^*]. \tag{2.5}$$

There is an isomorphism of L-algebras

$$\mathrm{Map}(\Gamma^*, L^c)^{\Omega_L} \simeq \prod_{\gamma^* \in \Omega_L\backslash\Gamma^*} L[\gamma^*]; \quad f \mapsto (f(\gamma^*)_{\gamma^* \in \Omega_L\backslash\Gamma^*}, \tag{2.6}$$

and we may identify A with $\mathrm{Map}(\Gamma^*, L^c)^{\Omega_L}$ via (2.5) and (2.6).

We view each element $\gamma^* \in \Gamma^*$ as being a character of Γ, and we write

$$\mathrm{ev}_{\gamma^*} : A^\times \to L[\gamma^*]^\times \tag{2.7}$$

for the map $a \mapsto a(\gamma^*)$ afforded by (2.5) and (2.6) given by 'evaluation at γ^*'. □

The following result gives a description of the homomorphism η_L (see Corollary 2.4 in terms of Kummer theory.

Proposition 2.7. *Let the hypotheses and notation be as above. Then the following diagram is commutative:*

$$\begin{array}{ccc} H^1(L,\Gamma) & \xrightarrow{\gamma^*} & H^1(L[\gamma^*],\mu_N) \\ {\scriptstyle \eta_L}\downarrow & & \uparrow{\scriptstyle \text{Kummer}} \\ A^\times/A^{\times N} & \xrightarrow{\mathrm{ev}_{\gamma^*}} & L[\gamma^*]^\times/L[\gamma^*]^{\times N}. \end{array} \tag{2.8}$$

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

Proof. This may be shown via an argument virtually identical to that used to prove [7, Proposition 3.2]. □

Proposition 2.8. *Let K be any algebraic extension of L, and write R_K for the integral closure of R in K. Then the following diagram is commutative:*

$$\begin{array}{ccc} \mathrm{Ker}(\psi_R) & \xrightarrow{\Upsilon_R} & H(A) \\ {\scriptstyle \mathrm{Res}}\big\downarrow & & \big\downarrow \\ \mathrm{Ker}(\psi_{R_K}) & \xrightarrow{\Upsilon_{R_K}} & H(A_{R_K}). \end{array} \tag{2.9}$$

Here the left-hand vertical arrow is induced by the restriction map $H^1(R, G) \to H^1(R_K, G)$ on cohomology, and the right-hand vertical arrow is the homomorphism induced by the inclusion map $i : \mathbf{H}(A) \to \mathbf{H}(A_{R_K})$ of resolvends.

Proof. Let $\pi : X \to \mathrm{Spec}(R)$ be any G-torsor with $\pi \in \mathrm{Ker}(\psi_R)$, and let $s : A \xrightarrow{\sim} \mathcal{L}_\pi$ be any trivialisation of $\mathcal{L}_\pi$. Then it follows via a straightforward computation that the Ω_K-cocycle associated to $i(\mathbf{r}(s))$ is equal to the restriction of the Ω_L-cocycle associated to $\mathbf{r}(s)$ (cf. Remark 2.3). Since the natural maps $H^1(R, G) \to H^1(L, G)$ and $H^1(R_K, G) \to H^1(K, G)$ are injective, this implies the desired result. □

Suppose now that K is a finite Galois extension of L with $[K : L] = n$, say. Let $\omega_1, \ldots, \omega_n$ be a transversal of Ω_K in Ω_L. Then we have a norm homomorphism

$$\mathcal{N}_{K/L} : A^\times_{R_K^c} \to A^\times_{R^c}; \qquad a \mapsto \prod_{i=1}^{n} a^{\omega_i}. \tag{2.10}$$

This induces homomorphisms (which we denote by the same symbol)

$$\mathcal{N}_{K/L} : \mathbf{H}(A_{R_K}) \to \mathbf{H}(A), \qquad \mathcal{N}_{K/L} : H(A_{R_K}) \to H(A_R).$$

Proposition 2.9. *The following diagram is commutative:*

$$\begin{array}{ccc} \mathrm{Ker}(\psi_{R_K}) & \xrightarrow{\Upsilon_{R_K}} & H(A_{R_K}) \\ {\scriptstyle \mathrm{Cores}_{K/L}}\downarrow & & \downarrow{\scriptstyle \mathcal{N}_{K/L}} \\ \mathrm{Ker}(\psi_R) & \xrightarrow{\Upsilon_R} & H(A). \end{array} \tag{2.11}$$

where the left-hand vertical arrow is induced by the corestriction map $H^1(R_K, G) \to H^1(R, G)$.

Proof. The proof of this result is very similar to that of Proposition 2.8. Let $\pi : X \to \mathrm{Spec}(R_K)$ be any G-torsor with $\pi \in \mathrm{Ker}(\psi_{R_K})$, and let $s_\pi : A_{R_K} \xrightarrow{\sim} \mathcal{L}_\pi$ be any trivialisation of $\mathcal{L}_\pi$. Then it follows via a straightforward computation that the Ω_L-cocycle associated to $\mathcal{N}_{K/L}(\mathbf{r}(s_\pi))$ is equal to the corestriction of the Ω_K-cocycle associated to $\mathbf{r}(s_\pi)$ (cf. Remark 2.3), and this in turn implies that the given diagram commutes. □

We shall need to apply the results of this section to certain p-divisible group schemes. In order to do this, we shall require some further notation that we now describe.

