EXOTIC SELMER GROUPS, p-ADIC HEIGHT PAIRINGS, AND GALOIS MODULE STRUCTURE

A. AGBOOLA

Abstract. In this paper we generalise the theory of class invariants in way that it may be applied to p-adic representations of absolute Galois groups of number fields. Our main idea involves a new way of using relative algebraic K-theory and resolvends associated to torsors of certain finite group schemes to describe certain Selmer groups. We show that certain of the class invariants that we construct are closely connected with the conjectured non-degeneracy of certain p-adic height pairings attached to arbitrary p-adic Galois representations. This yields a generalisation of certain results that up to now have only been known in certain cases involving elliptic curves with complex multiplication.

Contents

Date: Version of November 7, 2014.

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

1. Introduction

In this paper we shall introduce and study invariants which measure the Galois structure of certain torsors that are constructed via p-adic Galois representations. As we shall explain below, these Galois structure invariants are intimately connected with the conjectured non-degeneracy of a certain p-adic height pairing attached to an arbitrary p-adic representation, first constructed by B. Perrin-Riou in [24].

We begin by describing the background to the questions that we intend to discuss. Let Y be any scheme, and suppose that $G \to Y$ is a finite, flat, commutative group scheme. Write G^* for the Cartier dual of G. Let $\widetilde{G}^*$ denote the normalisation of G^*, and let $i : \widetilde{G}^* \to G^*$ be the natural map. Suppose that $\pi : X \to Y$ is 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 $\mathcal{O}_{G^*}$-module (see e.g. [13]). As an $\mathcal{O}_{G^*}$-module, the structure sheaf $\mathcal{O}_X$ is locally free of rank one, and so it gives a line bundle $\mathfrak{L}_\pi$ on G^*. Set

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

Then the maps

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

$$\varphi : H^1(Y, G) \to \mathrm{Pic}(\widetilde{G}^*), \qquad [\pi] \mapsto [i^*\mathcal{L}_\pi] \tag{1.2}$$

are homomorphisms which are often referred to as 'class invariant homomorphisms'.

The initial motivation for studying class invariant homomorphisms arose from Galois module theory. Let F be a number field with ring of integers O_F, and suppose that $Y = \mathrm{Spec}(O_F)$. Write $G^* = \mathrm{Spec}(A)$, $G = \mathrm{Spec}(B)$, and $X = \mathrm{Spec}(C)$. Then the algebra C is a twisted form of B, and the homomorphisms ψ and φ measure the Galois module structure of this twisted

form. The homomorphism ψ was first introduced by W. Waterhouse (see [35]), and was further developed in the context of Galois module theory by M. Taylor ([32]). Taylor originally considered the case in which G is a torsion subgroup scheme of an abelian variety with complex multiplication. The corresponding torsors are obtained by dividing points in the Mordell-Weil groups of such abelian varieties, and they are closely related to rings of integers of abelian extensions of F. In [29], it was shown that, for elliptic curves with complex multiplication, the class invariant homomorphism ψ vanishes on the classes of torsors obtained by dividing torsion points of order coprime to 6. This implies the existence of Hopf Galois generators for certain rings of integers of abelian extensions of imaginary quadratic fields, and it may be viewed as an integral version of the Kronecker Jugendtraum (see [33], [12]). This vanishing result was extended to all elliptic curves in [2] and [22].

Since their introduction, class invariants of torsors obtained by dividing points on abelian varieties have been studied in greater generality by several authors. For example, suppose that $\mathcal{X}$ is a projective curve over $\mathrm{Spec}(\mathbf{Z})$ which is equipped with a free action of a finite group. In [23], it is shown that the behaviour of the equivariant projective Euler characteristic of $\mathcal{O}_{\mathcal{X}}$ is partly governed by class invariants of torsors arising from torsion points on the Jacobian of $\mathcal{X}$. In [6], an Arakelov (i.e. arithmetic) version of class invariants of torsors coming from points on abelian varieties is considered. There it is shown that in general such torsors are completely determined by their arithmetic class invariants, and that these invariants are related to Mazur-Tate heights on the abelian variety (see [19]). Finally we mention that in [1], [3], and [7], class invariants arising from points on elliptic curves with complex multiplication are studied using Iwasawa theory, and they are shown to be closely related to the p-adic height pairing on the elliptic curve.

The main goal of this paper is to develop a theory of class invariants for arbitrary p-adic Galois representations, and to thereby generalise a number of results that up to now have only been known in certain cases involving elliptic curves with complex multiplication.

We now describe the approach and the main results contained in this paper. Suppose that p is an odd prime, and let V be a d-dimensional $\mathbf{Q}_p$-vector space. Let F^c be an algebraic closure of F, and write $\Omega_F := \mathrm{Gal}(F^c/F)$. Suppose that $\rho : \Omega_F \to \mathrm{GL}(V)$ is a continuous representation of Ω_F that is ramified at only finitely many primes of F. Set $V^* := \mathrm{Hom}_{\mathbf{Q}_p}(V, \mathbf{Q}_p(1))$, and let $\rho^* : \Omega_F \to \mathrm{GL}(V^*)$ be the corresponding representation of Ω_F. Suppose that $T \subseteq V$ is an Ω_F-stable $\mathbf{Z}_p$-lattice, and write $T^* := \mathrm{Hom}_{\mathbf{Z}_p}(T, \mathbf{Z}_p(1))$. (Note that for each construction in this paper that depends upon T, there is also a corresponding construction that depends upon T^*; this will not always be explicitly stated.)

For each positive integer n, we may define finite, commutative group schemes G_n and G_n^* over $\mathrm{Spec}(F)$ by

$$G_n(F^c) = \Gamma_n := p^{-n}T/T; \qquad G_n^*(F^c) = \Gamma_n^* := p^{-n}T^*/T^*.$$

Then G_n^* is the Cartier dual of G_n, and we may write $G_n^* = \mathrm{Spec}(A_n)$ for some Hopf algebra A_n over F (see Remark 2.16 below).

Let $\pi_n \in H^1(F, G_n)$. The starting point of our approach is the observation that, because π_n becomes trivial over F^c, there is a natural isomorphism $\xi_{\pi_n} : \mathcal{L}_{\pi_n} \otimes_F F^c \simeq A_n \otimes_F F^c$, and so the triple $(\mathcal{L}_{\pi_n}, A_n; \xi_{\pi_n})$ determines an element in a quotient of a certain relative algebraic K-group that we denote by $\bar{K}_0(A_n, F^c)$ (see [5] and Section 2.3 below). This yields a homomorphism

$$\hat{\psi}_{A_n} : H^1(F, G_n) \to \bar{K}_0(A_n, F^c); \quad [\mathcal{L}_{\pi_n}, A_n; \xi_{\pi_n}]. \tag{1.3}$$

Suppose now that $\mathfrak{A}_n \subseteq A_n$ is any O_F-algebra. (In particular, we do not assume that $\mathfrak{A}_n$ is an O_F-Hopf algebra.) We use the description of $H^1(F, G)$ afforded by (1.3) to give a new way of imposing local conditions on cohomology classes in terms of $\mathfrak{A}_n$. (Roughly speaking, if $\pi \in H^1(F, G_n)$, then we use $\mathfrak{A}_n$ to impose local conditions on the line bundle $\mathcal{L}_\pi$ associated to π.) This yields a certain Selmer group in $H^1(F, G_n)$ which we denote by $H^1_{\mathfrak{A}_n}(F, G_n)$. We also show that $\mathfrak{A}_n$ determines a subgroup $K_0(A_n, F^c)_{\mathfrak{A}_n}$ of $K_0(A, F^c)$, together with a homomorphism

$$K_0(A_n, F^c)_{\mathfrak{A}_n} \to \mathrm{Cl}(\mathfrak{A}_n). \tag{1.4}$$

Via restriction, the map $\hat{\psi}_{A_n}$ yields a homomorphism

$$\hat{\psi}_{\mathfrak{A}_n} : H^1_{\mathfrak{A}_n}(F, G) \to K_0(A_n, F^c)_{\mathfrak{A}_n},$$

and we write

$$\psi_{\mathfrak{A}_n} : H^1_{\mathfrak{A}_n}(F, G) \to \mathrm{Cl}(\mathfrak{A}_n) \tag{1.5}$$

for the composition of $\hat{\psi}_{\mathfrak{A}_n}$ with the homomorphism of (1.4).

The homomorphism (1.5) generalises the class invariant homomorphisms (1.1) and (1.2) above. For suppose now that G_n is the generic fibre of a finite, flat group scheme $\mathcal{G}_n$ over $\mathrm{Spec}(O_F)$. If we choose $\mathfrak{A}_n$ to be the O_F-Hopf algebra representing the Cartier dual $\mathcal{G}_n^*$ of $\mathcal{G}_n$, then $H^1_{\mathfrak{A}_n}(F, G_n) = H^1(\mathrm{Spec}(O_F), \mathcal{G}_n)$, and $\psi_{\mathfrak{A}_n}$ is the same as the homomorphism (1.1) in this case. If on the other hand we take $\mathfrak{A}_n$ to be the maximal O_F-order $\mathfrak{M}_n$ in A_n, then $\mathrm{Spec}(\mathfrak{A}_n)$ is equal to the normalisation $\tilde{\mathcal{G}}_n^*$ of $\mathcal{G}_n^*$. In this case, $H^1(\mathrm{Spec}(O_F), \mathcal{G}_n)$ is contained in $H^1_{\mathfrak{M}_n}(F, G_n)$, and the restriction of $\psi_{\mathfrak{M}_n}$ to $H^1(\mathrm{Spec}(O_F), \mathcal{G}_n)$ is the homomorphism (1.2).

