GALOIS MODULES AND p-ADIC REPRESENTATIONS

A. AGBOOLA

Abstract. In this paper we develop a theory of class invariants associated to p-adic representations of absolute Galois groups of number fields. Our main tool for doing this involves a new way of describing certain Selmer groups attached to p-adic representations in terms of resolvends associated to torsors of finite group schemes.

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. 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 $\tilde{G}^*$ denote the normalisation of G^*, and let $i : \tilde{G}^* \to G^*$ 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 $\mathcal{O}_X$ is an $\mathcal{O}_G$-comodule, and so it is also an $\mathcal{O}_{G^*}$-module (see e.g. [12]). 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 $\mathcal{M}_\pi$ on G^*. Set

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

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 [31]), and was further developed in the context of Galois module theory by M. Taylor ([28]). Taylor originally considered the case in which G is a torsion subgroup scheme of an abelian variety with complex multiplication.

Date: Version of June 19, 2006.

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

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 [27], 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 [29], [11]). This vanishing result was extended to all elliptic curves in [2] and [20].

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 [21], 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 [5], 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 [18]). Finally we mention that in [1], [3], and [6], 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 representations, and to 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 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 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.

For any (not necessarily finitely generated) O_F algebra $\mathfrak{A}_n \subseteq A_n$ satisfying certain quite mild conditions (see Section §3 below), we use a description of $H^1(F, G_n)$ which arises via studying the Galois structure of G_n-torsors in terms of A_n to give a new way of imposing local conditions on cohomology classes in terms of the algebra $\mathfrak{A}_n$. (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 $H^1_{\mathfrak{A}_n}(F, G_n)$. Suppose that $\pi : X \to \mathrm{Spec}(F)$ is any G_n-torsor whose isomorphism class lies in $H^1_{\mathfrak{A}_n}(F, G_n)$. We shall explain how to use the methods of [9], [19] and [31] to construct a natural homomorphism

$$\phi_{\mathfrak{A}_n} : H^1_{\mathfrak{A}_n}(F, G_n) \to \mathrm{Pic}(\mathrm{Spec}(\mathfrak{A}_n)). \tag{1.3}$$

This generalises the class invariant homomorphisms (1.1) and (1.2) above. For suppose 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 $\phi_{\mathfrak{A}_n}$ 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 $H^1_{\mathfrak{A}_n}(F, G_n)$, and the restriction of $\phi_{\mathfrak{A}_n}$ to $H^1(\mathrm{Spec}(O_F), \mathcal{G}_n)$ is the homomorphism (1.2). (See Example 3.5 below.)

In this paper we shall mainly be concerned with the cases

$$\mathfrak{A}_n = \mathfrak{M}_n, \qquad \mathfrak{A}_n = \mathfrak{M}_n \otimes_{O_F} O_F[1/p] := \mathfrak{M}_n^{\{p\}}.$$

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

$$H^1_f(F_v, T) := \mathrm{Ker}\left[H^1(F_v, T) \to H^1(F_v^{\mathrm{nr}}, T)\right]. \tag{1.4}$$

Following [22, §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 3.6 below)

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

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 $\varprojlim H^1_{\mathfrak{M}_n^{\{p\}}}(F, G_n)$ 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

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

The natural inclusions $G_n^* \to G_{n+1}^*$ induce pullback homomorphisms

$$\mathrm{Pic}(\mathrm{Spec}(\mathfrak{M}_{n+1})) \to \mathrm{Pic}(\mathrm{Spec}(\mathfrak{M}_n)), \qquad \mathrm{Pic}(\mathrm{Spec}(\mathfrak{M}_{n+1}^{\{p\}})) \to \mathrm{Pic}(\mathrm{Spec}(\mathfrak{M}_n^{\{p\}})).$$

We shall show that we may take inverse limits in (1.3) to obtain homomorphisms

$$\Phi_F : H^1_u(F,T) \to \varprojlim \operatorname{Pic}(\operatorname{Spec}(\mathfrak{M}_n)), \qquad \Phi_F^{\{p\}} : H^1_{f,\{p\}}(F,T) \to \varprojlim \operatorname{Pic}(\operatorname{Spec}(\mathfrak{M}_n^{\{p\}})).$$

Our first result shows that the homomorphism $\Phi_F^{\{p\}}$ 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

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

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 [14, p.131–132], and further studied by A. Plater in [23] and [24] (see also [17]).

Let

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

denote the natural localisation map. In [22, Section 3.1.4], Perrin-Riou constructs a p-adic height pairing

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

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

$$\langle\langle\, ,\, \rangle\rangle : \frac{H^1_{f,\{p\}}(F,T)}{\mathfrak{G}_F(T)} \times \operatorname{Ker}(\operatorname{Loc}_{F,T^*}) \to \mathbf{Q}_p \tag{1.5}$$

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 result shows that this conjecture implies that $\mathfrak{G}_F(T)$ also has a natural characterisation in terms of Galois module structure (see Propositions 6.3 and 6.5 below).

Theorem 1.1. *(a) If $x \in \mathfrak{G}_F(T)$, then $\Phi_F^{\{p\}}(x)$ is of finite order.*

(b) If $x \in H^1_{f,\{p\}}(F,T)$ and $\Phi_F^{\{p\}}(x)$ has 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, then $x \in \mathfrak{G}_F(T)$ if and only if $\Phi_F^{\{p\}}(x)$ is of finite order.

Remark 1.2. It would be interesting if one could show directly (without, of course, assuming the non-degeneracy of the pairing $\langle\langle\, ,\, \rangle\rangle$!) that

$$\{x \in H^1_{f,\{p\}}(F,T) |\, \Phi_F^{\{p\}}(x) \text{ has finite order}\} = \text{the left-hand kernel of the pairing } B_F.$$

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 $\Phi_F^{\{p\}}(x)$ is of finite order. Unfortunately we do not know how to do this at present. $\square$

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^*.

Corollary 1.3. *Suppose that the pairing $\langle\langle\, ,\, \rangle\rangle$ is non-degenerate modulo torsion, and that*

$$H^2(F^S/C_\infty, V^*/T^*) = 0. \tag{1.6}$$

Then the restriction of $\Phi_F^{\{p\}}$ to $\mathrm{Ker}(\mathrm{Loc}_{F,T})$ has finite kernel.

Proof. It follows from [22, Remark at the end of §3.4.2] that if (1.6) holds, then $\mathfrak{G}_F(T) \cap \mathrm{Ker}(\mathrm{Loc}_{F,T})$ is finite. The result now follows from Theorem 1.1. $\square$

We now turn to the homomorphism Φ_F.

For each integer n, the action of Ω_F on Γ_n^* yields a representation $\rho_n^* : \Omega_F \to \mathrm{Aut}(\Gamma_n^*)$. Write F_n^* for the fixed field of ρ_n^*; then $F_\infty^* := \cup_n F_n^*$ is the extension of F cut out by ρ^*. Set

$$\mathfrak{C}_F(T) := \{x \in H_u^1(F,T) \mid Mx \in \cap_n \mathrm{Cores}_{F_n^*/F}(H_u^1(F_n^*, T)) \text{ for some integer } M > 0\}.$$

Theorem 1.4. *Suppose that $x \in \mathfrak{C}_F(T)$. Then $\Phi_F(x)$ is of finite order.*

Remark 1.5. Whether or not the the converse of Theorem 1.4 holds in general is an open question, and it appears to be a very delicate problem. If T has $\mathbf{Z}_p$-rank one, then it may be shown that $\mathfrak{C}_F(T) = \mathfrak{G}_F(T) \cap H_u^1(F,T)$, and that the converse to Theorem 1.4 holds in this case. $\square$

Acknowledgements. This paper owes a great deal to ideas first introduced in [5], and I am extremely grateful to G. Pappas for many interesting and helpful conversations. I would like to thank B. Conrad, R. Greenberg and S. Howson for useful discussions. I am grateful to the anonymous referees for pointing out some mistakes in earlier versions of this paper, and for a number of very helpful comments. I would also like to thank the Mathematics Department of Harvard University for their hospitality while a part of this work was carried out. This research was partially supported by NSF grants.

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 $P_v := P \otimes_{O_L} O_{L_v}$.

For any $\mathbf{Z}$-module Q, we set $\check{Q} := \varprojlim_n Q/p^n Q$.

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

In this section, R denotes either a field K, or a Dedekind domain with field of fractions K. In the second case, the symbol R^c denotes the integral closure of R in K^c. We assume (in both cases) that K is of characteristic zero. Let $Y = \mathrm{Spec}(R)$. We shall explain how the cohomology group $H^1(Y, G)$ may be described in terms of the Hopf algebra A representing G^*. Set $\Gamma := G(R^c)$ and $\Gamma^* := G^*(R^c)$.

Recall that there is a canonical isomorphism

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

(see [31], [15, éxposé VII], or [21]). This implies that given any G-torsor $\pi : X \to Y$, we can associate to it a canonical commutative extension

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

The scheme $G(\pi)$ is a $\mathbf{G}_m$-torsor over G^*, and its associated G^*-line bundle is equal to $\mathcal{L}_\pi$. (This construction is explained in detail by Waterhouse in [31].)