Let $(G_n)_{n\geq 0}$ be a p-divisible group scheme over R, and let $T := \varprojlim_n \Gamma_n$ (where $\Gamma_n := G_n(F^c)$) be its Tate module. We write

$$G_n^D = \mathrm{Spec}(A(T)_n)$$

for the Cartier dual of G_n, and we set

$$A(T) := \varinjlim A(T)_n, \quad \mathbf{H}(A(T)) := \varinjlim \mathbf{H}(A(T)_n),$$
$$H(A(T)) := \varinjlim H(A(T)_n).$$

We have that

$$H(A(T)) \simeq \frac{\mathbf{H}(A(T))}{T \cdot A(T)^\times}$$

because the natural maps $\Gamma_n \cdot A(T)_n^{\times} \to \Gamma_{n-1} \cdot A(T)_{n-1}^{\times}$ induced by the multiplication by p map $\Gamma_n \to \Gamma_{n-1}$ are surjective.

We write

$$\psi_{T,n} : H^1(R, G_n) \to \mathrm{Cl}(A(T)_n)$$

for the class invariant map associated to G_n, and we set

$$\Psi = \Psi_T := \varprojlim_{T,n} \psi_{T,n} : \varprojlim H^1(R, G_n) \to \varprojlim \mathrm{Cl}(A(T)_n).$$

Proposition 2.10. *(a) There are isomorphisms*

$$\mathrm{Ker}(\Psi_T) \simeq H(A(T)) \simeq \frac{\mathbf{H}(A(T))}{T \cdot A(T)^{\times}}.$$

(b) If R is a local ring, then there are isomorphisms

$$\varprojlim H^1(R, G_n) \simeq H(A(T)) \simeq \frac{\mathbf{H}(A(T))}{T \cdot A(T)^{\times}}.$$

Proof. This follows directly from Theorem 2.2 and Corollary 2.4. □

We recall that if L is a number field or a local field with ring of integers R, then there is a natural identification

$$\varprojlim H^1(R, G_n) \simeq H^1_f(L, T) \tag{2.12}$$

of $\varprojlim H^1(R, G_n)$ with the Bloch-Kato Selmer group $H^1_f(L, T)$ (see [10]).

3. The p-adic height pairing

We now return to the setting described in the Introduction, and we recall the definition of the p-adic height pairing

$$\langle\ ,\ \rangle : H^1_f(F, T) \times H^1_f(F, T^*) \to \mathbf{Q}_p \tag{3.1}$$

given in [21] (see also [22]).

Suppose that $y \in H^1_f(F, T^*)$. Via the isomorphism

$$H^1(F, T^*) \simeq \mathrm{Ext}_{\Omega_F}(\mathbf{Z}_p, T^*),$$

the element y gives rise to an extension

$$0 \to T^* \to T'_y \to \mathbf{Z}_p \to 0. \tag{3.2}$$

Taking $\mathbf{Z}_p(1)$ duals of (3.2) yields an exact sequence

$$1 \to \mathbf{Z}_p(1) \xrightarrow{i} T_y \xrightarrow{j} T \to 0. \tag{3.3}$$

The sequence (3.3) may be described in terms of finite group schemes over O_F as follows. If we identify $H^1_f(F, T^*)$ with $\varprojlim H^1(O_F, E^D[p^n])$ (cf. (2.12)), and write $y = (y_n)_n$, with each $y_n \in H^1(O_F, E^D[p^n])$, then via (2.1), y_n yields an extension

$$1 \to \mathbf{G}_m \to G'_{y_n} \to E[p^n] \to 0 \tag{3.4}$$

of commutative O_F-group schemes. Setting

$$G_{y,n} := G'_{y,n}[p^n]$$

yields an exact sequence

$$1 \to \underline{\mu_{p^n}} \to G_{y,n} \to E[p^n] \to 0. \tag{3.5}$$

of finite, flat, commutative O_F group schemes. Then T_y is the p-adic Tate module of the p-divisible group $(G_{y,n})_n$.

For any finite extension L/F, we may consider the global and local Galois cohomology of (3.3) for each finite place v of L:

$$\begin{array}{ccccccc} H^1(L, \mathbf{Z}_p(1)) & \xrightarrow{i} & H^1(L, T_y) & \xrightarrow{j} & H^1(L, T) & \longrightarrow & H^2(F, \mathbf{Z}_p(1)) \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ H^1(L_v, \mathbf{Z}_p(1)) & \xrightarrow{i_v} & H^1(L_v, T_y) & \xrightarrow{j_v} & H^1(L_v, T) & \longrightarrow & H^2(L_v, \mathbf{Z}_p(1)). \end{array} \tag{3.6}$$

It may be shown via Tate local duality that

$$H^1_f(L_v, T) \subseteq j_v(H^1_f(L_v, T_y))$$

for all finite places v of L.