Set

$$\mathcal{R}_F := O_F[1/p]$$

and write

$$\mathcal{M}_n := \mathfrak{M}_n \otimes_{O_F} \mathcal{R}_F.$$

In this paper we shall mainly be concerned with the case in which

$$\mathfrak{A}_n = \mathcal{M}_n.$$

For each finite place v of F, let F_v^{nr} denote the maximal unramified extension of F_v in a fixed algebraic closure of F_v. If $v \nmid p$, then define

$$H^1_f(F_v, T) := \mathrm{Ker}\left[H^1(F_v, T) \to H^1(F_v^{\mathrm{nr}}, T)\right].$$

Following [24, §3.1.4], we set

$$H^1_{f,\{p\}}(F, T) = \mathrm{Ker}\left[H^1(F, T) \to \oplus_{v \nmid p} \frac{H^1(F_v, T)}{H^1_f(F_v, T)}\right].$$

It may be shown that (see Remark 3.1 below)

$$H^1_{f,\{p\}}(F, T) \subseteq \varprojlim H^1_{\mathcal{M}_n}(F, G_n).$$

Here the inverse limit is taken with respect to the maps induced by the 'multiplication by p' maps $G_{n+1} \to G_n$, and we view $\varprojlim H^1_{\mathcal{M}_n}(F, G_n)$ as being a subgroup of $H^1(F, T)$ via the canonical isomorphism $\varprojlim H^1(F, G_n) \simeq H^1(F, T)$. Set

$$H^1_{\mathcal{M}(T)}(F, T) := \varprojlim H^1_{\mathcal{M}_n}(F, G_n).$$

The natural maps $G_n \to G_{n-1}$ induce homomorphisms

$$\mathrm{Cl}(\mathcal{M}_n) \to \mathrm{Cl}(\mathcal{M}_{n-1}),$$

and we set

$$\mathrm{Cl}(\mathcal{M}) := \varprojlim \mathrm{Cl}(\mathcal{M}_n).$$

We shall show that we may take inverse limits in (1.5) to obtain a homomorphism

$$\Psi_{\mathcal{M}} : H^1_{\mathcal{M}}(F, T) \to \mathrm{Cl}(\mathcal{M}).$$

Our main result shows that the homomorphism $\Psi_{\mathcal{M}}$ is closely related to a p-adic height pairing associated to T. In order to describe why this is so, we have to introduce some further notation.

Let C_n/F denote the n-th layer of the cyclotomic $\mathbf{Z}_p$-extension of F, and set

$$\mathfrak{G}_F(T) :=$$
$$\{x \in H^1_{f,\{p\}}(F,T) \mid Mx \in \cap_n \mathrm{Cores}_{C_n/F}(H^1_{f,\{p\}}(C_n,T)) \text{ for some integer } M > 0\}.$$

When T is the p-adic Tate module of an elliptic curve, $\mathfrak{G}_F(T)$ is the same as the canonical subgroup that was defined by R. Greenberg in [15, p.131–132], and further studied by A. Plater in [25] and [26] (see also [18]).

Let

$$\mathrm{Loc}_{F,T^*} : H^1_{f,\{p\}}(F,T^*) \to \prod_{v|p} H^1(F_v,T^*)$$

denote the natural localisation map. In [24, Section 3.1.4], Perrin-Riou constructs a p-adic height pairing

$$B_F : H^1_{f,\{p\}}(F,T) \times \mathrm{Ker}(\mathrm{Loc}_{F,T^*}) \to \mathbf{Q}_p,$$

and she shows that the group $\mathfrak{G}_F(T)$ lies in the left-hand kernel of B_F. Write

$$\langle\langle\ ,\ \rangle\rangle : \frac{H^1_{f,\{p\}}(F,T)}{\mathfrak{G}_F(T)} \times \mathrm{Ker}(\mathrm{Loc}_{F,T^*}) \to \mathbf{Q}_p \tag{1.6}$$

for the pairing induced by B_F. We remark that it follows from the definition of $\mathfrak{G}_F(T)$ that the group $H^1_{f,\{p\}}(F,T)/\mathfrak{G}_F(T)$ is torsion-free. It is conjectured that $\langle\langle\ ,\ \rangle\rangle$ is always non-degenerate modulo torsion. If this conjecture is true, then it implies that $\mathfrak{G}_F(T)$ has a natural characterisation in terms of p-adic height pairings attached to T. The following two results show that this conjecture also implies that $\mathfrak{G}_F(T)$ has a natural characterisation in terms of Galois module structure.

Theorem A. *If $x \in \mathfrak{G}_F(T)$, then $\Psi_{\mathcal{M}}(x)$ is of finite order.*

Theorem B. *Suppose that $H^0(F,T) = 0$. If $x \in H^1_{f,\{p\}}(F,T) \subseteq H^1_{\mathcal{M}}(F,T)$ and $\Psi_{\mathcal{M}}(x)$ is of finite order, then x lies in the left-hand kernel of the pairing B_F.*

Hence if the pairing $\langle\langle\ ,\ \rangle\rangle$ is non-degenerate modulo torsion, and if $H^0(F,T) = 0$, then $x \in \mathfrak{G}_F(T)$ only if $\Psi_{\mathcal{M}}(x)$ is of finite order.

Remark 1.1. It would be interesting if one could show directly (without, of course, assuming the non-degeneracy of the pairing (1.6)!) that the left-hand kernel of the pairing B_F is precisely equal to the set of all $x \in H^1_{f,\{p\}}(F,T)$ such that $\Psi_{\mathcal{M}}(x)$ has finite order. This would imply that the non-degeneracy modulo torsion of the pairing $\langle\langle\ ,\ \rangle\rangle$ is equivalent to the statement that $x \in \mathfrak{G}_F(T)$ if and only if $\Psi_{\mathcal{M}}(x)$ is of finite order. Unfortunately we do not know how to do this at present. □

Let S be a finite set of places of F containing the places lying over p, the places at which ρ is ramified, and the set of infinite places. Let F^S/F denote the maximal extension of F which is unramified outside S. A conjecture of Greenberg asserts that the group $H^2(F^S/C_\infty, V^*/T^*)$ always vanishes. This may be viewed as an analogue of a weak form of Leopoldt's conjecture for the Galois representation V^*.

Theorem C. *Suppose that the pairing $\langle\langle\ ,\ \rangle\rangle$ is non-degenerate modulo torsion, and that*

$$H^2(F^S/C_\infty, V^*/T^*) = 0. \tag{1.7}$$

Suppose also that $H^0(F,T) = 0$. Then the restriction of $\Psi_{\mathcal{M}}$ to $\mathrm{Ker}(\mathrm{Loc}_{F,T})$ has finite kernel.

Proof. It follows from [24, Remark at the end of §3.4.2] that if (1.7) holds, then $\mathfrak{G}_F(T) \cap \mathrm{Ker}(\mathrm{Loc}_{F,T})$ is finite. The result now follows from Theorem B. □

Acknowledgements. This paper owes a great deal to ideas first introduced in [6], and I am extremely grateful to G. Pappas for many interesting and helpful conversations. I would like to thank T. Chinburg, B. Conrad, R. Greenberg and S. Howson for useful discussions. I would also like to thank the Mathematics Departments of Harvard University, Humboldt University and the Université de Bordeaux I for their hospitality while parts of this work were carried out. This research was partially supported by NSA and NSF grants. I am also very grateful to the ALGANT consortium for financial support while this paper was being written.

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, and we set $\mathcal{R}_L := O_L[1/p]$.

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. Relative K-groups and twisted forms

In this section we shall first recall certain basic results concerning categorical twisted forms and relative algebraic K-groups. We refer the reader to

[5] and [30, Chapter 15] for some of the details that we omit. We then use these results to generalise the class invariant map of [35].

Suppose that R is a Dedekind domain with field of fractions L of characteristic zero, and write R^c for the integral closure of R in L. (For notational convenience, we shall sometimes also allow ourselves to take $R = L$, in which case the symbol R^c refers to an algebraic closure L^c of L.) Let $\mathfrak{A}$ be any commutative R-algebra and set $A := \mathfrak{A} \otimes_R L$.

Definition 2.1. Let Λ be any extension of R, and write $\mathcal{P}(\mathfrak{A})$ and $\mathcal{P}(\mathfrak{A} \otimes_R \Lambda)$ for the categories of finitely generated, projective $\mathfrak{A}$ and $\mathfrak{A} \otimes_R \Lambda$-modules respectively. A *categorical Λ-twisted $\mathfrak{A}$-form* (or *twisted form* for short) is an element of the fibre product category $\mathcal{P}(\mathfrak{A}) \times_{\mathcal{P}(\mathfrak{A} \otimes_R \Lambda)} \mathcal{P}(\mathfrak{A})$, where the fibre product is taken with respect to the functor $\mathcal{P}(\mathfrak{A}) \to \mathcal{P}(\mathfrak{A} \otimes_R \Lambda)$ afforded by extension of scalars. In concrete terms, therefore, a twisted form consists of a triple $(M, N; \xi)$, where M and N are finitely generated, projective $\mathfrak{A}$-modules, and

$$\xi : M \otimes_R \Lambda \xrightarrow{\sim} N \otimes_R \Lambda$$

is an isomorphism of $\mathfrak{A} \otimes_R \Lambda$-modules. □

Example 2.2. In this paper we shall mainly be concerned with twisted forms of the following type.

Let $Y = \mathrm{Spec}(R)$, and let $G \to Y$ be a finite, flat, commutative group scheme. Write $G^D = \mathrm{Spec}(\mathfrak{A})$ for the Cartier dual of G, and set $\Gamma := G(R^c)$.

Recall that there is a canonical isomorphism

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

(see [35], [16, éxposé VII], or [23]); this explained in some detail by Waterhouse in [35].)