Over $\mathrm{Spec}(R^c)$, the G-torsors π_0 and π become isomorphic, i.e. there is an isomorphism $X \otimes_R R^c \simeq G \otimes_R R^c$ 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 [31], we obtain 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.

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, [19].) Note that $\mathbf{r}(s_\pi)$ depends upon the choice of ξ_π as well as upon s_π. We shall sometimes not make the dependence of $\mathbf{r}(s_\pi)$ upon ξ_π explicit.

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

$$\mathbf{H}(A) := \left\{ \alpha \in A^{\times}_{R^c} \,\Big|\, \frac{\alpha^{\omega}}{\alpha} \in \Gamma \text{ for all } \omega \in \Omega_K. \right\},$$

$$H(A) := \frac{\mathbf{H}(A)}{\Gamma \cdot A^{\times}}.$$

□

If $\omega \in \Omega_K$, 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 [19, 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 [9, 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_K-cohomology of the exact sequence

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

of Ω_K-modules. We give a different approach using a method that involves combining the functoriality of Waterhouse's cosntruction with the theory of descent.

Theorem 2.2. *Let G be a finite, flat commutative group scheme over* $\mathrm{Spec}(R)$*, and let $G^* =$* $\mathrm{Spec}(A)$ *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 $\pi_1 : X_1 \to \mathrm{Spec}(R)$ and $\pi_2 : X_2 \to \mathrm{Spec}(R)$ are G-torsors satisfying $\psi(\pi_1) = \psi(\pi_2) = 0$. For $i = 1, 2$, let

$$\xi_{\pi_i} : \mathcal{L}_{\pi_1} \otimes_R R^c \xrightarrow{\sim} A_{R^c}$$

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 $\mathrm{Map}_S(G^*, \mathbf{G}_m)$ for the set of scheme morphisms $G^* \times_{\mathrm{Spec}(R)} S \to \mathbf{G}_m \times_{\mathrm{Spec}(R)} S$. Since G^* is affine, the functor $S \mapsto \mathrm{Map}_S(G^*, \mathbf{G}_m)$ is representable by an affine group scheme over R, which we denote by $\mathcal{M}(G^*, \mathbf{G}_m)$. The group scheme G (which represents the functor $S \mapsto \mathrm{Hom}_S(G^*, \mathbf{G}_m)$) is a closed subgroup scheme of $\mathcal{M}(G^*, \mathbf{G}_m)$.

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

$$G_\alpha := \alpha \cdot [G \otimes_R R^c] \tag{2.1}$$

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

$$\Xi_\alpha : G \otimes_R R^c \xrightarrow{\sim} G_\alpha \tag{2.2}$$

of schemes with $G \otimes_R R^c$ 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 $G_\alpha = Z_\alpha \otimes_R R^c$. (We refer the reader to [8, 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/K^c} of G_α descends to a scheme over $\mathrm{Spec}(K)$. This in turn follows via Galois descent, and may be seen as follows. We first note that the isomorphism Ξ_α induces a bijection $\Gamma \to G_\alpha(K^c)$ of sets. Define $z_\alpha : \Omega_K \to \Gamma$ by $z(\omega) = \alpha^\omega \alpha^{-1}$; thus z_α is the Γ-valued cocycle of Ω_K associated to α. Then it is easy to check that the action of Ω_K on $G_\alpha(K^c)$ is given by

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

for all $g \in \Gamma$ and $\omega \in \Omega_K$. This implies that G_{α/K^c} descends to $Z_{\alpha/K}$ over $\mathrm{Spec}(K)$. 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 $\omega \in \Omega_K$ 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 $G_\alpha(K^c) \xrightarrow{\sim} G_\beta(K^c)$ of Ω_K-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. Suppose that $R = K$. Then it is not hard to check that (using the notation established in the proof of Theorem 2.2) the map $\Omega_K \to \Gamma$ defined by $\omega \mapsto \mathbf{r}(s_\pi)^\omega \mathbf{r}(s_\pi)^{-1}$ is an Ω_K-cocycle representing $[\pi] \in H^1(K, G)$. □

If R is a local ring, then $\mathrm{Pic}(G^*) = 0$, 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 [30],[10, Chapter 3, §4]) and by N. Byott (see [9, §3]).

Recall that N denotes the exponent of G.

Corollary 2.4. *Suppose that R is a local ring.*

(a) There is an isomorphism

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

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

$$\eta_R : H^1(R, G) \to \frac{A^\times}{(A^\times)^N}.$$

□

Remark 2.5. Suppose that $R = K$, and for each $\gamma^* \in \Gamma^*$, write $K[\gamma^*]$ for the smallest extension of K whose absolute Galois group fixes γ^*. Let $\Gamma^* \backslash \Omega_K$ denote a set of representatives of Ω_K-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 K-algebra A is given by

$$A \simeq (K^c\Gamma)^{\Omega_K} \simeq \prod_{\gamma^* \in \Gamma^* \backslash \Omega_K} K[\gamma^*]. \tag{2.3}$$

□

Proposition 2.6. *Suppose that $R = K$, and that G^* is a constant group scheme over* $\mathrm{Spec}(K)$*. Then $A \simeq \mathrm{Map}(\Gamma^*, K)$, and the map η_K of Corollary 2.4(b) induces an isomorphism*

$$\eta_K : H^1(K, G) \xrightarrow{\sim} \mathrm{Hom}(\Gamma^*, K^\times/(K^\times)^N) \subset \mathrm{Map}(\Gamma^*, K^\times/(K^\times)^N) \simeq A^\times/(A^\times)^N.$$

Proof. See [5, Corollary 3.4]. □

Proposition 2.7. *Suppose that $R = K$, and let L be any algebraic extension of K. Then the following diagram is commutative:*

$$\begin{array}{ccc} H^1(K,G) & \xrightarrow{\Upsilon_K} & H(A) \\ {\scriptstyle \mathrm{Res}}\big\downarrow & & \big\downarrow \\ H^1(L,G) & \xrightarrow{\Upsilon_L} & H(A_L). \end{array} \tag{2.4}$$

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 $i : \mathbf{H}(A) \to \mathbf{H}(A_L)$.

Proof. Let $\pi : X \to \mathrm{Spec}(K)$ be any G-torsor, 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_L-cocycle associated to $i(\mathbf{r}(s))$ is equal to the restriction of the Ω_K-cocycle associated to $\mathbf{r}(s)$ (cf. Remark 2.3). □

Remark 2.8. Suppose that $R = K$, and that $\pi \in \mathrm{Ker}(\eta_K)$. Let $\mathbf{r}(s_\pi) \in \mathbf{H}(A)$ be any resolvend associated to π. Then $\mathbf{r}(s_\pi)^N = \alpha^N \in A^{\times N}$, and so $\mathbf{r}(\alpha^{-1}s_\pi)^N = 1$. Hence $\mathbf{r}(\alpha^{-1}s_\pi) \in A^\times_{K(\mu_N)}$, and so Proposition 2.7 implies that π lies in the kernel of the restriction map

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

Conversely, if $\pi \in \mathrm{Res}_{K/K(\mu_N)}$, then, since π is trivialised over $K(\mu_N)$, it follows that $\mathbf{r}(s_\pi) \in A^\times_{K(\mu_N)}$ for any choice of s_π. We therefore deduce from Corollary 2.4(b) that $\mathbf{r}(s_\pi)^N \in A^\times \cap A^{\times N}_{K(\mu_N)}$. Hence, if $A^{\times N} = A^\times \cap A^{\times N}_{K(\mu_N)}$, then $\mathbf{r}(s_\pi)^N \in A^{\times N}$, and so $\pi \in \mathrm{Ker}(\eta_K)$. □

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

$$\mathcal{N}_{L/K} : A_{L^c} \to A_{K^c}; \qquad a \mapsto \prod_{i=1}^n a^{\omega_i}. \tag{2.5}$$

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

$$\mathcal{N}_{L/K} : \mathbf{H}(A_L) \to \mathbf{H}(A_K), \qquad \mathcal{N}_{L/K} : H(A_L) \to H(A_K).$$

Proposition 2.9. *The following diagram is commutative:*

$$\begin{tikzcd} H^1(L,G) \arrow[r, "\Upsilon_L"] \arrow[d, "\mathrm{Cores}_{L/K}"'] & H(A_L) \arrow[d, "\mathcal{N}_{L/K}"] \\ H^1(K,G) \arrow[r, "\Upsilon_K"] & H(A_K), \end{tikzcd} \tag{2.6}$$

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

Proof. Let $\pi_L : X_L \to \mathrm{Spec}(L)$ be any G-torsor and let $s_{\pi_L} : A_L \xrightarrow{\sim} \mathcal{L}_{\pi_L}$ be any trivialisation of $\mathcal{L}_{\pi_L}$. Then it follows via a straightforward computation that the Ω_K-cocycle associated to $\mathcal{N}_{L/K}(\mathbf{r}(s_{\pi_L}))$ is equal to the corestriction of the Ω_L-cocycle associated to $\mathbf{r}(s_{\pi_L})$ (cf. Remark 2.3). □

Let $(G_n)_{n\geq 1}$ be a p-divisible group over $\mathrm{Spec}(R)$. For each n, set $G_n^* = \mathrm{Spec}(A_n)$, and set $\Gamma_n := G_n(R^c)$, $\Gamma_n^* := G_n^*(R^c)$. We write $p_n := [p] : G_n \to G_{n-1}$ for the multiplication-by-p map, and we use the same symbol to denote the induced map $H^1(\mathrm{Spec}(R), G_n) \to H^1(\mathrm{Spec}(R), G_{n-1})$.