Global class field theory implies that the natural map

$$H^2(L, \mathbf{Z}_p(1)) \to \bigoplus_v H^2(L_v, \mathbf{Z}_p(1))$$

is injective, and so we deduce from (3.6) that

$$H^1_f(L, T) \subseteq j(H^1_f(L, T_y)).$$

Let F_∞/F denote the cyclotomic $\mathbf{Z}_p$-extension of F. For each finite place v of F, we write

$$H^1_f(F_v, T)_u := \cap_n \mathrm{Cores}_{F_{n,v}/F_v} H^1_f(F_{n,v}, T).$$

Then, as p is a prime of ordinary reduction for E, we have that $|H^1_f(F_v, T) : H^1_f(F_v, T)_u| < \infty$ for each v, and that

$$H^1_f(F, T)^0 := \{x \in H^1_f(F, T) \mid \mathrm{loc}_v(x) \in H^1_f(F_v, T)_u \text{ for all } v.\}$$

is of finite index in $H^1_f(F, T)$. The pairing (3.1) is obtained by first defining a pairing

$$\langle\ ,\ \rangle : H^1_f(F, T^*) \times H^1_f(F, T)^0 \to \mathbf{Z}_p \tag{3.7}$$

and then extending to $H^1_f(F, T^*) \times H^1_f(F, T)$ via linearity.

Suppose that $x \in H^1_f(F, T)^0$, and set $x_v := \mathrm{loc}_v(x)$ for each place v of F. For each integer n, we may write

$$x_v = \mathrm{Cores}_{F_{n,v}/F_v}(x_{n,v})$$

for some $x_{n,v} \in H^1_f(F_{n,v}, T)$. Choose $\tilde{x}_{n,v} \in H^1_f(F_v, T_y)$ such that

$$j_v(\tilde{x}_{n,v}) = x_{n,v},$$

and set $z_{n,v} := \mathrm{Cores}_{F_{n,v}/F_v}(\tilde{x}_{n,v})$. Define

$$t_y(x_v) := \lim_{n \to \infty} z_{n,v}.$$

It follows from the construction that $t_y(x_v)$ is a well-defined element of $H^1_f(F_v, T_y)/i_v[H^1_f(F_v, \mathbf{Z}_p(1))_u]$, where

$$H^1_f(F_v, \mathbf{Z}_p(1))_u := \cap_n \mathrm{Cores}_{F_{n,v}/F_v} H^1_f(F_v, \mathbf{Z}_p(1)).$$

Now let $\tilde{x} \in H^1_f(F, T)$ be such that $j(\tilde{x}) = x$, so $\tilde{x}$ is well-defined in $H^1_f(F, T)/i[H^1_f(F, \mathbf{Z}_p(1))]$. Then, for each v, we have that

$$t_y(x_v) - \mathrm{loc}_v(\tilde{x}) \in i_v[H^1_f(F_v, \mathbf{Z}_p(1)],$$

and so we may view this as being a well-defined element

$$t_y(x_v) - \mathrm{loc}_v(\tilde{x}) \in \frac{H^1_f(F_v, \mathbf{Z}_p(1))}{H^1_f(F_v, \mathbf{Z}_p(1))_u \cdot \mathrm{loc}_v[H^1_f(F, \mathbf{Z}_p(1))]},$$

where here we have identified $H^1_f(F_v, \mathbf{Z}_p(1))$ with its image $i_v(H^1_f(F_v, \mathbf{Z}_p(1)))$ in $H^1_f(F_v, T_y)$. Let $\log_p$ denote Iwasawa's branch of the p-adic logarithm (so $\log_p(p) = 0$). We define

$$\langle y, x \rangle = \sum_v \log_p[\mathrm{Norm}_{F_v/\mathbf{Q}_v}(t_y(x_v) - \mathrm{loc}_v(\tilde{x}))] \in \mathbf{Z}_p.$$

This definition makes sense because if $u_v \in H^1_f(F_v, \mathbf{Z}_p)_u$, then

$$\log_p[\mathrm{Norm}_{F_v/\mathbf{Q}_v}(u_v)] = 0,$$

while if $u \in H^1_f(F, \mathbf{Z}_p(1))$, then

$$\sum_v \log_p[\mathrm{Norm}_{F_v/\mathbf{Q}_v}(\mathrm{loc}_v(u))] = 0.$$

4. An exact sequence

In this section we shall establish the following result which will be used in the proof of Theorem B.