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

$$X \otimes_R R^c \simeq G \otimes_R R^c \tag{2.1}$$

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 [35], the isomorphism (2.1) induces an isomorphism

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

We shall refer to ξ_π as a *splitting isomorphism* for π

We see from the definitions that $(\mathcal{L}_\pi, \mathfrak{A}; \xi_\pi)$ is a categorical R^c-twisted $\mathfrak{A}$-form. □

We write $K_0(\mathfrak{A}, \Lambda)$ for the Grothendieck group associated to the fibre product category $\mathcal{P}(\mathfrak{A}) \times_{\mathcal{P}(\mathfrak{A} \otimes_R \Lambda)} \mathcal{P}(\mathfrak{A})$, and we write $[M, N; \xi]$ for the isomorphism class of the twisted form $(M, N; \xi)$ in $K_0(\mathfrak{A}, \Lambda)$. Recall (see [30, Theorem 15.5] that there is a long exact sequence of relative algebraic K-theory:

$$K_1(\mathfrak{A}) \to K_1(\mathfrak{A} \otimes_R \Lambda) \xrightarrow{\partial^1_{\mathfrak{A},\Lambda}} K_0(\mathfrak{A}, \Lambda) \xrightarrow{\partial^0_{\mathfrak{A},\Lambda}} K_0(\mathfrak{A}) \to K_0(\mathfrak{A} \otimes_R \Lambda). \tag{2.2}$$

The first and last arrows in this sequence are afforded by extension of scalars from R to Λ. The map $\partial^0_{\mathfrak{A},\Lambda}$ is defined by

$$\partial^0_{\mathfrak{A},\Lambda}([M, N; \lambda]) = [M] - [N].$$

The map $\partial^1_{\mathfrak{A},\Lambda}$ is defined by first recalling that the group $K_1(\mathfrak{A} \otimes_R \Lambda)$ is generated by pairs of the form (W, ϕ), where W is a finitely generated, free, $\mathfrak{A} \otimes_R \Lambda$-module, and $\phi : W \xrightarrow{\sim} W$ is an $\mathfrak{A} \otimes_R \Lambda$-isomorphism. If Q is any projective $\mathfrak{A}$-submodule of W satisfying $Q \otimes_{\mathfrak{A}} \Lambda \simeq W$, then we set

$$\partial^1_{\mathfrak{A},\Lambda}(W, \phi) = [Q, Q; \phi].$$

It may be shown that this definition is independent of the choice of Q.

We shall often ease notation and write e.g. ∂^0 rather than $\partial^0_{\mathfrak{A},\Lambda}$ when no confusion is likely to result.

2.1. **Idelic description and localisation.** Let us retain the notation established above, and suppose in addition that L is a number field. For each finite place v of L, we write

$$\mathrm{loc}_v : A^\times \to A_v^\times$$

for the obvious localisation map.

Definition 2.3. We define the idele group $J(A)$ of A to be the restricted direct product of the groups $A_v^\times$ with respect to the subgroups $\mathfrak{A}_v^\times$ for all finite places v of L. (The group $J(A)$ does not depend upon $\mathfrak{A}$ because $\mathfrak{A}_v$ is an O_{L_v}-maximal order in A_v for almost all v.) □

Let $\mathrm{Cl}(\mathfrak{A})$ denote the locally free class group of $\mathfrak{A}$.

Theorem 2.4. *There is a natural isomorphism*

$$\mathrm{Cl}(\mathfrak{A}) \simeq \frac{J(A)}{A^\times \cdot \prod_v \mathfrak{A}_v^\times}.$$

Proof. See [31, Chapter I], for example.

If M is a locally free rank one $\mathfrak{A}$-module, then an element of $J(A)$ representing the class of M may be constructed as follows. We choose an A-basis m_∞ of M_L, and for each finite place v of L, we choose an $\mathfrak{A}_v$-basis of M_v. Then we may write $m_\infty = \alpha_v \cdot m_v$, with $\alpha_v \in A_v$. The idele $(\alpha_v)_v \in J(A)$ is then a representative of the class of M. □

If E is any extension of L, then the homomorphism

$$A^\times \to J(A) \times A_E^\times; \quad x \mapsto ((\mathrm{loc}_v(x))_v, x^{-1})$$

induces a homomorphism

$$\Delta_{\mathfrak{A},E} : A^\times \to \frac{J(A)}{\prod_v \mathfrak{A}_v^\times} \times A_E^\times.$$

The following result is proved in [5, Theorem 3.5].

Theorem 2.5. *There is a natural isomorphism*

$$h_{\mathfrak{A},E} : K_0(\mathfrak{A}, E) \xrightarrow{\sim} \mathrm{Coker}(\Delta_{\mathfrak{A},E}).$$

□

If $[M, N; \xi] \in K_0(\mathfrak{A}, E)$ and M, N are locally free $\mathfrak{A}$-modules of rank one (which is the only case that we shall need in this paper), then $h_{\mathfrak{A},E}([M, N; \lambda])$ may be described as follows.

For each finite place v of L, we choose $\mathfrak{A}_v$-bases m_v of M and n_v of N. We also choose an A basis n_∞ of N_L, as well as an A-module isomorphism $\theta : M_L \xrightarrow{\sim} N_L$. Then, for each v, we may write $n_v = \nu_v \cdot n_\infty$, wth $\nu_v \in A_v^\times$. As $\theta^{-1}(n_\infty)$ is an A-basis of M_L, we may write $m_v = \mu_v \cdot \theta^{-1}(n_\infty)$, with $\mu_v \in A_v^\times$. Finally, writing θ_E for the map $M_E \to N_E$ afforded by θ via extension of scalars from L to E, we have that $(\theta_E^{-1} \circ \xi)(n_\infty) = \nu_\infty \cdot n_\infty$ for some $\nu_\infty \in A_E^\times$. Then a representative of $h_{\mathfrak{A},E}([M, N; \lambda])$ is given by the image of $[(\mu_v \cdot \nu_v^{-1})_v, \nu_\infty]$ in $J(A) \times K_1(A_E)$.

Example 2.6. Let us make the above description more explicit in the situation considered in Example 2.2. The element $[\mathcal{L}_\pi, \mathfrak{A}; \xi_\pi] \in K_0(\mathfrak{A}, L^c)$ may be described as follows.

We first observe that $\mathcal{L}_{\pi,F}$ and $\mathcal{L}_{\pi_v}$ (for each finite place v of L) are free A and $\mathfrak{A}_v$-modules respectively, and so we may choose trivialisations

$$s_\pi : A \xrightarrow{\sim} \mathcal{L}_{\pi,L}, \quad s_{\pi_v} : \mathfrak{A}_v \xrightarrow{\sim} \mathcal{L}_{\pi_v}.$$

Then the compositions

$$A_{L^c} \xrightarrow{s_\pi \otimes L^c} \mathcal{L}_{\pi,L^c} \xrightarrow{\xi_\pi \otimes L^c} A_{L^c}$$
$$A_{L_v^c} \xrightarrow{s_{\pi_v} \otimes L_v^c} \mathcal{L}_{\pi,L_v^c} \xrightarrow{\xi_\pi \otimes L_v^c} A_{L_v^c}$$

are isomorphisms of A_{L^c} and $A_{L_v^c}$-modules respectively, and so are given by multiplication by elements $r(s_\pi) \in A_{L^c}^\times$ and $r(s_{\pi_v}) \in A_{L_v^c}^\times$ respectively. The elements $r(s_\pi)$ and $r(s_{\pi_v})$ are called the *resolvends* of s_π and s_{π_v} —this terminology is due to L. McCulloh, [20]. (Note that the resolvends depend upon the choice of splitting isomorphism ξ_π as well as upon the choice of trivialisation; we shall usually not make the dependence upon the choice of ξ_π explicit.) If $\omega \in \Omega_L$, then $\xi_\pi^\omega = g_\omega \cdot \xi_\pi$ for some $g_\omega \in \Gamma$. As $s_\pi^\omega = s_\pi$, it follows that $r(s_\pi)^\omega = g_\omega \cdot r(s_\pi)$. The cohomology class in $H^1(L,\Gamma)$ of the cocycle $\omega \mapsto g_\omega$ is equal to the image of π under the natural injection $H^1(O_F, G) \to H^1(F,\Gamma)$. Similar remarks apply to the resolvend $r(s_{\pi_v})$.

The element $[\mathcal{L}_\pi, \mathfrak{A}; \xi_\pi] \in K_0(\mathfrak{A}, L^c)$ is represented by

$$\left[\prod_v (r(s_{\pi_v}) \cdot r(s_\pi)^{-1})\right] \times r(s_\pi) \in J(A) \times A_{F^c}^\times.$$

□

Definition 2.7. Suppose that Γ is any finite abelian group on which Ω_L acts, and that A is any L-algebra such that $A_{L^c} = L^c\Gamma$. We set

$$\mathbf{H}(A) := \{\alpha \in A_{L^c} \mid \alpha^\omega \cdot \alpha^{-1} \in \Gamma \quad \text{for each } \omega \in \Omega_L\}.$$

If $\mathfrak{A} \subset A$ is any R-algebra, we set

$$\mathbf{H}(\mathfrak{A}) := \mathfrak{A}_{R^c}^\times \cap \mathbf{H}(A).$$

Each $x \in \mathbf{H}(A)$ yields an element $\pi \in H(L,\Gamma)$ given by the class of the Γ-valued Ω_F-cocycle $\omega \to x^\omega x^{-1}$ ($\omega \in \Omega_F$) in $H^1(L,\Gamma)$. We say that x *is a resolvend associated to* π.

If $\pi \in H^1(L, \Gamma)$, then we shall often write $r(\pi)$ for a resolvend associated to π. □

Lemma 2.8. *Suppose that R is a local ring, and that Λ is an extension of R. Then there is an isomorphism*

$$K_0(\mathfrak{A}, \Lambda) \simeq \mathfrak{A}_\Lambda^\times / \mathfrak{A}^\times.$$

Proof. This follows directly from the long exact sequence of relative K-theory (2.2) applied to $K_0(\mathfrak{A}, \Lambda)$.) □

Recall that E is any extension of L. For each finite place v of L, there is a localisation map on relative K-groups:

$$\lambda_v : K_0(\mathfrak{A}, E) \to K_0(\mathfrak{A}_v, E_v); \quad [M, N; \xi] \mapsto [M_v, N_v; \xi_v],$$

where ξ_v denotes the map obtained from ξ via extension of scalars from E to E_v. It is not hard to check that, in terms of the descriptions of $K_0(\mathfrak{A}, E)$ and $K_0(\mathfrak{A}_v, E_v)$ afforded by Theorem 2.5 and Lemma 2.8, the map λ_v is that induced by the homomorphism (which we denote by the same symbol λ_v)

$$\lambda_v : J(A) \times A_E^\times \to A_{E_v}^\times; \quad [(x_v)_v, x_\infty] \mapsto [x_v \cdot \mathrm{loc}_v(x_\infty)].$$

2.2. **Local conditions: relative K-groups.** We continue to assume that L is a number field. We now explain how to impose local conditions on elements of $K_0(A, L^c)$ in terms of $\mathfrak{A}$.