The map p_n induces a dual inclusion map $p_n^D : G_{n-1}^* \to G_n^*$, and we may identify A_{n-1} with the pullback $(p_n^D)^* A_n$ of A_n via p_n^D. Thus (via pullback) p_n^D induces a homomorphism $q_n : A_n \to A_{n-1}$ which extends to a homomorphism (which we denote by the same symbol) $A_{n,K^c} \to A_{n-1,K^c}$. It is easy to check that $q_n(\mathbf{H}(A_n)) \subseteq \mathbf{H}(A_{n-1})$, and that $q_n(\Gamma_n \cdot A_n^\times) \subseteq \Gamma_{n-1} \cdot A_{n-1}^\times$.

Proposition 2.10. *Suppose that R is a local ring. Then the following diagram is commutative:*

$$\begin{tikzcd} H^1(\mathrm{Spec}(R), G_n) \arrow[r, "\Upsilon_{R,n}"] \arrow[d, "p_n"'] & H(A_n) \arrow[d, "q_n"] \\ H^1(\mathrm{Spec}(R), G_{n-1}) \arrow[r, "\Upsilon_{R,n-1}"] & H(A_{n-1}). \end{tikzcd} \tag{2.7}$$

Proof. Suppose that $\pi_n : X_n \to \mathrm{Spec}(R)$ is any G_n-torsor, and let $s_{\pi_n} : A_n \xrightarrow{\sim} \mathcal{L}_{\pi_n}$ be any trivialisation of $\mathcal{L}_{\pi_n}$. Set $\pi_{n-1} := p_n(\pi_n)$. Then it follows via the functoriality of Waterhouse's construction in [31] that there is a natural identification $\mathcal{L}_{\pi_{n-1}} \simeq (p_n^D)^* \mathcal{L}_{\pi_n}$. Consider the trivialisation $s_{\pi_{n-1}} := (p_n^D)^* s_{\pi_n} : A_{n-1} \xrightarrow{\sim} \mathcal{L}_{\pi_{n-1}}$ of $\mathcal{L}_{\pi_{n-1}}$ obtained by pulling back s_{π_n} along p_n^D. We have

$$\Upsilon_{R,n-1}(\pi_{n-1}) = [\mathbf{r}(s_{\pi_{n-1}})] = [\mathbf{r}((p_n^D)^* s_{\pi_n})] = [q_n(\mathbf{r}(s_{\pi_n}))].$$

This establishes the result. □

Suppose now that $R = K$. Fix a positive integer n, and assume that G_n^* is a constant group scheme. Then we have

$$A_n^\times / (A_n^\times)^{p^n} \simeq \mathrm{Map}(\Gamma_n^*, K^\times/(K^\times)^{p^n}).$$

For each element $P : \mathrm{Spec}(K) \to G_n^*$ in Γ_n^*, write $\chi_P : G_n \to \mu_{p^n}$ for the corresponding character of G_n. Then χ_P induces a homomorphism (which we denote by the same symbol):

$$\chi_P : H^1(K, G_n) \to H^1(K, \mu_{p^n}); \qquad [\pi] \mapsto [\pi(\chi_P)].$$

Write

$$\mathrm{ev}_P : A_n^\times/(A_n^\times)^{p^n} \simeq \mathrm{Map}(\Gamma_n^*, K^\times/(K^\times)^{p^n}) \to K^\times/(K^\times)^{p^n}$$

for the map $a \mapsto a(P)$ given by 'evaluation at P'. The following result shows how to describe the map η_K of Corollary 2.4 in terms of Kummer theory.

Proposition 2.11. *Let the hypotheses and notation be as above. Then the following diagram is commutative:*

$$\begin{tikzcd} H^1(K, G_n) \arrow[r, "\chi_P"] \arrow[d, "\eta_K"'] & H^1(K, \mu_{p^n}) \\ A_n^\times/(A_n^\times)^{p^n} \arrow[r, "\mathrm{ev}_P"] & K^\times/(K^\times)^{p^n}. \arrow[u, "\text{Kummer}"'] \end{tikzcd} \tag{2.8}$$

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

Proof. See [5, Proposition 3.2]. □

Corollary 2.12. *Let the hypotheses and notation be as above. For each integer n, let*

$$r_n : \mathrm{Hom}(\Gamma_n^*, K^\times/(K^\times)^{p^n}) \to \mathrm{Hom}(\Gamma_{n-1}^*, K^\times/(K^\times)^{p^{n-1}})$$

be the homomorphism given by $f \mapsto f|_{\Gamma_{n-1}^*}$. Then the following diagram commutes:

$$\begin{tikzcd} H^1(K, G_n) \arrow[r, "\eta_K"] \arrow[d, "p_n"'] & \mathrm{Hom}(\Gamma_n^*, K^\times/(K^\times)^{p^n}) \arrow[d, "r_n"] \\ H^1(K, G_{n-1}) \arrow[r, "\eta_K"] & \mathrm{Hom}(\Gamma_{n-1}^*, K^\times/(K^\times)^{p^{n-1}}). \end{tikzcd}$$

Proof. Suppose that $P \in \Gamma_{n-1}^*$. Then, by definition, the following diagram commutes:

$$\begin{tikzcd} H^1(K, G_n) \arrow[r, "\chi_P"] \arrow[d, "p_n"'] & H^1(K, \mu_{p^n}) \simeq K^\times/(K^\times)^{p^n} \arrow[d, "\text{red}"] \\ H^1(K, G_{n-1}) \arrow[r, "\chi_P"] & H^1(K, \mu_{p^{n-1}}) \simeq K^\times/(K^\times)^{p^{n-1}}. \end{tikzcd} \tag{2.9}$$

(Here the right-hand vertical arrow denotes the natural reduction map.) The result now follows from Propositions 2.11 and 2.6. □

3. Selmer conditions and Galois structure

In this section we shall apply the results of §2 to explain how resolvends may be used to impose local conditions on G-torsors. This enables us to define certain Selmer groups. We then show that there are natural homomorphisms from these Selmer groups into suitable locally free classgroups. These generalise the class invariant homomorphisms described at the begining of the introduction to this paper.

In what follows, F will denote either a number field or a local field (depending upon the context), with ring of integers O_F. We suppose given a finite, flat, commutative group scheme G over $\mathrm{Spec}(F)$, and we let $G^* = \mathrm{Spec}(A)$. As usual, we set $\Gamma = G(F^c)$, and we write $\mathfrak{M}$ for the unique O_F-maximal order contained in A.

Let $\mathfrak{A}$ denote any O_F-algebra in A satisfying the following conditions:

(i) $F \cdot \mathfrak{A} = A$;

(ii) $\Gamma \subseteq \mathfrak{A}_{O_{F^c}}$;

(iii) If F is a number field, then $\mathfrak{A}_v = \mathfrak{M}_v$ for all but finitely many places v of F.

Note that we do not assume that $\mathfrak{A}$ is finitely generated over O_F.

Set

$$\mathbf{H}(\mathfrak{A}) := \left\{ \alpha \in \mathfrak{A}^{\times}_{O_{F^c}} \;\middle|\; \frac{\alpha^{\omega}}{\alpha} \in \Gamma \text{ for all } \omega \in \Omega_K. \right\}.$$

We shall be interested in using the groups $\mathbf{H}(\mathfrak{A})$ and $\mathbf{H}(A)$ to impose Selmer-type conditions on elements of $H^1(F,G)$. The following definition is motivated by Corollary 2.4(a). (Recall that the isomorphism Υ_F below was defined in Corollary 2.4.)