Theorem 4.1. *There is an exact sequence*

$$0 \to \mathrm{Ker}(\Psi_{\mathbf{Z}_p(1)}) \to \mathrm{Ker}(\Psi_{T_y}) \to \mathrm{Ker}(\Psi_T),$$

and the cokernel of the last arrow is annihilated by the classnumber h_F of F. □

Remark 4.2. As $A(\mathbf{Z}_p(1))_{O_F,n} \simeq \oplus_{i=1}^{p^n} O_F$ we see from Theorem 2.2 and Corollary 2.4 that, for each n, the kernel of the class invariant map

$$\Psi_{\mathbf{Z}_p(1),n} : H^1(O_F, \underline{\mu_{p^n}}) \to \mathrm{Cl}(A(\mathbf{Z}_p(1))_n)$$

is equal to $O_F^{\times}/O_F^{\times p^n}$. This in turn implies that

$$\mathrm{Ker}(\Psi_{\mathbf{Z}_p(1)}) \simeq O_F^{\times} \otimes_{\mathbf{Z}} \mathbf{Z}_p \simeq H^1_f(F, \mathbf{Z}_p(1)).$$

□

The proof of Theorem 4.1 proceeds via a series of lemmas.

Lemma 4.3. *(a) There is an exact sequence*

$$1 \to A(\mathbf{Z}_p(1))^{\times}_{n,O_{F^c}} \to A(T_y)^{\times}_{n,O_{F^c}} \to A(T)^{\times}_{n,O_{F^c}} \to 1. \tag{4.1}$$

(b) For each finite place v of F, there is an exact sequence

$$1 \to A(\mathbf{Z}_p(1))^{\times}_{n,v} \to A(T_y)^{\times}_{n,v} \to A(T)^{\times}_{n,v} \to 1. \tag{4.2}$$

Proof. (a) For each $n \geq 1$, applying Cartier duality to (3.5) yields an exact sequence

$$0 \to E^D[p^n] \to G^D_{y,n} \to \underline{\mathbf{Z}/p^n\mathbf{Z}} \to 0.$$

This in turn gives (using the notation established in the proof of Theorem 2.2):

$$1 \to \mathcal{M}(\underline{\mathbf{Z}/p^n\mathbf{Z}}, \mathbf{G}_m) \to \mathcal{M}(G^D_{y,n}, \mathbf{G}_m) \to \mathcal{M}(E^D[p^n], \mathbf{G}_m), \tag{4.3}$$

which is exact on the left, but not *a priori* on the right.

Now over $\mathrm{Spec}(O_{F^c})$ there is an isomorphism of group schemes

$$G_{y,n/O_{F^c}} \simeq \left(\underline{\mu_{p^n}} \times_{\mathrm{Spec}(O_F)} E[p^n]\right)_{/O_{F^c}} \tag{4.4}$$

(cf. (2.2)); this in turn induces an isomorphism of group schemes

$$\mathcal{M}(G_{y,n}^D, \mathbf{G}_m)_{/O_{F^c}} \simeq \mathcal{M}(\underline{\mathbf{Z}/p^n\mathbf{Z}} \times_{\mathrm{Spec}(O_F)} E^D[p^n], \mathbf{G}_m)_{/O_{F^c}}.$$

It follows from this last isomorphism that the natural map

$$\mathcal{M}(G_{y,n}^D, \mathbf{G}_m)(O_{F^c}) \to \mathcal{M}(E^D[p^n], \mathbf{G}_m)(O_{F^c})$$

is surjective. We now see from (4.3) that there is an exact sequence

$$1 \to A(\mathbf{Z}_p(1))^\times_{n,O_{F^c}} \to A(T_y)^\times_{n,O_{F^c}} \to A(T)^\times_{n,O_{F^c}} \to 1$$

as claimed.

(b) Since O_{F_v} is a local ring, we may choose an isomorphism of schemes (but not of group schemes) over $\mathrm{Spec}(O_{F_v})$:

$$G_{y,n/O_{F_v}} \simeq \left(\underline{\mu_{p^n}} \times_{\mathrm{Spec}(O_F)} E[p^n]\right)_{/O_{F_v}},$$

which in turn implies that the natural map

$$\mathcal{M}(G_{y,n}^D, \mathbf{G}_m)(O_{F_v}) \to \mathcal{M}(E^D[p^n], \mathbf{G}_m)(O_{F_v})$$

is surjective. The desired result now follows as in part (a). □

Lemma 4.4. *The kernel of the natural map*

$$H^1(F, A(\mathbf{Z}_p(1))^\times_{O_{F^c}}) \to \prod_v H^1(F_v, A(\mathbf{Z}_p(1))^\times_{O_{F_v^c}}),$$

(where the product on the right is over all finite places v of F), is annihilated by h_F.

Proof. For each n, the Wedderburn decomposition of $A(\mathbf{Z}_p(1))_{n,O_{F^c}}$ is given by

$$A(\mathbf{Z}_p(1))_{n,O_{F^c}} \simeq \prod_{i=1}^{p^n} O_{F^c}.$$

In order to prove the lemma, it therefore suffices to show that the kernel of the natural map

$$H^1(F, O_{F^c}^\times) \to \prod_v H^1(F_v, O_{F_v^c}^\times)$$

is annihilated by h_F.