Definition 2.9. (a) For each finite place v of L, we define $K_0(A_v, L_v^c)_{\mathfrak{A}_v}$ to be the image of the homomorphism

$$K_0(\mathfrak{A}_v, O_{L_v^c}) \to K_0(A_v, L^c); \quad [M, N; \xi] \mapsto [M_L, N_L; \xi \otimes L^c].$$

Thus, in terms of the isomorphisms

$$K_0(\mathfrak{A}_v, O_{L_v^c}) \simeq \mathfrak{A}_{O_{L_v^c}}^\times / \mathfrak{A}_v^\times, \quad K_0(A_v, L_v^c) \simeq A_{L_v^c}^\times / A_v^\times$$

afforded by Lemma 2.8, we have

$$\begin{aligned} K_0(A_v, L_v^c)_{\mathfrak{A}_v} &\simeq \mathrm{Im}[\mathfrak{A}_{O_{L_v^c}}^\times / \mathfrak{A}_v^\times \to A_{L_v^c}^\times / A_v^\times] \\ &\simeq [\mathfrak{A}_{O_{L_v^c}}^\times \cdot A_v^\times]/A_v^\times. \end{aligned}$$

(b) We define $K_0(A, L^c)_{\mathfrak{A}}$ by

$$K_0(A, L^c)_{\mathfrak{A}} := \{x \in K_0(A, L^c) \mid \lambda_v(x) \in K_0(A_v, L_v^c)_{\mathfrak{A}_v} \quad \text{for each } v\}.$$

□

Definition 2.10. We now define a homomorphism

$$\nu = \nu_{\mathfrak{A}} : K_0(A, L^c)_{\mathfrak{A}} \to \mathrm{Cl}(\mathfrak{A}).$$

We first note that Lemma 2.8 implies that

$$K_0(A, L^c) \simeq A_{L^c}^\times / A^\times.$$

Suppose that $x \in K_0(A, L^c)_{\mathfrak{A}}$, and let $a_x \in A_{L^c}^\times$ be a representative of x. Then, for each place v, there exists $\alpha_{x,v} \in A_v^\times$ such that $\alpha_{x,v} \cdot a_x \in \mathfrak{A}_{O_{L_v^c}}^\times$. If also $\beta_{x,v} \in A_v^\times$ satisfies $\beta_{x,v} \cdot a_x \in \mathfrak{A}_{O_{L_v^c}}^\times$, then

$$\alpha_{x,v} \cdot \beta_{x,v}^{-1} \in (\mathfrak{A}_{O_{L_v^c}}^\times)^{\Omega_{L_v}} \subseteq \mathfrak{A}_v^\times.$$

It follows that the idele $(\alpha_{x,v})_v \in J(A)$ gives a well-defined element $[(\alpha_{x,v})_v] \in \mathrm{Cl}(\mathfrak{A})$ via Theorem 2.4. We set $\nu(x) := [(\alpha_{x,v})_v]$. □

Proposition 2.11. *There is an exact sequence*

$$1 \to [\mathfrak{A}_{O_{L^c}}^\times \cdot A^\times]/A^\times \to K_0(A, L^c)_{\mathfrak{A}} \xrightarrow{\nu} \mathrm{Cl}(\mathfrak{A}).$$

Proof. Suppose that $\nu(x) = 0$, and let $a \in A_{L^c}^\times$ be a representative of x. Then, using the notation established in Definition 2.10, we have that $(\alpha_{x,v})_v \in A^\times \cdot \prod_v \mathfrak{A}_v^\times$ and that $\alpha_{x,v} \cdot a_x \in \mathfrak{A}_{O_{L_v}}^\times$ for each v. Hence there exists $a \in A^\times$ such that $\mathrm{loc}_v(a \cdot a_x) \in \mathfrak{A}_{O_{L_v}}^\times$ for each v. This implies that $a \cdot a_x \in \mathfrak{A}_{O_{L^c}}^\times$, and so establishes the result. □

2.3. **Local conditions: cohomology groups.** We now identify $K_0(A, L^c)$ with $A_{L^c}^\times/A^\times$ via Lemma 2.8, and we set

$$\bar{K}_0(A, L^c) := A_{L^c}^\times/[\Gamma \cdot A^\times].$$

Let $\bar{K}_0(A, L^c)_{\mathfrak{A}}$ denote the image of $K_0(A, L^c)_{\mathfrak{A}}$ in $\bar{K}_0(A, L^c)$. It is easy to check that the homomorphism $\nu : K_0(A, L^c)_{\mathfrak{A}} \to \mathrm{Cl}(\mathfrak{A})$ induces a homomorphism (which we shall denote by the same symbol) $\nu : \bar{K}_0(A, L^c)_{\mathfrak{A}} \to \mathrm{Cl}(\mathfrak{A})$.

Recall the notation established in Example 2.2. It is shown in [5, Theorem 6.9] that if $\pi \in H^1(L, \Gamma)$, then the image of $[\mathcal{L}_\pi, A; \xi_\pi] \in K_0(A, L^c)$ in $\bar{K}_0(A, L^c)$ depends only upon π, and that the map

$$\hat{\psi}_A : H^1(L, \Gamma) \to \bar{K}_0(A, L^c); \quad \pi \mapsto [\mathcal{L}_\pi, A; \xi_\pi]$$

is an injective group homomorphism. We have that

$$\hat{\psi}_A(\pi) = [r_\pi] \in \frac{A_{L^c}^\times}{\Gamma \cdot A^\times}, \tag{2.3}$$

where r_π is any resolvend associated to π (see Definition 2.7).

Definition 2.12. (a) For each finite place v of L, we define $H^1_{\mathfrak{A}_v}(L_v, \Gamma) \subseteq H^1(L_v, \Gamma)$ by

$$H^1_{\mathfrak{A}_v}(L_v, \Gamma) := \hat{\psi}_{A_v}^{-1}[\bar{K}_0(A_v, L_v^c)_{\mathfrak{A}_v} \cap \mathrm{Im}(\hat{\psi}_{A_v})]$$

(b) We define $H^1_{\mathfrak{A}}(L, \Gamma) \subseteq H^1(L, \Gamma)$ by

$$H^1_{\mathfrak{A}}(L, \Gamma) := \hat{\psi}_A^{-1}[\bar{K}_0(A, L^c)_{\mathfrak{A}} \cap \mathrm{Im}(\hat{\psi}_A)].$$

It therefore follows from the definitions that we have

$$H^1_{\mathfrak{A}}(L, \Gamma) = \mathrm{Ker}\left[H^1(L, \Gamma) \to \prod_v \frac{H^1(L_v, \Gamma)}{H^1_{\mathfrak{A}_v}(L_v, \Gamma)}\right].$$

(c) We write

$$\hat{\psi}_{\mathfrak{A}_v} : H^1_{\mathfrak{A}_v}(L_v, \Gamma) \to \bar{K}_0(A_v, L_v^c)_{\mathfrak{A}_v}$$

for the restriction of $\hat{\psi}_{A_v}$ to $H^1_{\mathfrak{A}_v}(L_v, \Gamma)$,

$$\hat{\psi}_{\mathfrak{A}} : H^1_{\mathfrak{A}}(L, \Gamma) \to \bar{K}_0(A, L^c)_{\mathfrak{A}}$$

for the restriction of $\hat{\psi}_A$ to $H^1_{\mathfrak{A}}(L, \Gamma)$, and

$$\psi_{\mathfrak{A}} : H^1_{\mathfrak{A}}(L, \Gamma) \to \mathrm{Cl}(\mathfrak{A})$$

for the composition of $\hat{\psi}_{\mathfrak{A}}$ with the homomorphism $\nu : \bar{K}_0(A, L^c)_{\mathfrak{A}} \to \mathrm{Cl}(\mathfrak{A})$. □

Remark 2.13. Let us place ourselves in the setting considered in Examples 2.2 and 2.6. Unwinding the definitions shows that

$$H^1_{\mathfrak{A}}(L, \Gamma) = \mathrm{Im}[H^1(O_L, G) \to H^1(L, \Gamma)],$$

and that the homomorphism

$$\hat{\psi}_{\mathfrak{A}} : H^1_{\mathfrak{A}}(L, \Gamma) \to \bar{K}_0(\mathfrak{A}, L^c)_{\mathfrak{A}} \subseteq \bar{K}_0(A, L^c)$$

is the same as that obtained by composing the refined class invariant homomorphism $H^1(O_F, G) \to \bar{K}_0(\mathfrak{A}, L^c)$ introduced in [5] with the natural homomorphism $\bar{K}_0(\mathfrak{A}, L^c) \to \bar{K}_0(A, L^c)$. We see therefore that the homomorphism $\psi_{\mathfrak{A}}$ that we have constructed is a generalisation of Waterhouse's class invariant map in [35]. □

2.4. **Functorial Properties.**

Proposition 2.14. *Let L be a number field, and let v be any finite place of L.*

(a) There are isomorphisms

$$H^1(L, \Gamma) \simeq \frac{\mathbf{H}(A)}{\Gamma \cdot A^\times}, \quad H^1(L_v, \Gamma) \simeq \frac{\mathbf{H}(A_v)}{\Gamma \cdot A_v^\times};$$

$$H^1_{\mathfrak{A}_v}(L_v, \Gamma) \simeq \frac{\mathbf{H}(\mathfrak{A}_v)}{\Gamma \cdot \mathfrak{A}_v^\times},$$

induced by $\hat{\psi}_A$, $\hat{\psi}_{A_v}$, *and* $\hat{\psi}_{\mathfrak{A}_v}$ *respectively.*

(b) There is an exact sequence

$$1 \to [\mathbf{H}(\mathfrak{A}) \cdot A^\times]/[\Gamma \cdot A^\times] \to H^1_{\mathfrak{A}}(L, \Gamma) \xrightarrow{\psi_{\mathfrak{A}}} \mathrm{Cl}(\mathfrak{A}).$$