Definition 3.1. Suppose that F is a local field. Then we define the subgroup $H^1_{\mathfrak{A}}(F,G)$ of $H^1(F,G)$ by:

$$H^1_{\mathfrak{A}}(F,G) = \left\{ x \in H^1(F,G) \;\middle|\; \Upsilon_F(x) \in \frac{\mathbf{H}(\mathfrak{A}) \cdot A^{\times}}{\Gamma \cdot A^{\times}} \subseteq \frac{\mathbf{H}(A)}{\Gamma \cdot A^{\times}} = H(A) \right\}.$$

Hence a G-torsor $\pi : X \to \mathrm{Spec}(F)$ lies in $H^1_{\mathfrak{A}}(F,G)$ if and only if there exists a trivialisation $s_\pi : A \xrightarrow{\sim} \mathcal{L}_\pi$ with $\mathbf{r}(s_\pi) \in \mathbf{H}(\mathfrak{A}) \subseteq \mathbf{H}(A)$. The resolvend $\mathbf{r}(s_\pi)$ of such a trivialisation is well-defined up to multiplication by an element of $\Gamma \cdot \mathfrak{A}^{\times}$. □

Definition 3.2. If F is a number field, then we define $H^1_{\mathfrak{A}}(F,G)$ by

$$H^1_{\mathfrak{A}}(F,G) = \mathrm{Ker}\left[H^1(F,G) \to \prod_{v \nmid \infty} \frac{H^1(F_v,G)}{H^1_{\mathfrak{A}_v}(F_v,G)} \right].$$

□

Remark 3.3. Suppose that F is either a number field or a local field, and assume that $\pi \in H^1(F,G)$ lies in $\mathrm{Ker}(\eta_F)$. Then it follows from the discussion in Remark 2.8 that there exists a resolvend $\mathbf{r}(s_\pi) \in \mathbf{H}(A)$ associated to π such that $\mathbf{r}(s_\pi)^N = 1$. Hence $\mathbf{r}(s_\pi) \in \mathbf{H}(\mathfrak{M})$, and so $\pi \in H^1_{\mathfrak{M}}(F,G)$. $\square$

Now suppose that F is a number field. Let $J_f(A)$ denote the group of finite ideles of A, i.e. $J_f(A)$ is the restricted direct product of the groups $A_v^\times$ with respect to the subgroups $\mathfrak{M}_v^\times$ for $v \nmid \infty$. We view $A^\times$ as being a subgroup of $J_f(A)$ via the obvious diagonal embedding. Write $\mathrm{Cl}(\mathfrak{A})$ for the locally free classgroup of $\mathfrak{A}$. Thus, $\mathrm{Cl}(\mathfrak{A})$ is the Grothendieck group of locally free $\mathfrak{A}$-modules of finite rank, and it may be identified with the group $\mathrm{Pic}(\mathrm{Spec}(\mathfrak{A}))$. Then it is a standard result from the theory of classgroups (see e.g. [13, §52]) that there is a natural isomorphism

$$\mathrm{Cl}(\mathfrak{A}) \simeq \frac{J_f(A)}{\left(\prod_{v\nmid\infty} \mathfrak{A}_v^\times\right) \cdot A^\times}. \tag{3.1}$$

Theorem 3.4. *Let F be a number field.*

(a) There is a natural homomorphism

$$\phi_{\mathfrak{A}} : H^1_{\mathfrak{A}}(F,G) \to \mathrm{Cl}(\mathfrak{A}).$$

(b) The isomorphism

$$\Upsilon_F : H^1(F,G) \xrightarrow{\sim} H(A)$$

of Corollary 2.4 induces an isomorphism

$$\Upsilon_{F,\mathfrak{A}} : \mathrm{Ker}(\phi_{\mathfrak{A}}) \xrightarrow{\sim} H(\mathfrak{A}) \subseteq H(A).$$

(c) We have $\mathrm{Ker}(\eta_F) \subseteq \mathrm{Ker}(\phi_{\mathfrak{M}})$.

Proof. (a) Suppose that $\pi : X \to \mathrm{Spec}(F)$ is a G-torsor with $[\pi] \in H^1_{\mathfrak{A}}(F,G)$, and let $\xi_\pi : \mathcal{L}_\pi \otimes_F F^c \xrightarrow{\sim} A_{F^c}$ be a splitting isomorphism for π. Fix a trivialisation $s_\pi : A \xrightarrow{\sim} \mathcal{L}_\pi$. Then the resolvend $\mathbf{r}(s_\pi) \in \mathbf{H}(A)$ (defined using ξ_π) is well-defined up to multiplication by an element of $A^\times$.

For each finite place v of F, write π_v for the torsor $X \otimes_F F_v \to \mathrm{Spec}(F_v)$. Since $[\pi_v] \in H^1_{\mathfrak{A}_v}(F_v,G)$, we may choose a trivialisation $t_{\pi_v} : A_v \xrightarrow{\sim} \mathcal{L}_{\pi_v}$ whose resolvend $\mathbf{r}(t_{\pi_v})$ (computed using the local completion ξ_{π_v} of ξ_π at v) satisfies $\mathbf{r}(t_{\pi_v}) \in \mathbf{H}(\mathfrak{A}_v)$. Then $\mathbf{r}(t_{\pi_v})$ is well-defined up to multiplication by an element of $\mathfrak{A}_v^\times$, and $\mathbf{r}(t_{\pi_v})\mathbf{r}(s_\pi)^{-1} \in A_v^\times$. We also note that $\mathbf{r}(t_{\pi_v})\mathbf{r}(s_\pi)^{-1} \in A_v^\times$ is in fact independent of the choice of the splitting isomorphism ξ_π, because changing ξ_π alters both $\mathbf{r}(s_\pi)$ and $\mathbf{r}(t_{\pi_v})$ by multiplication by the same element of Γ. Furthermore, for all but finitely many places v, both $\mathbf{r}(s_\pi)$ and $\mathbf{r}(t_{\pi_v})$ lie in $\mathbf{H}(\mathfrak{M}_v)$, and so $\mathbf{r}(t_{\pi_v})\mathbf{r}(s_\pi)^{-1} \in \mathfrak{M}_v^\times$ for all such v.

It therefore follows that the element $(\mathbf{r}(t_{\pi_v})\mathbf{r}(s_\pi)^{-1})_v$ lies in $J_f(A)$, and that its image in

$$\frac{J_f(A)}{\left(\prod_{v\nmid\infty} \mathfrak{A}_v^\times\right) \cdot A^\times} \simeq \mathrm{Cl}(\mathfrak{A})$$

is well-defined. We define

$$\phi_{\mathfrak{A}}(\pi) = [(\mathbf{r}(t_{\pi_v})\mathbf{r}(s_\pi)^{-1})_v] \in \mathrm{Cl}(\mathfrak{A}).$$

We now show that $\phi_{\mathfrak{A}}$ is a homomorphism. Suppose that $\pi_i : X_i \to \mathrm{Spec}(F)$ $(i = 1, 2)$ are G-torsors. For each i, fix a splitting isomorphism ξ_{π_i} of π_i, and let s_{π_i} and $t_{\pi i,v}$ $(v \nmid \infty)$ be defined analogously to s_π and t_π above. Then it follows from 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

$$\begin{aligned}
\xi_{\pi_3} &:= \xi_{\pi_1} \otimes \xi_{\pi_2} : (\mathcal{L}_{\pi_1} \otimes_A \mathcal{L}_{\pi_2}) \otimes_F F^c \xrightarrow{\sim} A_{F^c}, \\
s_{\pi_3} &:= s_{\pi_1} \otimes s_{\pi_2} : \mathcal{L}_{\pi_1} \otimes_A \mathcal{L}_{\pi_2} \xrightarrow{\sim} A, \\
t_{\pi_{3,v}} &:= t_{\pi_{1,v}} \otimes t_{\pi_{2,v}} : \mathcal{L}_{\pi_{1,v}} \otimes_{A_v} \mathcal{L}_{\pi_{2,v}} \xrightarrow{\sim} A_v,
\end{aligned}$$

then $\mathbf{r}(s_{\pi_3}) = \mathbf{r}(s_{\pi_1})\mathbf{r}(s_{\pi_2})$, and $\mathbf{r}(t_{\pi_{3,v}}) = \mathbf{r}(t_{\pi_{1,v}})\mathbf{r}(t_{\pi_{2,v}})$ (where, for each i the resolvends $\mathbf{r}(s_{\pi_i})$ and $\mathbf{r}(t_{\pi_{i,v}})$ are defined using the splitting isomorphisms ξ_{π_i} and $\xi_{\pi_{i,v}}$ respectively).

Hence it follows that

$$\begin{aligned}
\phi_{\mathfrak{A}}(\pi_3) &= [(\mathbf{r}(t_{\pi_{3,v}})\mathbf{r}(s_{\pi_3})^{-1})_v] \\
&= [(\mathbf{r}(t_{\pi_{1,v}})\mathbf{r}(s_{\pi_1})^{-1})_v][(\mathbf{r}(t_{\pi_{2,v}})\mathbf{r}(s_{\pi_2})^{-1})_v] \\
&= \phi_{\mathfrak{A}}(\pi_1)\phi_{\mathfrak{A}}(\pi_2),
\end{aligned}$$

as asserted.

(b) Suppose that $\pi : X \to \mathrm{Spec}(F)$ is a G-torsor satisfying $\mathbf{r}(s_\pi) \in \mathbf{H}(\mathfrak{A})$ for some choice of trivialisation $s_\pi : A \xrightarrow{\sim} \mathcal{L}_\pi$ of $\mathcal{L}_\pi$. Write $s_{\pi,v} : A_v \xrightarrow{\sim} \mathcal{L}_{\pi_v}$ for the trivialisation of $\mathcal{L}_{\pi_v}$ induced by s_π. Then $\mathbf{r}(s_{\pi,v}) \in \mathbf{H}(\mathfrak{A}_v)$ for all finite places v of F. Hence $\pi \in H^1_{\mathfrak{A}}(F, G)$, and we may take $t_{\pi_v} = s_{\pi,v}$ in the definition of $\phi_{\mathfrak{A}}(\pi)$ given in part (a). This in turn gives $\phi_{\mathfrak{A}}(\pi) = 0$.