Via taking Ω_F cohomology of the exact sequence

$$1 \to O_{F^c}^\times \to F^{c\times} \to F^{c\times}/O_{F^c}^\times \to 1,$$

we see that

$$H^1(F, O_{F^c}^\times) \simeq \frac{I(O_{F^c})^{\Omega_F}}{P(O_F)},$$

where $I(O_{F^c})$ denotes the group of fractional O_{F^c}-ideals (note that every such ideal is principal) and $P(O_F)$ denotes the group of principal O_F-ideals. A similar argument also shows that

$$H^1(F_v, O_{F_v^c}^\times) \simeq \frac{I(O_{F_v^c})^{\Omega_{F_v}}}{P(O_{F_v})}.$$

Each element lying in the kernel of the natural map

$$\frac{I(O_{F^c})^{\Omega_F}}{P(O_F)} \to \prod_v \frac{I(O_{F_v^c})^{\Omega_{F_v}}}{P(O_{F_v})}$$

is represented by an O_{F^c}-ideal that is a lift of an O_F-ideal, and so is annihilated by h_F. This proves the lemma. □

Lemma 4.5. *The kernel of the natural map*

$$H^1\left(F, \frac{A(\mathbf{Z}_p(1))_{O_{F^c}}^\times}{\mathbf{Z}_p(1)}\right) \to \prod_v H^1\left(F_v, \frac{A(\mathbf{Z}_p(1))_{O_{F_v^c}}^\times}{\mathbf{Z}_p(1)}\right) \tag{4.5}$$

(where the product on the right is over all finite places of F) is annhilated by h_F.

Proof. Consider the exact sequence

$$1 \to \mathbf{Z}_p(1) \to A(\mathbf{Z}_p(1))^{\times}_{O_{F^c}} \to \frac{A(\mathbf{Z}_p(1))^{\times}_{O_{F^c}}}{\mathbf{Z}_p(1)} \to 1.$$

Taking Ω_F-cohomology of this sequence gives

$$1 \to A(\mathbf{Z}_p(1))^{\times} \to \mathbf{H}(A(\mathbf{Z}_p(1))) \to H^1(F, \mathbf{Z}_p(1)) \to H^1(F, A(\mathbf{Z}_p(1))^{\times}_{O_{F^c}}) \to$$
$$\to H^1(F, A(\mathbf{Z}_p(1))^{\times}_{O_{F^c}}/\mathbf{Z}_p(1)) \to H^2(F, \mathbf{Z}_p(1)).$$

Since

$$H(A(\mathbf{Z}_p(1))) = \frac{\mathbf{H}(A(\mathbf{Z}_p(1)))}{A(\mathbf{Z}_p(1))^{\times}} \simeq \mathrm{Ker}(\Psi_{\mathbf{Z}_p(1)}) = H^1_f(F, \mathbf{Z}_p(1)),$$

(see Remark 4.2 above), we obtain

$$0 \to \frac{H^1(F, \mathbf{Z}_p(1))}{H^1_f(F, \mathbf{Z}_p(1))} \to H^1(F, A(\mathbf{Z}_p(1))^{\times}_{O_{F^c}}) \to H^1(F, A(\mathbf{Z}_p(1))^{\times}_{O_{F^c}}/\mathbf{Z}_p(1)) \to$$
$$\to H^2(F, \mathbf{Z}_p(1)).$$

As the natural maps

$$\frac{H^1(F, \mathbf{Z}_p(1))}{H^1_f(F, \mathbf{Z}_p(1))} \to \prod_v \frac{H^1(F_v, \mathbf{Z}_p(1))}{H^1_f(F_v, \mathbf{Z}_p(1))}$$

and

$$H^2(F, \mathbf{Z}_p(1)) \to \prod_v H^2(F_v, \mathbf{Z}_p(1))$$

are both injective, Lemma 4.4 implies that the kernel of

$$H^1\left(F, \frac{A(\mathbf{Z}_p(1))^{\times}_{O_{F^c}}}{\mathbf{Z}_p(1)}\right) \to \prod_v H^1\left(F_v, \frac{A(\mathbf{Z}_p(1))^{\times}_{O_{F_v^c}}}{\mathbf{Z}_p(1)}\right)$$

is annihilated by h_F, as claimed. □

Lemma 4.6. *There is an exact sequence of resolvends*

$$1 \to \mathbf{H}(A(\mathbf{Z}_p(1))) \to \mathbf{H}(A(T_y)) \to \mathbf{H}(A(T)),$$

and the cokernel of the last arrow is annihilated by h_F.