Hence we have that

$$\mathrm{Ker}(\psi_{\mathfrak{A}}) \simeq \frac{\mathbf{H}(\mathfrak{A})}{\Gamma \cdot \mathfrak{A}^\times}.$$

Proof. This follows from Lemma 2.8, Proposition 2.11, and the definitions of the relevant maps $\hat{\psi}_?$ and $\psi_?$. □

Corollary 2.15. *Suppose that* Γ *is of exponent* N*. Then there is a homomorphism*

$$\eta_A : H^1(L, \Gamma) \to \frac{A^\times}{A^{\times N}}; \quad [\pi] \mapsto [r(\pi)^N].$$

There are similar homomorphisms

$$\eta_{\mathfrak{A}_v} : H^1_{\mathfrak{A}_v}(L_v, \Gamma) \to \frac{\mathfrak{A}_v^\times}{\mathfrak{A}_v^{\times N}}$$

for each finite place v *of* L*, and*

$$\eta_{\mathfrak{A}} : \mathrm{Ker}(\psi_{\mathfrak{A}}) \to \frac{\mathfrak{A}^\times}{\mathfrak{A}^{\times N}}.$$

Proof. Follows directly from Proposition 2.14. □

Set

$$\Gamma^* := \mathrm{Hom}(\Gamma, \mu_N).$$

Remark 2.16. 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 [1, Lemma 3.3], it may be shown that the Wedderburn decomposition of the L-algebra A is given by

$$A \simeq (L^c\Gamma)^{\Omega_L} \simeq \prod_{\gamma^* \in \Omega_L \backslash \Gamma^*} L[\gamma^*]. \tag{2.4}$$

There is an isomorphism of L-algebras

$$\mathrm{Map}(\Gamma^*, L^c)^{\Omega_L} \simeq \prod_{\gamma^* \in \Omega_L \backslash \Gamma^*} L[\gamma^*]; \quad f \mapsto (f(\gamma^*))_{\gamma^* \in \Omega_L \backslash \Gamma^*}, \tag{2.5}$$

and we may identify A with $\mathrm{Map}(\Gamma^*, L^c)^{\Omega_L}$ via (2.4) and (2.5) □

We shall now explain the relationship between the homomorphism η_A of Proposition 2.14 and the Kummer theory of the Wedderburn components of A.

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

$$\mathrm{ev}_{\gamma^*} : A^\times \to L[\gamma^*]^\times \tag{2.6}$$

for the map $a \mapsto a(\gamma^*)$ afforded by (2.4) and (2.5) given by 'evaluation at γ^*'. The following result describes the homorphism η_A of Proposition 2.14 in terms of Kummer theory.

Proposition 2.17. *Let the hypotheses and notation be as above. Then the following diagram is commutative:*

$$\begin{array}{ccc} H^1(L,\Gamma) & \xrightarrow{\gamma^*} & H^1(L[\gamma^*],\mu_N) \\ {\scriptstyle \eta_A}\downarrow & & \uparrow{\scriptstyle \text{Kummer}} \\ A^\times/A^{\times N} & \xrightarrow{\mathrm{ev}_{\gamma^*}} & L[\gamma^*]^\times/L[\gamma^*]^{\times N}. \end{array} \tag{2.7}$$

(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 [6, Proposition 3.2]. □

Proposition 2.18. *Let E be any algebraic extension of L. Then the following diagram is commutative:*

$$\begin{array}{ccc} H^1(L,\Gamma) & \xrightarrow{\hat{\psi}_A} & K_0(A,L^c) \\ {\scriptstyle \mathrm{Res}}\downarrow & & \downarrow{\scriptstyle i} \\ H^1(E,\Gamma) & \xrightarrow{\hat{\psi}_{A_E}} & K_0(A_E,E^c). \end{array} \tag{2.8}$$

Here the left-hand vertical arrow is the restriction map on cohomology, and the right-hand vertical arrow is the homomorphism induced by the inclusion map $i : A \to A_E$.

Proof. If $\pi \in H^1(L,\Gamma)$ and $r(\pi) \in \mathbf{H}(A)$ is any resolvend associated to π, then the Ω_E-cocycle defined by $i(r(\pi))$ is equal to the restriction of the Ω_L-cocycle defined by $r(\pi)$. This implies that the diagram commutes. □

Remark 2.19. Suppose that $\pi \in \mathrm{Ker}(\eta_A)$. Let $r(\pi) \in \mathbf{H}(A)$ be any resolvend associated to π. Then $r(\pi)^N = \alpha^N \in A^{\times N}$ for some $\alpha \in A^\times$. Hence $\alpha^{-1}r(\pi) \in A^\times_{L(\mu_N)}$, and so Proposition 2.18 implies that π lies in the kernel of the restriction map

$$\mathrm{Res}_{L/L(\mu_N)} : H^1(L,\Gamma) \to H^1(L(\mu_N),\Gamma).$$

Conversely, if $\pi \in \mathrm{Res}_{L/L(\mu_N)}$, then, since π is trivialised over $L(\mu_N)$, it follows that $r(\pi) \in A^\times_{L(\mu_N)}$ for any choice of $r(\pi)$. We therefore deduce from Corollary 2.15 that $r(\pi)^N \in A^\times \cap A^{\times N}_{L(\mu_N)}$. Hence, if $A^{\times N} = A^\times \cap A^{\times N}_{L(\mu_N)}$, then $r(\pi)^N \in A^{\times N}$, and so $\pi \in \mathrm{Ker}(\eta_A)$. □

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

$$\mathcal{N}_{E/L} : A^\times_{E^c} \to A^\times_{L^c}; \qquad a \mapsto \prod_{i=1}^{n} a^{\omega_i}. \tag{2.9}$$

This induces a homomorphism (which we denote by the same symbol):

$$\mathcal{N}_{E/L} : K_0(A_E, E^c) \to K_0(A, L^c).$$

Proposition 2.20. *The following diagram is commutative:*

$$\begin{array}{ccc} H^1(E,\Gamma) & \xrightarrow{\hat{\psi}_{A_E}} & K_0(A,E^c) \\ {\scriptstyle \mathrm{Cores}_{E/L}}\downarrow & & \downarrow{\scriptstyle \mathcal{N}_{E/L}} \\ H^1(L,\Gamma) & \xrightarrow{\hat{\psi}_{A}} & K_0(A,L^c), \end{array} \tag{2.10}$$

where the left-hand vertical arrow is the corestriction map on cohomology.

Proof. If $\pi \in H^1(E,\Gamma)$ and $r(\pi) \in \mathbf{H}(A_E)$ is any resolvend associated to π, then it follows via a routine computation that the Ω_L-cocycle associated to $\mathcal{N}_{E/L}(r(\pi))$ is equal to the corestriction of the Ω_E-cocycle associated to $r(\pi)$. This implies that the diagram commutes. □

3. Class invariants and p-adic representations

We now explain how the results of Section 2 may be used to construct class invariants associated to certain Selmer groups attached to p-adic representations.

Let F be a number field, and let V be a d-dimensional $\mathbf{Q}_p$-vector space. Suppose that $\rho : \Omega_F \to \mathrm{GL}(V)$ is a continuous representation that is ramified at only finitely many places of F. Let $T \subset V$ be an Ω_F-stable $\mathbf{Z}_p$-lattice.

For each integer $n \geq 1$, we set

$$\Gamma_n := p^{-n}T/T, \quad A_n := (F^c\Gamma_n)^{\Omega_F}.$$

The algebra A_n depends upon the choice of T, and when we need to indicate this dependence we shall write $A_n(T)$ instead of just A_n. We set

$$A = A(T) := \varprojlim A_n,$$

where the inverse limit is taken with repect to the maps $A_n \to A_{n-1}$ induced by the multiplication-by-p map $[p] : \Gamma_n \to \Gamma_{n-1}$. It is easy to check that $[p]$ induces a homomorphism $\mathbf{H}(A_n) \to \mathbf{H}(A_{n-1})$ on resolvends, and that this in turn implies that the following diagram commutes:

$$\begin{array}{ccc} H^1(F,\Gamma_n) & \xrightarrow{\hat{\psi}_{A_n}} & \bar{K}_0(A_n,F^c) \\ {\scriptstyle [p]}\downarrow & & {\scriptstyle [p]}\downarrow \\ H^1(F,\Gamma_{n-1}) & \xrightarrow{\hat{\psi}_{A_{n-1}}} & \bar{K}_0(A_{n-1},F^c). \end{array}$$

For each $n \geq 1$, suppose that $\mathfrak{A}_n \subseteq A_n$ is an O_F-algebra such that $[p](\mathfrak{A}_n) \subseteq \mathfrak{A}_{n-1}$. It is not hard to check that the following diagram commutes:

$$\begin{array}{ccccc} H^1_{\mathfrak{A}_n}(F,\Gamma_n) & \xrightarrow{\hat{\psi}_{\mathfrak{A}_n}} & \bar{K}_0(A_n,F^c)_{\mathfrak{A}_n} & \xrightarrow{\nu_n} & \mathrm{Cl}(\mathfrak{A}_n) \\ \downarrow & & \downarrow & & \downarrow \\ H^1_{\mathfrak{A}_{n-1}}(F,\Gamma_{n-1}) & \xrightarrow{\hat{\psi}_{\mathfrak{A}_{n-1}}} & \bar{K}_0(A_{n-1},F^c)_{\mathfrak{A}_{n-1}} & \xrightarrow{\nu_{n-1}} & \mathrm{Cl}(\mathfrak{A}_{n-1}) \end{array}$$

We set

$$\begin{aligned} &\mathfrak{A} = \mathfrak{A}(T) = \varprojlim \mathfrak{A}_n; \\ &H^1_{\mathfrak{A}}(F,T) := \varprojlim H^1_{\mathfrak{A}_n}(F,\Gamma_n); \\ &\bar{K}_0(A,F^c) := \varprojlim \bar{K}_0(A_n,F^c), \quad \bar{K}_0(A,F^c)_{\mathfrak{A}} := \varprojlim \bar{K}_0(A_n,F^c)_{\mathfrak{A}_n}; \\ &\mathrm{Cl}(\mathfrak{A}) := \varprojlim \mathrm{Cl}(\mathfrak{A}_n); \\ &\hat{\Psi}_{\mathfrak{A}} := \varprojlim \hat{\psi}_{\mathfrak{A}_n} : H^1_{\mathfrak{A}}(F,T) \to \bar{K}_0(A,F^c)_{\mathfrak{A}}; \\ &\Psi_{\mathfrak{A}} := \varprojlim \psi_{\mathfrak{A}_n} : H^1_{\mathfrak{A}}(F,T) \to \mathrm{Cl}(\mathfrak{A}), \end{aligned}$$

where all inverse limits are taken with respect to the maps induced by

$$[p] : \Gamma_n \to \Gamma_{n-1}.$$

We write $\mathfrak{M}_n$ for the (unique) O_F-maximal order in A_n.