Now suppose conversely that $\pi \in H^1_{\mathfrak{A}}(F, G)$ with $\phi_{\mathfrak{A}}(\pi) = 0$. Then for any trivialisations s_π and $\mathbf{r}(t_{\pi_v})$ chosen as in part (a), we have

$$(\mathbf{r}(t_{\pi_v})\mathbf{r}(s_\pi)^{-1})_v = \alpha \cdot (\beta_v)_v \in A^\times \cdot \prod_{v \nmid \infty} \mathfrak{A}_v^\times.$$

Hence if we replace s_π by $s'_\pi := \alpha s_\pi$, then

$$(\mathbf{r}(t_{\pi_v})\mathbf{r}(s'_\pi)^{-1})_v = (\beta_v)_v \in \prod_{v \nmid \infty} \mathfrak{A}_v^\times \subseteq \prod_{v \nmid \infty} \mathbf{H}(\mathfrak{A}_v).$$

This implies that $\mathbf{r}(s'_\pi) \in \mathbf{H}(\mathfrak{A}_v)$ for each place $v \nmid \infty$, and so it follows that $\mathbf{r}(s'_\pi) \in \mathbf{H}(\mathfrak{A})$. Hence $\Upsilon_F(\pi) \in H(\mathfrak{A}) \subseteq H(A)$, as claimed.

(c) This follows directly from Remark 3.3 and part (b) above. ☐

Example 3.5. Suppose that F is a number field. Let $\mathcal{G}$ be a finite, flat, commutative group scheme over $\mathrm{Spec}(O_F)$, with generic fibre G. Let $\mathcal{G}^* = \mathrm{Spec}(\mathfrak{A})$ denote the Cartier dual of $\mathcal{G}^*$; then

$G^* = \operatorname{Spec}(A)$ is the generic fibre of $\mathcal{G}^*$. Corollary 2.4(a) implies that $H^1_{\mathfrak{A}_v}(F_v, G) = H^1(O_{F_v}, G)$ for each finite place v of F, and so it follows that

$$H^1_{\mathfrak{A}}(F, G) = H^1(O_F, \mathcal{G}).$$

Hence we obtain a description of the flat Selmer group of $\mathcal{G}$ in terms of resolvends. In this case, the map

$$\phi_{\mathfrak{A}} : H^1(O_F, \mathcal{G}) \to \mathrm{Cl}(\mathfrak{A}) \simeq \mathrm{Pic}(\mathcal{G}^*)$$

is the same as the class invariant homomorphism (1.1) for the group $\mathcal{G}$.

Also, we have

$$H^1(O_F, \mathcal{G}) = H^1_{\mathfrak{A}}(F, G) \subseteq H^1_{\mathfrak{M}}(F, G),$$

and $\operatorname{Spec}(\mathfrak{M})$ is the normalisation of $\mathcal{G}^*$. The restriction of the homomorphism

$$\phi_{\mathfrak{M}} : H^1_{\mathfrak{M}}(F, G) \to \mathrm{Cl}(\mathfrak{M}) \simeq \mathrm{Pic}(\operatorname{Spec}(\mathfrak{M}))$$

to $H^1(O_F, \mathcal{G})$ is the same as the class invariant homomorphism (1.2). $\square$

Remark 3.6. Suppose that F is a number field, and let N denote the exponent of G. If v is a place of F with $v \nmid N$, set

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

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

If $\pi \in H^1_f(F_v, G)$, and $\mathbf{r}(s_\pi)$ is any resolvend asociated to π, then Proposition 2.7 implies that $\mathbf{r}(s_\pi) \in A^\times_{v, F_v^{\mathrm{nr}}}$. Since F_v^{nr}/F_v is unramified, it follows (via considering the Wedderburn decomposition (2.3) of A_v) that there exists $\alpha \in A_v^\times$ such that $\alpha^{-1}\mathbf{r}(s_\pi) = \mathbf{r}(\alpha^{-1}s_\pi) \in \mathfrak{M}^\times_{v, O_{F_v^{\mathrm{nr}}}}$. This implies that $\pi \in H^1_{\mathfrak{M}}(F, G)$, and so

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

Suppose further that G is unramified at v. Then $\mathcal{G} := \operatorname{Spec}(\mathfrak{M}_v)$ is a finite, flat, commutative O_{F_v}-group scheme, and it is a standard result that $H^1_f(F_v, G) = H^1(O_{F_v}, \mathcal{G})$. We therefore deduce that in this case, we have $H^1_f(F_v, G) = H^1_{\mathfrak{M}}(F_v, G)$. $\square$

Remark 3.7. It is not difficult to define refinements of the homomorphism $\phi_{\mathfrak{A}}$ taking values in relative algebraic K-groups as in [4], or in Arakelov Picard groups as in [5]. However, for the sake of brevity, we shall not go into this here. $\square$

Now suppose that F is a number field, and let L/F be a finite extension. It is not hard to check that the homomorphism $\mathcal{N}_{L/F}$ of (2.5) induces a homomorphism

$$\mathcal{N}_{L/K} : \mathrm{Cl}(\mathfrak{A}_{O_L}) \to \mathrm{Cl}(\mathfrak{A}).$$

Proposition 3.8. *If F is a number field, and L/F is a finite extension, then the following diagram is commutative:*

$$\begin{tikzcd} H^1_{\mathfrak{A}_{O_L}}(L,G) \arrow[r, "\phi_{\mathfrak{A}_{O_L}}"] \arrow[d, "\mathrm{Cores}_{L/F}"'] & \mathrm{Cl}(\mathfrak{A}_{O_L}) \arrow[d, "\mathcal{N}_{L/F}"'] \\ H^1_{\mathfrak{A}}(F,G) \arrow[r, "\phi_{\mathfrak{A}}"] & \mathrm{Cl}(\mathfrak{A}). \end{tikzcd} \tag{3.2}$$

Proof. Let $\pi : X \to \mathrm{Spec}(L)$ be a G-torsor with $[\pi] \in H^1_{\mathfrak{A}_{O_L}}(L,G)$, and let $s_\pi : A_L \xrightarrow{\sim} \mathcal{L}_\pi$ be any trivialisation of $\mathcal{L}_\pi$. For each finite place v of L, let $t_{\pi_v} : A_{L_v} \xrightarrow{\sim} \mathcal{L}_{\pi_v}$ be a trivialisation of $\mathcal{L}_{\pi_v}$ satisfying $\mathbf{r}(t_{\pi_v}) \in \mathbf{H}(\mathfrak{A}_{O_{L_v}})$, Then

$$\phi_{\mathfrak{A}_{O_L}}(\pi) = [(\mathbf{r}(t_{\pi_v})\mathbf{r}(s_\pi)^{-1})_v] \in \mathrm{Cl}(\mathfrak{A}_{O_L}).$$

The result now follows via a similar argument to that used in the proof of Proposition 2.9. □

For the rest of this paper, we shall mainly be concerned with the special cases in which $\mathfrak{A} = \mathfrak{M}$ or $\mathfrak{A} = \mathfrak{M} \otimes_{O_F} O_F[1/p] := \mathfrak{M}^{\{p\}}$. We identify $\mathrm{Pic}(\mathrm{Spec}(\mathfrak{M}))$ and $\mathrm{Pic}(\mathrm{Spec}(\mathfrak{M}^{\{p\}}))$ with the locally free classgroups $\mathrm{Cl}(\mathfrak{M})$ and $\mathrm{Cl}(\mathfrak{M}^{\{p\}})$ of $\mathfrak{M}$ and $\mathfrak{M}^{\{p\}}$ respectively. We set

$$H^1_u(F,G) := H^1_{\mathfrak{M}}(F,G), \qquad H^1_{u,\{p\}}(F,G) := H^1_{\mathfrak{M}^{\{p\}}}(F,G),$$

and we write

$$\phi : H^1_u(F,G) \to \mathrm{Cl}(\mathfrak{M}), \quad \phi^{\{p\}} : H^1_{u,\{p\}}(F,G) \to \mathrm{Cl}(\mathfrak{M}^{\{p\}})$$

for the homomorphisms given by Theorem 3.4.

Proposition 3.9. *Let F be a number field, and suppose that G^* is constant over* $\mathrm{Spec}(F)$*.*

(i) If v is any finite place of F, then the isomorphism η_{F_v} of Proposition 2.6 induces an isomorphism

$$H^1_u(F_v,G) \xrightarrow{\sim} \mathrm{Hom}(\Gamma^*, O_{F_v}^\times/(O_{F_v}^\times)^N).$$

(ii) The isomorphism η_F induces isomorphisms

$$\mathrm{Ker}(\phi) \xrightarrow{\sim} \mathrm{Hom}(\Gamma^*, O_F^\times/(O_F^\times)^N),$$
$$\mathrm{Ker}(\phi^{\{p\}}) \xrightarrow{\sim} \mathrm{Hom}(\Gamma^*, O_F[1/p]^\times/(O_F[1/p]^\times)^N)$$

Proof. Since G^* is constant over $\mathrm{Spec}(F)$, we have

$$A \simeq \mathrm{Map}(\Gamma^*, F), \qquad \mathfrak{M} \simeq \mathrm{Map}(\Gamma^*, O_F), \qquad \mathfrak{M}^{\{p\}} \simeq \mathrm{Map}(\Gamma^*, O_F[1/p]).$$

Proposition 2.6 implies that we have isomorphisms

$$H^1(F,G) \simeq \mathrm{Hom}(\Gamma^*, F^\times/(F^\times)^N), \tag{3.3}$$

$$H^1(F_v,G) \simeq \mathrm{Hom}(\Gamma^*, F_v^\times/(F_v^\times)^N). \tag{3.4}$$

Hence (i) follows from (3.4) and the definition of $H^1(F_v, G)$, while (ii) follows from (3.3) together with Theorem 3.4(b). $\square$

4. p-ADIC REPRESENTATIONS

In this section, we shall apply our previous work to the situation described in the introduction. We first recall the relevant notation.