Proof. Set $\Gamma_n := E[p^n](O_{F^c})$ and $\Gamma_{n,y} := G_{y,n}(O_{F^c})$. As the isomorphism (4.4) is well-defined up to an element of Γ_n, we may pass to inverse limits with respect to n over the exact sequences

$$1 \to A(\mathbf{Z}_p(1))^{\times}_{n,O_{F^c}}/\mu_{p^n} \to A(T_y)^{\times}_{n,O_{F^c}}/\Gamma_{y,n} \to A(T)^{\times}_{n,O_{F^c}}/\Gamma_n \to 1.$$

afforded by Lemma 4.3(a) to obtain an exact sequence

$$1 \to A(\mathbf{Z}_p(1))^{\times}_{O_{F^c}}/\mathbf{Z}_p(1) \to A(T_y)^{\times}_{O_{F^c}}/T_y \to A(T)^{\times}_{O_{F^c}}/T \to 1.$$

Taking Ω_F-cohomology of this last sequence gives

$$1 \to \mathbf{H}(A(\mathbf{Z}_p(1))) \to \mathbf{H}(A(T_y)) \to \mathbf{H}(A(T)) \xrightarrow{f_4} H^1\left(F, A(\mathbf{Z}_p(1))^{\times}_{O_{F^c}}/\mathbf{Z}_p(1)\right).$$

For each finite place v of F, it follows from the exact sequence

$$0 \to H^1_f(F_v, \mathbf{Z}_p(1)) \to H^1_f(F_v, T_y) \to H^1_f(F_v, T) \to 0$$

(see the discussion following (3.6)), and Proposition 2.10) that there is an exact sequence

$$0 \to H(A(\mathbf{Z}_p(1))_v) \to H(A(T_y)_v) \to H(A(T)_v) \to 0,$$

and so Lemma 4.3(b) implies that there is also an exact sequence

$$1 \to \mathbf{H}(A(\mathbf{Z}_p(1))_v) \to \mathbf{H}(A(T_y)_v) \to \mathbf{H}(A(T)_v) \to 1.$$

Hence, if $z \in \mathbf{H}(A(T))$, then $\mathrm{loc}_v(f_4(z)) = 0$ for each finite place v of F. We now deduce from Lemma 4.4 that $f_4(h_F \cdot z) = 0$, and this proves the desired result. □

Proposition 4.1 is now a direct consequence of Lemma 4.6.

5. Proof of Theorem B

We retain the notation established in Section 3.

In this section, we shall prove Theorem B by establishing the following result.

Proposition 5.1. *Suppose that $x \in h_F \cdot H^1_f(F,T)^0$, and that $y \in H^1_f(F,T^*)$. Then for every finite place v of F, we have that*

$$t_y(x_v) - \mathrm{loc}_v(\tilde{x}) \in H^1_f(F_v, \mathbf{Z}_p(1))_u \cdot \mathrm{loc}_v[H^1_f(F, \mathbf{Z}_p(1))]. \tag{5.1}$$

Hence $\langle y, x \rangle = 0$.

Proof. We shall establish (5.1) by analysing resolvends associated to $t_y(x_v)$ and $\mathrm{loc}_v(\tilde{x})$.

Since $x \in h_F \cdot H^1_f(F,T)^0$ with $\Psi_T(x) = 0$, Theorem 4.1 implies that we may choose $\tilde{x} \in H^1_f(F,T_y)$ with $\tilde{x} \in \mathrm{Ker}(\Psi_{T_y})$. Let $\mathbf{r}(\tilde{x}) \in \mathbf{H}(A(T_y))$ be any resolvend associated to $\tilde{x}$. Then $\mathbf{r}(\tilde{x})$ may be viewed as being a well-defined element of

$$\frac{\mathbf{H}(A(T_y))}{T_y \cdot A(T_y)^\times \cdot i[\mathbf{H}(A(\mathbf{Z}_p(1)))]}.$$

For each $\tilde{x}_{n,v} \in H^1_f(F_{n,v}, T_y)$, we choose an associated resolvend $\mathbf{r}(\tilde{x}_{n,v}) \in \mathbf{H}(A(T_y)_{O_{F_{n,v}}})$, and we set

$$\mathbf{r}(z_{n,v}) := \mathcal{N}_{F_{n,v}/F_v}(\mathbf{r}(\tilde{x}_{n,v})).$$

Then $\mathbf{r}(z_{n,v})$ is a resolvend associated to $z_{n,v}$, and we may view it as lying in

$$\frac{\mathcal{N}_{F_{n,v}/F_v}(\mathbf{H}(A(T_y)_{O_{F_{n,v}}}))}{\mathcal{N}_{F_{n,v}/F_v}\{(T_y \cdot A(T_y)^\times_{O_{F_{n,v}}}) \cdot i_v[\mathbf{H}(A(\mathbf{Z}_p(1))_{O_{F_{n,v}}})]\}}.$$

Letting $n \to \infty$ yields an element of

$$\frac{\cap_{n\geq 1}[\mathcal{N}_{F_{n,v}/F_v}(\mathbf{H}(A(T_y)_{O_{F_{n,v}}}))]}{\cap_{n\geq 1}[\mathcal{N}_{F_{n,v}/F_v}\{(T_y \cdot A(T_y)^{\times}_{O_{F_{n,v}}}) \cdot i_v[\mathbf{H}(A(\mathbf{Z}_p(1))_{O_{F_{n,v}}})]\}]}$$
$$:= \frac{\mathbf{H}(A(T_y)_{O_{F_v}})_u}{[T_y \cdot A(T_y)^{\times}_{O_{F_v}} \cdot i_v[\mathbf{H}(A(\mathbf{Z}_p(1))_{O_{F_v}})]]_u}.$$

We choose a representative $\mathbf{r}(t_y(x_v)) \in \mathbf{H}(A(T_y)_{O_{F_v}})_u$ of this element; then $\mathbf{r}(t_y(x_v))$ is a resolvend associated to $t_y(x_v)$.