Remark 3.1. If v is a place of F with $v \nmid p$, set

$$H^1_f(F_v, \Gamma_n) := \mathrm{Ker}\left[H^1(F_v, \Gamma_n) \to H^1(F_v^{\mathrm{nr}}, \Gamma_n)\right],$$

where F_v^{nr} is the maximal unramified extension of F_v in a fixed algebraic closure of F_v.

If $\pi_v \in H^1_f(F_v, \Gamma_n)$, and $r(s_{\pi_v})$ is any resolvend associated to π_v, then $r(s_{\pi_v}) \in A^{\times}_{n, F_v^{\mathrm{nr}}}$, because π_v is becomes trivial over F_v^{nr}. Since $F_v^{\mathrm{nr}}/F_{n,v}$ is unramified, it follows that there exists $\alpha \in A^{\times}_{n,v}$ such that $\alpha^{-1} r(s_{\pi_v}) = r(\alpha^{-1} s_{\pi_v}) \in \mathfrak{M}^{\times}_{n, O_{F_v^{\mathrm{nr}}}}$. This implies that $\pi_v \in H^1_{\mathfrak{M}_v}(F, \Gamma)$, and so

$$H^1_f(F_v, \Gamma_n) \subseteq H^1_{\mathfrak{M}_v}(F_v, \Gamma_n).$$

Suppose further that the action of Ω_{F_v} on Γ_n is unramified. Then $\mathcal{G}_{n,v} := \mathrm{Spec}(\mathfrak{M}_{n,v})$ is a finite, flat, commutative, O_{F_v}- group scheme , and it is a standard result that $H^1_f(F_v, \Gamma_n) = H^1(O_{F_v}, \mathcal{G}_{n,v})$. Hence, in this case, we see that $H^1_f(F_v, \Gamma_n) = H^1_{\mathfrak{M}_{n,v}}(F_v, \Gamma_n)$. □

Definition 3.2. If $v \nmid p$, then define

$$H^1_f(F_v, T) := \mathrm{Ker}\left[H^1(F_v, T) \to H^1(F_v^{\mathrm{nr}}, T)\right], \tag{3.1}$$

and set (following [24, §3.1.4]):

$$H^1_{f,\{p\}}(F, T) = \mathrm{Ker}\left[H^1(F, T) \to \oplus_{v \nmid p} \frac{H^1(F_v, T)}{H^1_f(F_v, T)}\right].$$

We see from Remark 3.1 that

$$H^1_{f,\{p\}}(F, T) \subseteq H^1_{\mathcal{M}}(F, T).$$

□

Remark 3.3. In order to ease notation in what follows, we shall frequently write $\Psi_T^{\{p\}}$ instead of $\Psi_{\mathcal{M}}$. We shall also write $\Psi_{T,f}^{\{p\}}$ for the restriction of $\Psi_{\mathcal{M}}$ to the subgroup $H^1_f(F, T)$ of $H^1_{\mathfrak{M}}(F, T)$. □

4. Proof of Theorem A

In this section, we shall prove Theorem A of the Introduction.

Recall that C_m/F denotes the m-th layer of the cyclotomic $\mathbf{Z}_p$-extension of F. It follows from the definition of $\mathfrak{G}_F(T)$ that Theorem A will follow if we show that, for any $x \in \cap_m \mathrm{Cores}_{F_m/F} H^1_{f,\{p\}}(F_m, T)$, we have $\Psi_T^{\{p\}}(x) = 0$. We shall require the following result.

Proposition 4.1. *Let L be a number field, and let L_∞/L be the cyclotomic $\mathbf{Z}_p$-extension of L. Let n be a fixed integer, and suppose that $(\alpha_m) \in \varprojlim_m L_m^\times/L_m^{\times p^n}$ satisfies the following property: for each finite place $v \nmid p$ of L_m, we have that $\mathrm{loc}_v(\alpha_m) \in [O^\times_{L_{m,v}} \cdot L_{m,v}^{\times p^n}]/L_{m,v}^{\times p^n}$.*

Write $\alpha = \alpha_0 \in L^\times/L^{\times p^n}$. Then $\alpha \in [\mathcal{R}_L^\times \cdot L^{\times p^n}]/L^{\times p^n}$.

Proof. Let $\tilde{\alpha}_m \in L_m^\times$ be a representative of α_m, and for each finite place $v \nmid p$ of L, let π_v be a fixed uniformiser of O_{L_v}. Our hypotheses imply that if w is any place L_m lying above v, then $\mathrm{loc}_w(\tilde{\alpha}_m) \cdot (\pi_v^{r_w})^{p^n} \in O^\times_{L_{m,w}}$ for some integer r_w. This in turn implies that we may write

$$\tilde{\alpha}_m \mathcal{R}_{L_m} = \tilde{\mathfrak{a}}_m^{p^n} O_{L_m},$$

where $\tilde{\mathfrak{a}}_m$ is an ideal of $\mathcal{R}_L$. Hence

$$\begin{aligned} \mathrm{Norm}_{L_m/L}(\tilde{\alpha}_m) O_L &= [\tilde{\mathfrak{a}}_m^{p^n}]^{p^m} \\ &= \tilde{\mathfrak{a}}_m^{p^{n+m}}. \end{aligned}$$

It follows that if t is the highest power of p dividing $|\mathrm{Cl}(\mathcal{R}_L)|$, then $\mathfrak{a}^{p^t}$ is principal in $\mathcal{R}_L$, and so, if m is sufficiently large, then we may write

$$\tilde{\mathfrak{a}}_m^{p^{n+m}} = \lambda_m^{p^n} \mathcal{R}_L$$

for some $\lambda_m \in L$. Then

$$\tilde{\alpha} := \mathrm{Norm}_{L_m/L}(\tilde{\alpha}_m) \cdot \lambda_m^{-p^n} \in \mathcal{R}_L^\times,$$

and $\tilde{\alpha}$ is a representative of $\alpha \in L^{\times}/L^{\times p^n}$. This establishes the desired result. $\square$

Now let $(x_m^{(n)})_m \in \varprojlim_m H^1(C_m, \Gamma_n)$ be the image of x under the obvious map

$$\varprojlim_m H^1_{f,\{p\}}(C_m, T) \to \varprojlim_m H^1(C_m, \Gamma_n).$$

For each m there is a homomorphism

$$\eta_{A_{n,C_m}} : H^1(C_m, \Gamma_n) \to \frac{\mathbf{H}(A_{n,C_m})}{\Gamma_n \cdot A^{\times}_{n,C_m}} \to \frac{A^{\times}_{n,C_m}}{A^{\times p^n}_{n,C_m}}$$

induced by

$$\pi \mapsto r(\pi) \mapsto r(\pi)^{p^n},$$

(see Corollary 2.15). Proposition 2.20 implies that these in turn yield a homomorphism

$$\eta_{A_{n,\infty}} : \varprojlim_m H^1(C_m, \Gamma_n) \to \varprojlim_m \frac{A^{\times}_{n,C_m}}{A^{\times p^n}_{n,C_m}},$$

where the last inverse limit is induced by the norm maps $C_m \to C_{m-1}$.

Since $x \in H^1_{f,\{p\}}(F, T)$, it follows that, for each $v \nmid p$, we have

$$\mathrm{loc}_v(r(x_m^{(n)})) \in \frac{\mathbf{H}(\mathcal{M}_{n,O_{C_{m,v}}}) \cdot A^{\times}_{n,C_{m,v}}}{\Gamma_n \cdot A^{\times}_{n,C_{m,v}}}$$

(see Proposition 2.14), and so

$$\mathrm{loc}_v[\eta_{A_{n,C_m}}(x_m^{(n)})] = \mathrm{loc}_v(r(x_m^{(n)}))^{p^n} \in \frac{\mathcal{M}^{\times}_{n,O_{C_{m,v}}} \cdot A^{\times p^n}_{n,C_{m,v}}}{A^{\times p^n}_{n,C_{m,v}}}.$$

Now set $\Gamma_n^* := \mathrm{Hom}(\Gamma_n, \mu_{p^n})$, and let

$$A_n \simeq \prod_{\gamma^* \in \Omega_F \backslash \Gamma_n^*} F[\gamma^*]$$

be the Wedderburn decomposition of A_n (cf. (2.4)). By replacing A_n by A_{n,C_k} for k sufficiently large if necessary, we may suppose that the Wedderburn decomposition of each A_{n,C_m} is given by

$$A_{n,C_m} \simeq \prod_{\gamma^* \in \Omega_F \backslash \Gamma_n^*} F[\gamma^*]_m,$$

where $F[\gamma^*]_m$ is the m-th layer in the cyclotomic $\mathbf{Z}_p$-extension of $F[\gamma^*]$.

Write

$$y_m^{(n)}(\gamma^*) := \mathrm{ev}_{\gamma^*}(\eta_{A_{n.C_m}}(x_m^{(n)})) \in F[\gamma^*]_m^\times / F[\gamma^*]_m^{\times p^n}$$

(see (2.6)).