Let F be a number field and V be a d-dimensional $\mathbf{Q}_p$-vector space. Suppose that $\rho : \Omega_F \to \mathrm{GL}(V)$ is a continuous representation which is ramified at only finitely many primes of F. We set $V^* := \mathrm{Hom}_{\mathbf{Q}_p}(V, \mathbf{Q}_p(1))$, and we write $\rho^* : \Omega_F \to \mathrm{GL}(V^*)$ for the corresponding representation of Ω_F. Let $T \subseteq V$ be any Ω_F-stable lattice, and write $T^* := \mathrm{Hom}_{\mathbf{Z}_p}(T, \mathbf{Z}_p(1))$. For each positive integer n, we define finite 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 with $G_n^* = \mathrm{Spec}(A_n)$ for the Hopf algebra $A_n = (F^c\Gamma_n)^{\Omega_F}$ over F.

Recall that $q_n : A_n \to A_{n-1}$ is the homomorphism induced by the dual p_n^D of the multiplication-by-p map $p_n : G_n \to G_{n-1}$. Suppose that, for each n, we are given an O_F-algebra $\mathfrak{A}_n \subseteq A_n$ satisfying the conditions stated at the begining of Section 3. Suppose also that $q_n(\mathfrak{A}_n) = \mathfrak{A}_{n-1}$ for each n. Then it is easy to check that q_n induces homomorphisms

$$\mathbf{H}(A_n) \to \mathbf{H}(A_{n-1}), \quad \text{and} \quad \mathbf{H}(\mathfrak{A}_{n,v}) \to \mathbf{H}(\mathfrak{A}_{n-1,v})$$

for each finite place v of F. This implies that the natural maps

$$H^1(F_v, G_n) \to H^1(F_v, G_{n-1}), \quad H^1(F, G_n) \to H^1(F, G_{n-1})$$

induce homomorphisms

$$H^1_{\mathfrak{A}_{n,v}}(F_v, G_n) \to H^1_{\mathfrak{A}_{n-1,v}}(F_v, G_{n-1}), \quad H^1_{\mathfrak{A}_n}(F, G_n) \to H^1_{\mathfrak{A}_{n-1}}(F, G_{n-1})$$

via restriction.

Set $\mathfrak{A}(T) := \varprojlim \mathfrak{A}_n$ and $\mathfrak{A}_v(T) := \varprojlim \mathfrak{A}_{n,v}$ (where the inverse limits are taken with respect to the maps q_n), and let

$$\mathbf{H}(\mathfrak{A}_v(T)) := \left\{ \alpha \in \mathfrak{A}_v(T)^\times_{O_{F_v^c}} \;\middle|\; \frac{\alpha^\omega}{\alpha} \in T \text{ for all } \omega \in \Omega_{F_v^c}. \right\},$$

$$H(\mathfrak{A}_v(T)) := \frac{\mathbf{H}(\mathfrak{A}_v(T))}{T \cdot \mathfrak{A}_v(T)^\times}.$$

Define $\mathbf{H}(\mathfrak{A}(T))$ and $H(\mathfrak{A}(T))$ in a similar way. Write

$$H^1_{\mathfrak{A}_v(T)}(F_v, T) := \varprojlim H^1_{\mathfrak{A}_{n,v}}(F_v, G_n), \quad H^1_{\mathfrak{A}(T)}(F, T) := \varprojlim H^1_{\mathfrak{A}_n}(F, G_n).$$

Proposition 4.1. *For each finite place v of F, we have*

$$H^1_{\mathfrak{A}_v(T)}(F_v, T) \simeq \frac{\mathbf{H}(\mathfrak{A}_v(T))}{T \cdot \mathfrak{A}_v^\times(T)}.$$

Proof. It follows from the definition of $H^1_{\mathfrak{A}_{n,v}}(F_v, G_n)$ (see Definition 3.1) that, for each n, there is an exact sequence

$$1 \to G_n \cdot \mathfrak{A}_{n,v}^\times \to \mathbf{H}(\mathfrak{A}_{n,v}) \to H^1_{\mathfrak{A}_{n,v}}(F_v, G_n) \to 0.$$

Passing to inverse limits, and using the fact that the inverse system $\{G_n \cdot \mathfrak{A}_{n,v}^\times\}_n$ satisfies the Mittag-Leffler condition yields

$$H^1_{\mathfrak{A}_v(T)}(F_v, T) \simeq \frac{\varprojlim \mathbf{H}(\mathfrak{A}_{n,v})}{T \cdot \mathfrak{A}_v(T)^\times}.$$

It follows easily from the definitions that

$$\mathbf{H}(\mathfrak{A}_v(T)) = \varprojlim \mathbf{H}(\mathfrak{A}_{n,v}),$$

and this implies the result. □

It is easy to check that p_n^D induces pullback homomorphisms

$$(p_n^D)^* : \mathrm{Cl}(\mathfrak{A}_n) \to \mathrm{Cl}(\mathfrak{A}_{n-1}).$$

Let

$$\phi_{\mathfrak{A}_n} : H^1_{\mathfrak{A}_n}(F, G_n) \to \mathrm{Cl}(\mathfrak{A}_n)$$

denote the natural homomorphism afforded by Theorem 3.4.

Theorem 4.2. *The following diagram is commutative:*

$$\begin{tikzcd} H^1_{\mathfrak{A}_n}(F, G_n) \arrow[r, "\phi_{\mathfrak{A}_n}"] \arrow[d, "p_n"'] & \mathrm{Cl}(\mathfrak{A}_n) \arrow[d, "(p_n^D)^*"] \\ H^1_{\mathfrak{A}_{n-1}}(F, G_{n-1}) \arrow[r, "\phi_{\mathfrak{A}_{n-1}}"] & \mathrm{Cl}(\mathfrak{A}_{n-1}), \end{tikzcd} \tag{4.1}$$

Proof. The proof of this is similar to that of Proposition 2.10. Let $\pi_n : X_n \to \mathrm{Spec}(F)$ be a G_n-torsor with $[\pi_n] \in H^1_{\mathfrak{A}_n}(F, G_n)$, and write $\pi_{n-1} := p_n(\pi_n)$. Fix a splitting isomorphism ξ_{π_n} of π_n. Let $s_{\pi_n} : A_n \xrightarrow{\sim} \mathcal{L}_{\pi_n}$ be any trivialisation of $\mathcal{L}_{\pi_n}$, and for each finite place v of F, let $t_{\pi_n,v} : A_{n,v} \xrightarrow{\sim} \mathcal{L}_{\pi_n,v}$ be a trivialisation of $\mathcal{L}_{\pi_n,v}$ satisfying $\mathbf{r}(t_{\pi_n,v}) \in \mathbf{H}(\mathfrak{A}_{n,v})$ (where $\mathbf{r}_{\pi_n,v}$ is defined using the splitting isomorphism $\xi_{\pi_n,v}$ of $\pi_{n,v}$ induced by $\xi_{\pi_n,v}$.

Then, via functoriality, we have that $(p_n^D)^*\mathcal{L}_{\pi_n} \simeq \mathcal{L}_{\pi_{n-1}}$. The pullbacks $(p_n^D)^* s_{\pi_n}$ and $(p_n^D)^* t_{\pi_n,v}$ of s_{π_n} and $t_{\pi_n,v}$ along p_n^D give trivialisations of $\mathcal{L}_{\pi_{n-1}}$ and $\mathcal{L}_{\pi_{n-1},v}$ respectively, while $(p_n^D)^*\xi_{\pi_n}$ and $(p_n^D)^*\xi_{\pi_n,v}$ are splitting isomorphisms of π_{n-1} and $\pi_{n-1,v}$ respectively. We have that

$$\mathbf{r}((p_n^D)^* t_{\pi_n,v}) = q_{n,v}(t_{\pi_n,v}) \in \mathbf{H}(\mathfrak{A}_{n-1,v}),$$

where $\mathbf{r}((p_n^D)^* t_{\pi_n,v})$ is defined using $(p_n^D)^*\xi_{\pi_n,v}$. The result now follows from the definitions of $\phi_{\mathfrak{A}_n}$ and $\phi_{\mathfrak{A}_{n-1}}$. $\square$

Set

$$\mathrm{Cl}(\mathfrak{A}(T)) := \varprojlim \mathrm{Cl}(\mathfrak{A}_n).$$

Then passing to inverse limits over the diagrams (4.1) yields a homomorphism

$$\Phi_{\mathfrak{A}(T)} : H^1_{\mathfrak{A}(T)}(F, T) \to \mathrm{Cl}(\mathfrak{A}(T)). \tag{4.2}$$