It follows from our construction that

$$\mathbf{r}(t_y(x_v)) \cdot \mathrm{loc}_v(\mathbf{r}(\tilde{x}))^{-1} \in \mathbf{H}(A(T_y)_{O_{F_v}})$$

is a resolvend associated to $t_y(x_v) - \mathrm{loc}_v(\tilde{x}) \in H^1_f(F_v, T_y)$. Since

$$t_y(x_v) - \mathrm{loc}_v(\tilde{x}) \in i[H^1_f(F_v, \mathbf{Z}_p(1))],$$

it follows that there exists $\delta_v \in T_y \cdot A(T_y)^{\times}_{O_{F_v}}$ and $\mathbf{r}(u_v) \in \mathbf{H}(A(\mathbf{Z}_p(1))_{O_{F_v}})$ such that

$$\mathbf{r}(u_v) = \mathbf{r}(t_y(x_v)) \cdot \mathrm{loc}_v(\mathbf{r}(\tilde{x})) \cdot \delta_v, \tag{5.2}$$

(where we have identified $\mathbf{H}(A(\mathbf{Z}_p(1))_{O_{F_v}})$ with its image in $\mathbf{H}(A(T_y)_{O_{F_v}})$.

For each integer m we consider the equality

$$\mathbf{r}(u_{v,m}) = \mathbf{r}(t_y(x_v)_m) \cdot \mathrm{loc}_v(\mathbf{r}(\tilde{x}_m)) \cdot \delta_{v,m}, \tag{5.3}$$

that is obtained via taking the image of (5.2) under the natural map

$$\mathbf{H}(A(T_y)_{O_{F_v}}) \to \mathbf{H}(A(T_y)_{m,O_{F_v}}).$$

We have that $\mathbf{r}(u_{v,m})$ is a resolvend associated to the image $t_y(x_v)_m - \tilde{x}_m$ in $H^1(F_v, \mu_{p^m})$ of $t_y(x_v) - \mathrm{loc}_v(\tilde{x}) \in H^1_f(F_v, \mathbf{Z}_p(1))$.

We now evaluate $t_y(x_v)_m - \tilde{x}_m$ using Proposition 2.7. From (5.3) we deduce that

$$\mathbf{r}(u_{v,m})^{p^m} = \mathbf{r}(t_y(x_v)_m)^{p^m} \cdot \mathrm{loc}_v(\mathbf{r}(\tilde{x}_m))^{p^m} \cdot \delta_{v,m}^{p^m}. \tag{5.4}$$

It follows from the definitions of u_v, $t_y(x_v)$, $\tilde{x}$, and δ_v that we have

$$\begin{aligned}
&u_{v,m}^{p^m} \in A(\mathbf{Z}_p(1))^{\times}_{m,O_{F_v}};\\
&\mathbf{r}(t_y(x_v)_m)^{p^m} \in \cap_n \mathcal{N}_{F_{n.v}/F_v}(A(T_y)^{\times}_{m,O_{F_{n,v}}}) := [A(T_y)^{\times}_{m,O_{F_v}}]_u;\\
&\mathrm{loc}_v(\mathbf{r}(\tilde{x}_m))^{p^m} \in \mathrm{loc}_v[A(T_y)^{\times}_m];\\
&\delta_{v,m}^{p^m} \in A(T_y)^{\times p^m}_{O_{F_v}}.
\end{aligned}$$

Hence, if $\mathbf{1}_m$ is a generator of $\mathbf{Z}/p^m\mathbf{Z} \subseteq G^D_{y,m}(F^c)$, then

$$\begin{aligned}
\mathrm{ev}_{\mathbf{1}_m}(u_{v,m}^{p^m}) &= \mathrm{ev}_{\mathbf{1}_m}[\mathbf{r}(t_y(x_v)_m)^{p^m} \cdot \mathrm{loc}_v(\mathbf{r}(\tilde{x}_m))^{p^m} \cdot \delta_{v,m}^{p^m}]\\
&\in [O^{\times}_{F,v}]_u \cdot \mathrm{loc}_v[O^{\times}_F] \cdot O^{\times p^m}_{F,v},
\end{aligned}$$

where $[O^{\times}_{F,v}]_u := \cap_n \mathrm{Norm}_{F_{n,v}/F_v}[O^{\times}_{F_{n,v}}]$.