Then for each finite place $w \nmid p$ of $F[\gamma^*]_m$, we have that

$$\mathrm{loc}_w(y_m^{(n)}(\gamma^*)) \in [O^\times_{F[\gamma^*]_m,w} \cdot F[\gamma^*]_{m,w}^{\times p^n} / F[\gamma^*]_{m,w}^{\times p^n}.$$

It therefore follows from Proposition 4.1 that

$$(y_m^{(n)}(\gamma^*))_m \in \varprojlim_m [\mathcal{R}^\times_{F[\gamma^*]_m} \cdot F[\gamma^*]_m^{\times p^n}] / F[\gamma^*]_m^{\times p^n}$$

for each $\gamma^* \in \Omega_F \backslash \Gamma_n^*$. Hence

$$\eta_{A_{n,\infty}}[(x_m^{(n)})_m] \in \varprojlim_m [\mathcal{M}^\times_{n,O_{C_m}} \cdot A_{n,C_m}^{\times p^n}] / A_{n,C_m}^{\times p^n},$$

which in turn implies that

$$[(r(x_m^{(n)})]_m \in \varprojlim \frac{\mathbf{H}(\mathcal{M}_{n,O_{C_m}}) \cdot A^\times_{n,C_m}}{\Gamma_n \cdot A^\times_{n,C_m}}.$$

Thus, for each n and for each m, it follows from Proposition 2.14(b) that

$$x_m^{(n)} \in \mathrm{Ker}(\psi_{\mathcal{M}_{n,O_{C_m}}}),$$

This implies in particular that $x \in \mathrm{Ker}(\Psi_T^{\{p\}})$, as claimed.

5. Proof of Theorem B

In this section we shall prove Theorem B of the Introduction.

We first recall the definition of the pairing

$$B_F : H^1_{f,\{p\}}(F,T) \times \mathrm{Ker}(\mathrm{Loc}_{F,T^*}) \to \mathbf{Q}_p$$

given in [24, Section 3.1.4].

Fix $x \in H^1_{f,\{p\}}(F,T)$ and $y \in \mathrm{Ker}(\mathrm{Loc}_{F,T^*})$. Then viewing y as an element of $H^1(F,T^*) \simeq \mathrm{Ext}^1_{\Omega_F}(\mathbf{Z}_p, T^*)$ yields an extension

$$0 \to T^* \to T'_y \to \mathbf{Z}_p \to 0. \tag{5.1}$$

Taking $\mathbf{Z}_p(1)$-duals of (5.1) yields an exact sequence

$$1 \to \mathbf{Z}_p(1) \to T_y \to T \to 0. \tag{5.2}$$

We may consider the global and local Galois cohomology of (5.2) for each finite place v of F:

$$\begin{array}{ccccccc} H^1(F,\mathbf{Z}_p(1)) & \xrightarrow{i} & H^1(F,T_y) & \xrightarrow{j} & H^1(F,T) & \longrightarrow & H^2(F,\mathbf{Z}_p(1)) \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ H^1(F_v,\mathbf{Z}_p(1)) & \xrightarrow{i_v} & H^1(F_v,T_y) & \xrightarrow{j_v} & H^1(F_v,T) & \longrightarrow & H^2(F_v,\mathbf{Z}_p(1)). \end{array} \tag{5.3}$$

It may be shown via Tate local duality that

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

for all places $v \nmid p$.

At places $v \mid p$ the extension (5.2) splits locally at v because $y \in \mathrm{Ker}(\mathrm{Loc}_{F,T^*})$, and so we have a corresponding splitting

$$H^1(F_v,T_y) = H^1(F_v,\mathbf{Z}_p(1)) \oplus H^1(F_v,T) \tag{5.4}$$

on the level of cohomology groups. Hence we have

$$H^1_f(F_v, T) = j_v(H^1_f(F_v, T_y))$$

in this case, and in fact every element $z \in H^1(F_v, T)$ has a canonical lifting to an element of $H^1(F_v, T_y)$ given by $z \mapsto (0, z)$.

Global classfield theory implies that the natural map

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

is injective, and so we deduce from (5.3) that

$$H^1_{f,\{p\}}(F, T) \subseteq j(H^1_{f,\{p\}}(F, T_y)).$$

Choose a global lifting $\tilde{x} \in H^1_{f,\{p\}}(F, T_y)$ of $x \in H^1_{f,\{p\}}(F, T)$. For each place v with $v \nmid p$, choose any local lifting $\lambda_v \in H^1_f(F_v, T_y)$ of $x_v \in H^1_f(F_v, T)$. For places v with $v \mid p$, define $\lambda_v \in H^1(F_v, T_y)$ to be the canonical lifting of x_v afforded by the splitting (5.4). Then for each place v of F, we have $\tilde{x}_v - \lambda_v \in i_v(H^1(F_v, \mathbf{Z}_p(1)))$. If $v \mid p$, then i_v is injective, and so we may in fact identify $i_v(H^1(F_v, \mathbf{Z}_p(1)))$ with $H^1(F_v, \mathbf{Z}_p(1))$.

Let

$$l_\chi : \bigoplus_v H^1(F_v, \mathbf{Z}_p(1)) \to \mathbf{Q}_p$$

denote the composition

$$\bigoplus_v H^1(F_v, \mathbf{Z}_p(1)) \simeq \oplus_v \check{F}_v^\times \xrightarrow{L_\chi} \mathbf{Q}_p,$$

where L_χ is defined by

$$L_\chi((u_v)_v) = \sum_{v|p} \log_p N_{F_v/\mathbf{Q}_p}(u_v) - \sum_{v\nmid p} (\log_p q_v) \operatorname{ord}_v(u_v).$$

(Here q_v denotes the cardinality of the residue field of F_v, and we choose Iwasawa's branch of the p-adic logarithm, so that $\log_p(p) = 0$.)

It may be shown that l_χ induces a well-defined map on $\oplus_v i_v(H^1(F_v, \mathbf{Z}_p(1)))$. We define

$$B_F(x,y) = l_\chi\left(\tilde{x}_v - \sum_v \lambda_v\right) \in \mathbf{Q}_p.$$

It is shown in [24, Section 3.1.4] that B_F induces a pairing

$$\langle\langle\ ,\ \rangle\rangle : \frac{H^1_{f,\{p\}}(F,T)}{\mathfrak{G}_F(T)} \times \mathrm{Ker}(\mathrm{Loc}_{F,T^*}) \to \mathbf{Q}_p,$$

and it is conjectured that this pairing is always non-degenerate. We shall relate this pairing to the homomorphism $\Psi_T^{\{p\}}$ by interpreting the pairing B_F in terms of resolvends. In order to do this, we must first establish some preparatory results.

Proposition 5.1. *Suppose that $H^0(F,T) = 0$. Then there is an exact sequence*

$$0 \to \mathrm{Ker}(\Psi^{\{p\}}_{\mathbf{Z}_p(1),f}) \to \mathrm{Ker}(\Psi^{\{p\}}_{T_y,f}) \to \mathrm{Ker}(\Psi^{\{p\}}_{T,f}) \to 0,$$

where the notation is as described in Remark 3.3 above.

Proof. As $H^0(F,T) = 0$, the discussion immediately after (5.2) shows that there is an exact sequence

$$0 \to H^1_f(F, \mathbf{Z}_p(1)) \xrightarrow{i} H^1_f(F, T_y) \to H^1(F,T) \to 0.$$

Via functoriality, we have that

$$\mathrm{Im}(\Psi^{\{p\}}_{\mathbf{Z}_p(1),f}) \simeq \Psi^{\{p\}}_{T_y,f}[i(H^1_f(F, \mathbf{Z}_p(1)))].$$

The desired result now follows by applying the Snake Lemma to the following commutative diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & H^1_f(F,\mathbf{Z}_p(1)) & \xrightarrow{i} & H^1_f(F,T_y) & \longrightarrow & H^1_f(F,T) & \longrightarrow & 0 \\
 & & \Psi^{\{p\}}_{\mathbf{Z}_p(1),f}\downarrow & & \Psi^{\{p\}}_{T_y,f}\downarrow & & \Psi^{\{p\}}_{T,f}\downarrow & & \\
0 & \longrightarrow & \mathrm{Im}(\Psi^{\{p\}}_{\mathbf{Z}_p(1),f}) & \longrightarrow & \mathrm{Im}(\Psi^{\{p\}}_{T_y,f}) & \longrightarrow & \mathrm{Im}(\Psi^{\{p\}}_{T,f}) & \longrightarrow & 0.
\end{array}$$

□

Remark 5.2. This is the only point in our argument where we use the hypothesis that $H^0(F,T)=0$. □

Next, we note that it follows from the standard identification of $H^1(F,T^*)$ with $\mathrm{Ext}^1_{\Omega_F}(\mathbf{Z}_p,T^*)$ that we may write

$$T_y=\mathbf{Z}_p(1)\times T \tag{5.5}$$

with Ω_F-action given by

$$(\zeta,t)^\sigma=\big(\zeta^\sigma\cdot\{f_y(\sigma^{-1})(t)\}^\sigma,t^\sigma\big)$$

for any fixed choice of Ω_F-cocycle f_y representing $y\in H^1(F,T^*)$. This implies that there is an isomorphism of F^c-algebras (but not of Ω_F-modules)

$$A(T_y)_{F^c}\xrightarrow{\sim}A(\mathbf{Z}_p(1))_{F^c}\otimes_{F^c}A(T)_{F^c}. \tag{5.6}$$

We write

$$k_1:A(T_y)_{F^c}\to A(\mathbf{Z}_p(1))_{F^c},\quad k_2:A(T_y)_{F^c}\to A(T)_{F^c}$$

for the algebra homomorphisms induced by the projections $T_y\to\mathbf{Z}_p(1)$, $T_y\to T$ given by (5.5), and we note that the latter projection respects Ω_F-action (while the former, in general, does not). We write

$$i_1:A(\mathbf{Z}_p(1))_{F^c}\to A(T_y)_{F^c},\quad i_2:A(T)_{F^c}\to A(T_y)_{F^c}$$

for the obvious inclusions $\mathbf{Z}_p(1)\to T_y$ and $T\to T_y$ given by (5.5), and we note that the first inclusion respects Ω_F-action (while the second, in general, does not).