Proposition 4.3. *Suppose that L/F is a finite extension. Then the map $\mathcal{N}_{L/K}$ (see (2.5)) induces a homomorphism*

$$\mathcal{N}_{L/K} : \mathrm{Cl}(\mathfrak{A}(T)_{O_L}) \to \mathrm{Cl}(\mathfrak{A}(T)),$$

and the following diagram is commutative:

$$\begin{array}{ccc} H^1_{\mathfrak{A}(T)_{O_L}}(F, G) & \xrightarrow{\phi_{\mathfrak{A}(T)_{O_L}}} & \mathrm{Cl}(\mathfrak{A}(T)_{O_L}) \\ {\scriptstyle \mathrm{Cores}_{L/F}}\big\downarrow & & {\scriptstyle \mathcal{N}_{L/F}}\big\downarrow \\ H^1_{\mathfrak{A}(T)}(F, G) & \xrightarrow{\phi_{\mathfrak{A}(T)}} & \mathrm{Cl}(\mathfrak{A}(T)). \end{array} \tag{4.3}$$

Proof. This follows from Proposition 3.8. $\square$

Proposition 4.4. *There is an isomorphism*

$$\Upsilon_{F,\mathfrak{A}(T)} : \mathrm{Ker}(\Phi_{\mathfrak{A}(T)}) \xrightarrow{\sim} H(\mathfrak{A}(T)) \subseteq H(A(T)).$$

Proof. This follows easily from Theorem 3.4(b). $\square$

Write

$$H^1_u(F, T) := \varprojlim H^1_u(F, G_n), \qquad H^1_{u,\{p\}}(F, T) := \varprojlim H^1_{u,\{p\}}(F, G_n).$$

Then (4.2) yields a homomorphism

$$\Phi_F := \Phi_{\mathfrak{M}(T)} : H^1_u(F, T) \to \mathrm{Cl}(\mathfrak{M}(T)). \tag{4.4}$$

From Remark 3.6, we see that

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

Hence, restricting $\Phi_{\mathfrak{M}^{\{p\}}(T)}$ to $H^1_{f,\{p\}}(F, T)$ yields a homomorphism

$$\Phi_F^{\{p\}} : H^1_{f,\{p\}}(F, T) \to \mathrm{Cl}(\mathfrak{M}^{\{p\}}(T)).$$

Remark 4.5. Let S be any finite set of places of F containing all places lying above p, as well as all places at which T is ramified, and let F^S/F denote the maximal extension of F which is unramified outside S. Then it follows from the definitions that $H^1_u(F, T) \subseteq H^1(F^S/F, T)$, and so we deduce that $H^1_u(F, T)$ is always a finitely generated $\mathbf{Z}_p$-module. $\square$

Remark 4.6. Suppose that $\mathcal{A}$ is an abelian scheme over $\mathrm{Spec}(O_F)$, and let T denote its p-adic Tate module. For each positive integer n, let $\mathcal{G}_n$ denote the O_F-group scheme of p^n-torsion on $\mathcal{A}$, and write $\mathcal{G}_n^*$ for its Cartier dual. Then taking inverse limits of the homomorphisms

$$\psi_n : H^1(\mathrm{Spec}(O_F), \mathcal{G}_n) \to \mathrm{Pic}(\mathcal{G}_n^*)$$

yield a homomorphism

$$\Psi_F : H^1_f(F, T) \to \varprojlim \mathrm{Pic}(\mathcal{G}_n^*)$$

(see [1], [6], [5]). It seems reasonable to conjecture that Ψ_F is injective modulo torsion. In [6], this conjecture is shown to be true (subject to certain technical hypotheses) when $\mathcal{A}_{/F}$ is an elliptic curve and p is a prime of ordinary reduction. □

Example 4.7. Let v be a place of F lying above p. In general, the group $H^1_u(F_v, T)$ is not equal to the group $H^1_f(F_v, T)$ introduced by Bloch and Kato in [7]. In order to illustrate this, we apply the theory developed above to the example of the Tate twist $T = \mathbf{Z}_p(i)$ ($i \in \mathbf{Z}$) for an odd prime p.

Assume for simplicity of exposition that F_v contains no non-trivial roots of unity of p-power order. Fix a generator $(\zeta_{p^n})_{n \geq 0}$ of $\mathbf{Z}_p(1)$; such a choice also determines a generator (which we shall denote by $(\zeta_{p^n}^{\otimes i})_n$) of $\mathbf{Z}_p(i)$ for each $i \in \mathbf{Z}$. Write $G_n^{(i)}$ for the group scheme over $\mathrm{Spec}(F_v)$ defined by

$$G_n^{(i)}(F_v^c) = \Gamma_n^{(i)} := p^{-n}\mathbf{Z}_p(i)/\mathbf{Z}_p(i).$$

The Cartier dual of $G_n^{(i)}$ is $G_n^{(1-i)}$, and we have $G_n^{(i)} = \mathrm{Spec}(A_n^{(i)})$, where

$$A_n^{(i)} = (F_v^c[\Gamma_n^{(1-i)}])^{\Omega_{F_v}}.$$

For each $i \in \mathbf{Z}$, and each non-negative integer j, let $F_v[\zeta_{p^j}^{\otimes i}]$ denote the smallest extension of F_v whose absolute Galois group fixes $\zeta_{p^j}^{\otimes i}$ (cf. Remark 2.5), i.e.

$$F_v[\zeta_{p^j}^{\otimes i}] = \begin{cases} F_v(\zeta_{p^j}), & \text{if } i \neq 0; \\ F_v & \text{if } i = 0. \end{cases}$$

Then, if $i \neq 0$, Remark 2.5 implies that the Wedderburn decomposition of $A_n^{(i)}$ is given by

$$A_n^{(i)} \simeq \oplus_{j=0}^{n} F_v[\zeta_{p^j}^{\otimes i}] = \oplus_{j=0}^{n} F_v(\zeta_{p^j}),$$

and if $i = 0$ (so $G_n^{(i)}$ is a constant group scheme), then

$$A_n^{(0)} \simeq \oplus_{j=0}^{p^n-1} F_v.$$

Let $k_n^{(i)}$ denote the following sequence of maps:

$$H^1(F_v, \mathbf{Z}_p(1)) \to H^1(F_v, \mu_{p^n}^{\otimes i}) \to H^1(F_v[\zeta_{p^n}^{\otimes(1-i)}], \mu_{p^n}^{\otimes i}) \xrightarrow{\sim}$$
$$H^1\left(\Gamma_n^{(1-i)}, \frac{F_v[\zeta_{p^n}^{\otimes(1-i)}]^\times}{F_v[\zeta_{p^n}^{\otimes(1-i)}]^{\times p^n}}\right) \to \frac{F_v[\zeta_{p^n}^{\otimes(1-i)}]^\times}{F_v[\zeta_{p^n}^{\otimes(1-i)}]^{\times p^n}}.$$

Here:

- the first arrow is induced by the natural quotient map $\mathbf{Z}_p(i) \to \mu_{p^n}^{\otimes i}$;
- the second arrow is given by corestriction;
- the third arrow is defined via the isomorphism afforded by Proposition 2.6;
- the fourth arrow is induced by "evaluation at $\zeta_{p^n}^{\otimes(1-i)}$".

Suppose now that $c \in H^1(F_v, \mathbf{Z}_p(i))$. It follows from the definitions that $c \in H^1_u(F_v, \mathbf{Z}_p(i))$ if and only if, for each $n \geq 0$, we have

$$k_n^{(i)}(c) \in \frac{O^\times_{F_v[\zeta_{p^n}^{\otimes(1-i)}]} \cdot F_v[\zeta_{p^n}^{\otimes(1-i)}]^{\times p^n}}{F_v[\zeta_{p^n}^{\otimes(1-i)}]^{\times p^n}}.$$

The cohomology groups $H^1(F_v, \mathbf{Z}_p(i))$ may be described using 'twisted Kummer theory' in the following way (see [26]). Set

$$X := \varprojlim F_v(\zeta_{p^n})^\times, \quad Y := \varprojlim O^\times_{F_v(\zeta_{p^n})},$$

where the inverse limits are taken with respect to the norm maps $N_n : F_v(\zeta_{p^n}) \to F_v(\zeta_{p^{n-1}})$. Let $H_\infty := \mathrm{Gal}(F_v(\zeta_{p^\infty})/F_v)$. A theorem of Iwasawa (see [16, Theorem 25]) implies that X and Y are $\mathbf{Z}_p[[H_\infty]]$-modules of rank $[F_v : \mathbf{Q}_p]$.

For each integer i, we write

$$X(i) := X \otimes_{\mathbf{Z}_p} \mathbf{Z}_p(i), \quad Y(i) := Y \otimes_{\mathbf{Z}_p} \mathbf{Z}_p(i).$$

The group H_∞ acts on $X(i)$ and $Y(i)$ diagonally. We write $X(i)_{H_\infty}$ and $Y(i)_{H_\infty}$ for the group of coinvariants of the H_∞-modules $X(i)$ and $Y(i)$ respectively.