We therefore deduce that

$$t_y(x_v)_m - \mathrm{loc}_v(\tilde{x}_m) \in \frac{[O^{\times}_{F,v}]_u \cdot \mathrm{loc}_v[O^{\times}_F] \cdot F_v^{\times p^m}}{F_v^{\times p^m}} \subseteq H^1(F_v, \mu_{p^m})$$

for every integer $m \geq 1$. This in turn implies that

$$t_y(x_v) - \mathrm{loc}_v(\tilde{x}) \in H^1_f(F_v, \mathbf{Z}_p(1))_u \cdot \mathrm{loc}_v(H^1_f(F, \mathbf{Z}_p(1))),$$

as claimed. □

References

[1] A. Agboola, *A geometric interpretation of the class invariant homomorphism*, Journal de Théorie des Nombres de Bordeaux, **8** (1994), 273–280.

[2] A. Agboola, *Abelian varieties and Galois module structure in global function fields*, Math. Zeit., **217**, (1994), 407–419.

[3] A. Agboola, *Iwasawa theory of elliptic curves and Galois module structure*, Duke Math. J., **71**, (1993), 441–462.

[4] A. Agboola, *Torsion points on elliptic curves and Galois module structure*, Invent. Math., **123**, (1996), 105–122.

[5] A. Agboola, *Exotic Selmer groups, p-adic height pairings, and Galois module structure*, preprint.

[6] A. Agboola, D. Burns, *On twisted forms and relative algebraic K-theory*, Proc. London Math. Soc., **92**, (2006), 1–28.

[7] A. Agboola, G. Pappas, *On arithmetic class invariants*, Math. Annalen., **320**, (2001), 339–365.

[8] A. Agboola, G.Pappas, *Line bundles, rational points and ideal classes*, Math. Res. Letters **7** (2000), 709–717.

[9] A. Agboola, M. J. Taylor, *Class invariants of Mordell-Weil groups*, Crelle, **447**, (1994), 23–61.

[10] S. Bloch, K. Kato, *L-functions and Tamagawa numbers of motives*, In: The Grothendieck Festchrift (Vol. I), P. Cartier, et al., eds, *Prog. in Math.*, **86**, Birkhäuser, 1990, 333–400.

[11] S. Bosch, W. Lütkebohmert, M. Raynaud, *Néron Models*, Springer Verlag, 1990.

[12] N. P. Byott, *Tame realisable classes over Hopf orders*, J. Algebra, **201**, (1998), 284-316.

[13] N. P. Byott, M. J. Taylor, *Hopf orders and Galois module structure*, In: Group rings and classgroups, K. W. Roggenkamp, M. J. Taylor (eds), Birkhäuser, 1992, pp. 153–210.

[14] Ph. Cassou-Noguès, M. J. Taylor, *Elliptic functions and rings of integers*, Prog. in Math. **66** Birkhäuser, 1987.

[15] T. Chinburg, B. Erez, G. Pappas, M. J. Taylor, *Tame actions for group schemes: integrals and slices*, Duke Math. Journal, **82**, (1996), 269–308.

[16] A. Grothendieck et al., *Groupes de monodromie en géometrie algébrique*, Lecture Notes in Mathematics, Vol. 288, Springer-Verlag, Berlin-New York, 1970.

[17] J. W. Jones, *Plater's p-adic orthogonality relation for abelian varieties*, Houston J. Math. **21**, (1995), 261–282.

[18] L. R. McCulloh, *Galois module structure of abelian extensions*, Crelle, **375/376**, (1987), 259-306.

[19] G. Pappas, *On torsion line bundles and torsion points on abelian varieties*, Duke Math. J., **91** (1998), 215–224.

[20] G. Pappas, *Galois modules and the theorem of the cube*, Invent. Math., **133** (1998), 193–225.

[21] B. Perrin-Riou, *Théorie d'Iwasawa et hauteurs p-adiques*, Invent. Math. **109** (1992), no.1, 137–185.

[22] B. Perrin-Riou, *Théorie d'Iwasawa et hauteurs p-adiques (cas de variétés abéliennes)*, Séminaire de théorie des nombres de Paris 1990-91.

[23] A. Plater, *Height pairings on elliptic curves*, Cambridge University Ph.D. thesis, 1991.

[24] A. Plater, *An orthogonality relation on the points of an elliptic curve*, J. London Math. Soc (2), **44** (1991), 227–249.

[25] A. Srivastav, M. J. Taylor, *Elliptic curves with complex multiplication and Galois module structure*, Invent. Math., **99**, (1990), 165–184.

[26] M. J. Taylor, *Mordell-Weil groups and the Galois module structure of rings of integers*, Ill. J. Math. **32** (1988), 428–452.

[27] M. J. Taylor, *Relative Galois module structure of rings of integers and elliptic functions II*, Ann. Math. (2) **121**, (1985), no. 3, 519–535.

[28] M. J. Taylor, *Résolvandes et espaces homogènes principaux de schémas en groupe*, Sém. Théor. Nombres Bordeaux (2) **2** (1990), no. 2, 255–271.

[29] W. Waterhouse, *Principal homogeneous spaces and group scheme extensions*, AMS Transactions **153**, (1971), 181-189.

Department of Mathematics, University of California, Santa Barbara, CA 93106.
E-mail address: agboola@math.ucsb.edu