Let us also note for future reference that if $y\in\mathrm{Ker}(\mathrm{Loc}_{F,T^*})$, then for each place v of F with $v|p$, the isomorphism

$$A(T_y)_{F_v^c}\xrightarrow{\sim}A(\mathbf{Z}_p(1))_{F_v^c}\otimes_{F_v^c}A(T)_{F_v^c}. \tag{5.7}$$

induced by (5.6) is Ω_{F_v}-equivariant.

We now make a choice of resolvends associated to $\tilde{x}$ and λ_v for each v.

First we observe that, without loss of generality, we may suppose that $x \in \mathrm{Ker}(\Psi_T^{\{p\}})$, and so, by Proposition 5.1, we may assume that $\tilde{x} \in \mathrm{Ker}(\Psi_{T_y}^{\{p\}})$. We choose a resolvend $\alpha \in \mathbf{H}(\mathcal{M}(T_y))$ associated to $\tilde{x}$, and we observe that $k_2(\alpha) \in \mathbf{H}(\mathcal{M}(T))$ is a resolvend associated to x.

For each place $v \nmid p$, we choose an arbitrary resolvend $\delta_v \in \mathbf{H}(\mathcal{M}_v(T_y))$ associated to λ_v.

For each place $v \mid p$, we set

$$\delta_v := \mathrm{loc}_v(i_2(k_2(\alpha)));$$

this is a resolvend associated to λ_v because y is locally trivial at v.

For each place v of F, we see from (5.1) and Proposition 2.14(a) that there is an exact sequence

$$\frac{\mathbf{H}(\mathcal{M}_v(\mathbf{Z}_p(1)))}{\mathbf{Z}_p(1) \cdot \mathcal{M}_v(\mathbf{Z}_p(1))^\times} \xrightarrow{i_v} \frac{\mathbf{H}(\mathcal{M}_v(T_y))}{T_y \cdot \mathcal{M}_v(T_y)^\times} \to \frac{\mathbf{H}(\mathcal{M}_v(T))}{T \cdot \mathcal{M}_v(T)^\times}. \tag{5.8}$$

Suppose that $v \nmid p$. It follows from (5.8) that we may suppose that

$$\tau_v := \mathrm{loc}_v(\alpha) \cdot \delta_v^{-1} \in i_v(\mathbf{H}(\mathcal{M}_v(\mathbf{Z}_p(1)))),$$

possibly after first multiplying τ_v by a suitable element of $T_y \cdot \mathcal{M}_v(T_y)^\times$. We have that τ_v is a resolvend associated to $\tilde{x}_v - \lambda_v \in i_v(H^1(F_v, \mathbf{Z}_p(1)))$. As $v \nmid p$, it follows that $\mathbf{Z}_p(1)$ is unramified at v, and so Remark 3.1 implies that we have

$$H(\mathcal{M}_v(\mathbf{Z}_p(1))) = H(\mathcal{M}_v(\mathbf{Z}_p(1))) \simeq H^1_f(F_v, \mathbf{Z}_p(1)) \simeq \check{O}^\times_{F_v}.$$

Hence it follows that $(\log_p(q_v))\,\mathrm{ord}_v(\tilde{x}_v - \lambda_v) = 0$.

Now suppose that $v \mid p$, and set

$$\tau := \alpha \cdot i_2(k_2(\alpha))^{-1} \in \mathcal{M}(T_y)^\times_{O_{F^c}}.$$

Then we have that

$$\begin{aligned}\tau_v := \mathrm{loc}_v(\tau) &= \mathrm{loc}_v(\alpha \cdot i_2(k_2(\alpha))^{-1}) \\ &= \mathrm{loc}_v(\alpha) \cdot \delta_v^{-1} \in \mathbf{H}(\mathcal{M}_v(T_y)),\end{aligned}$$

and the map $\omega \mapsto \tau_v^{\omega}\tau_v^{-1}$ is a $\mathbf{Z}_p(1)$-valued Ω_{F_v}-cocycle that represents $\tilde{x}_v - \lambda_v \in i_v(H^1(F_v, \mathbf{Z}_p(1)))$. Hence if we set

$$\tilde{\tau} := k_1(\tau) = k_1(\alpha) \in \mathcal{M}(\mathbf{Z}_p(1))^{\times}_{O_{Fc}},$$

then

$$\tilde{\tau}_v := \mathrm{loc}_v(\tilde{\tau}) \in \mathbf{H}(\mathcal{M}_v(\mathbf{Z}_p(1)))$$

is a resolvend associated to $\tilde{x}_v - \lambda_v$. In general, $\tilde{\tau}$ does not belong to $\mathbf{H}(\mathcal{M}(\mathbf{Z}_p(1)))$.

Let $n \geq 1$. Recall (see (2.4)) that

$$A(\mathbf{Z}_p(1))_n \simeq \oplus_{\mathbf{Z}/p^n\mathbf{Z}} F,$$

and fix a generator $\mathbf{1}_n$ of $\mathbf{Z}_p/p^n\mathbf{Z}$. We view $\mathbf{1}_n$ as being a character of μ_{p^n}.

Let $\tilde{\tau}_{v,n}$ and $(\tilde{x}_v - \lambda_v)_n$ denote the images of $\tilde{\tau}$ and $\tilde{x}_v - \lambda_v$ in $\mathbf{H}(A_v(\mathbf{Z}_p(1))_n)$ and $H^1(F_v, \mu_{p^n})$ respectively. Then Proposition 2.17 implies that the image of the resolvend $\tilde{\tau}_{v,n}$ in $H^1(F_v, \mu_{p^n}) \simeq F_v^{\times}/F_v^{\times p^n}$ is equal to the image of

$$\begin{aligned}\mathrm{ev}_{\mathbf{1}_n}((\tilde{\tau}_{v,n})^{p^n}) &= \mathrm{loc}_v(\mathrm{ev}_{\mathbf{1}_n}(\tau_n)^{p^n}) \\ &= \mathrm{loc}_v(\mathrm{ev}_{\mathbf{1}_n}((k_1(\alpha_n)^{p^n})))\end{aligned}$$

in $F_v^{\times}/F_v^{\times p^n}$. Since $\alpha_n \in \mathbf{H}(\mathcal{M}(T_y)_n)$, it follows that $\alpha_n^{p^n} \in \mathcal{M}(T_y)^{\times}$, and so $\mathrm{ev}_{\mathbf{1}_n}(k_1(\alpha_n^{p^n})) \in \mathcal{R}_F^{\times}$. Hence we see that

$$\bigoplus_{v|p}(\tilde{x}_v - \lambda_v)_n \in \bigoplus_{v|p} H^1(F_v, \mu_{p^n}) \simeq \bigoplus_{v|p} F_v^{\times}/F_v^{\times p^n}$$

lies in the image of $\mathcal{R}_F^{\times} F^{\times p^n}/F^{\times p^n}$ under the localisation map

$$F^{\times}/F^{\times p^n} \to \bigoplus_{v|p} F_v^{\times}/F_v^{\times p^n}.$$

This in turn implies that

$$\bigoplus_{v|p} N_{F_v/\mathbf{Q}_p}(\tilde{x}_v - \lambda_v)_n \in H^1(\mathbf{Q}_p, \mu_{p^n}) \simeq \mathbf{Q}_p^{\times}/\mathbf{Q}_p^{\times p^n}$$

lies in the image of $\mathbf{Z}[1/p]^{\times}\mathbf{Q}^{\times p^n}/\mathbf{Q}^{\times p^n}$ under the localisation map

$$H^1(\mathbf{Q}, \mu_{p^n}) \simeq \mathbf{Q}^{\times}/\mathbf{Q}^{\times p^n} \to H^1(\mathbf{Q}_p, \mu_{p^n}) \simeq \mathbf{Q}_p^{\times}/\mathbf{Q}_p^{\times p^n},$$

for all $n \geq 1$. As the function $\log_p(z)$ vanishes on the image of $\mathbf{Z}[1/p]^{\times}$ in $\mathbf{Q}_p^{\times}$, we conclude that

$$\sum_{v|p} \log_p \left(N_{F_v/\mathbf{Q}_p}(\tilde{x}_v - \lambda_v) \right) = 0.$$

We therefore deduce that $B_F(x, y) = 0$. This completes the proof of Theorem B.

References

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

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

[3] A. Agboola *On p-adic height pairings and locally free classgroups of Hopf orders*, Math. Proc. Cam. Phil. Soc., **123**, (1998), 447–459.

[4] A. Agboola, *On primitive and realisable classes*, Comp. Math., **126**, (2001), 113–122.

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

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

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

[8] 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.

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

[10] L. Breen, *Une th'eoreme d'annulation pour certain* Ext^i *de faisceaux abéliennes*, Ann. Sci. École Norm. Sup. **5** (1975), 339–352.

[11] 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.

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

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

[14] C. Curtis, I. Reiner, *Methods of Representation Theory, Volume II*, Wiley, 1987.

[15] R. Greenberg, *Iwasawa theory for p-adic representations*, Adv. Stud. Pure. Math. **17**, 97–137.

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

[17] K. Iwasawa, *On* $\mathbf{Z}_l$*-extensions of algebraic number fields*, Ann of Math. **98**, (1973), 246–326.

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

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

[21] J. Milne, *Arithmetic duality theorems*, Academic Press, 1986.

[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] B. Perrin-Riou, *p-adic L-functions and p-adic representations*, SMF/AMS Texts and Monographs, vol.3, American Mathematical Society, 2000. (This is an updated English translation of *Fonctions L p-adiques des représentations p-adiques*, Asterisque, **229**, (1995).)

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

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

[27] K. Rubin, *Euler Systems*, Annals of Mathematics Studies 147, Princeton University Press, 2000.

[28] C. Soulé, *On higher p-adic regulators*, Springer Lecture Notes in Mathematics **854**, (1981), 372–401.

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

[30] R. Swan, *Algebraic K-theory*, SLNM 76, (1968).

[31] M. J. Taylor *Classgroups of Group Rings*, CUP 1984.

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

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

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

[35] 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