Define a homomorphism

$$\tilde{\varphi}_i : X(i-1)_{H_\infty} \to H^1(F_v, \mathbf{Z}_p(i))$$

by

$$\tilde{\varphi}_i((u_n \otimes \zeta_{p^n}^{\otimes(i-1)})_n) = (N_n(u_n \cup z_n^{i-1}))_n,$$

where $z_n \in H^0(F_v(\zeta_{p^n}), \mu_{p^n})$ is the element corresponding to ζ_{p^n}, and $u_n \in F_v(\zeta_{p^n})^\times / F_v(\zeta_{p^n})^{\times p^n}$. It is shown in [26, §2] that $\tilde{\varphi}_i$ is well-defined, and is an isomorphism for $i \geq 2$. It may be checked that the same proof shows that $\tilde{\varphi}_i$ is also an isomorphism if $i \leq -1$. The theorem of Iwasawa mentioned above (together with standard Kummer theory and local Tate duality for the cases $i = 0$ and $i = 1$) then leads to the following result (cf. [26, p. 390, Remark 1]):

$$rk_{\mathbf{Z}_p}\left(H^1(F_v, \mathbf{Z}_p(i))\right) = \begin{cases} [F_v : \mathbf{Q}_p], & \text{if } i \leq -1; \\ [F_v : \mathbf{Q}_p] + 1, & \text{if } i = 0 \text{ or } i = 1; \\ [F_v : \mathbf{Q}_p], & \text{if } i \geq 2. \end{cases}$$

If $i \neq 1$ and $c \in \tilde{\varphi}_i(Y(i-1)_{H_\infty})$, then it may be checked that

$$k_n^{(i)}(c) \in \frac{O^\times_{F_v(\zeta_{p^n})} \cdot F_v(\zeta_{p^n})^{\times p^n}}{F_v(\zeta_{p^n})^{\times p^n}}$$

for all $n \geq 0$. This implies that $\tilde{\varphi}_i(Y(i-1)_{H_\infty}) \subseteq H^1_u(F_v, \mathbf{Z}_p(i))$ if $i \neq 1$. It may be shown using Iwasawa's theorem, together with (4.5) and a separate analysis of the case $i = 1$, that

$$\mathrm{rk}\left(H^1_u(F_v, \mathbf{Z}_p(i))\right) = [F_v : \mathbf{Q}_p]$$

for all $i \in \mathbf{Z}$.

On the other hand, it follows from the theory of Bloch and Kato (see [7, Example 3.9]) that

$$\mathrm{rk}_{\mathbf{Z}_p}\left(H^1_f(F_v, \mathbf{Z}_p(i))\right) = \begin{cases} 0, & \text{if } i \leq -1; \\ 1, & \text{if } i = 0; \\ [F_v : \mathbf{Q}_p], & \text{if } i \geq 1. \end{cases}$$

Hence, if $i \leq -1$, for example, then $H^1_u(F_v, \mathbf{Z}_p(i))$ is never equal to $H^1_f(F_v, \mathbf{Z}_p(i))$. $\square$

5. Proof of Theorem 1.4

In this section we give the proof of Theorem 1.4.

For each integer n the action of Ω_F on Γ_n^* yields a representation

$$\rho_n^* : \Omega_F \to \mathrm{Aut}(\Gamma_n^*).$$

Write F_n^* for the fixed field of ρ_n^*; then $F_\infty^* = \cup_n F_n^*$, where F_∞^* is the extension of F cut out by ρ^*. The group scheme G_n^* is constant over $\mathrm{Spec}(F_n^*)$, and we write

$$\eta_{n,F_n^*} : \mathrm{Ker}(\phi_{n,F_n^*}) \xrightarrow{\sim} \mathrm{Hom}(\Gamma_n^*, O^\times_{F_n^*}/(O^\times_{F_n^*})^{p^n})$$

for the isomorphism afforded by Proposition 3.9(ii).

Consider the map

$$d_n : H^1(F_n^*, \Gamma_n) \xrightarrow{p_n} H^1(F_n^*, \Gamma_{n-1}) \xrightarrow{\mathrm{Cores}_{F_n^*/F_{n-1}^*}} H^1(F_{n-1}^*, \Gamma_{n-1}).$$

Lemma 5.1. *Passing to the inverse limit of the maps*

$$d_n : H^1(F_n^*, \Gamma_n) \to H^1(F_{n-1}^*, \Gamma_{n-1})$$

induces isomorphisms

$$\varprojlim H^1(F_n^*, \Gamma_n) \xrightarrow{\sim} \varprojlim H^1(F_n^*, T), \tag{5.1}$$

$$\varprojlim H^1(F_{n,v}^*, \Gamma_n) \xrightarrow{\sim} \varprojlim H^1(F_{n,v}^*, T) \tag{5.2}$$

Proof. See e.g. [25, Lemma B.3.1]. □

Let h_n denote the composition

$$\begin{aligned} h_n : \mathrm{Hom}(\Gamma_n^*, F_n^{*\times}/(F_n^{*\times})^{p^n}) &\xrightarrow{r_n} \mathrm{Hom}(\Gamma_{n-1}^*, F_n^{*\times}/(F_n^{*\times})^{p^{n-1}}) \\ &\xrightarrow{N_{F_n^*/F_{n-1}^*}} \mathrm{Hom}(\Gamma_{n-1}^*, F_{n-1}^{*\times}/(F_{n-1}^{*\times})^{p^{n-1}}), \end{aligned}$$

where r_n is defined in Corollary 2.12, and $N_{F_n^*/F_{n-1}^*}$ is induced by the norm map from F_n^* to F_{n-1}^*.

We remind the reader that, for any $\mathbf{Z}$-module Q, we set

$$\check{Q} := \varprojlim_n Q/p^n Q.$$

Lemma 5.2. *Passing to the inverse limit of the maps*

$$h_n : \mathrm{Hom}(\Gamma_n^*, F_n^{*\times}/(F_n^{*\times})^{p^n}) \to \mathrm{Hom}(\Gamma_{n-1}^*, F_{n-1}^{*\times}/(F_{n-1}^{*\times})^{p^{n-1}})$$

induces isomorphisms

$$\varprojlim \mathrm{Hom}(\Gamma_n^*, F_n^{*\times}/(F_n^{*\times})^{p^n}) \xrightarrow{\sim} \mathrm{Hom}(T^*, \varprojlim \check{F}_n^{*\times}),$$

$$\varprojlim \mathrm{Hom}(\Gamma_n^*, O_{F_n^*}^{\times}/(O_{F_n^*}^{\times})^{p^n}) \xrightarrow{\sim} \mathrm{Hom}(T^*, \check{O}_{F_n^*}^{\times}).$$

Proof. This is proved by applying Lemma 5.1 to the p-divisible group schemes $(\mathbf{Z}/p^n\mathbf{Z})_{n\geq 1}$ and $(\boldsymbol{\mu}_{p^n})_{n\geq 1}$. We have

$$\begin{aligned} \varprojlim[\mathrm{Hom}(\Gamma_n^*, F_n^{*\times}/(F_n^{*\times})^{p^n})] &= \varprojlim[\mathrm{Hom}(\Gamma_n^*, \mathbf{Z}/p^n\mathbf{Z}) \otimes_{\mathbf{Z}_p} (F_n^{*\times}/(F_n^{*\times})^{p^n})] \\ &= [\varprojlim \mathrm{Hom}(\Gamma_n^*, \mathbf{Z}/p^n\mathbf{Z})] \otimes_{\mathbf{Z}_p} [\varprojlim(F_n^{*\times}/(F_n^{*\times})^{p^n})] \\ &= \mathrm{Hom}(T^*, \mathbf{Z}_p) \otimes_{\mathbf{Z}_p} \varprojlim H^1(F_n^*, \mu_{p^n}) \\ &= \mathrm{Hom}(T^*, \mathbf{Z}_p) \otimes_{\mathbf{Z}_p} \varprojlim H^1(F_n^*, \mathbf{Z}_p(1)) \\ &= \mathrm{Hom}(T^*, \mathbf{Z}_p) \otimes_{\mathbf{Z}_p} \varprojlim \check{F}_n^{*\times} \\ &= \mathrm{Hom}(T^*, \varprojlim \check{F}_n^{*\times}). \end{aligned}$$

The second isomorphism may be established in a similar manner. □

Lemma 5.3. *The following diagram is commutative:*

$$\begin{tikzcd} H^1(F_n^*, \Gamma_n) \arrow[r, "\eta_{n,F_n^*}"] \arrow[d, "d_n"'] & \mathrm{Hom}(\Gamma_n^*, F_n^{*\times}/(F_n^{*\times})^{p^n}) \arrow[d, "h_n"] \\ H^1(F_{n-1}^*, \Gamma_{n-1}) \arrow[r, "\eta_{n-1,F_{n-1}^*}"] & \mathrm{Hom}(\Gamma_{n-1}^*, F_{n-1}^{*\times}/(F_{n-1}^{*\times})^{p^{n-1}}). \end{tikzcd} \tag{5.3}$$

Proof. Note that G_n^* is constant over $\mathrm{Spec}(F_n^*)$. The result now follows from Proposition 2.9 and Corollary 2.12. □

Passing to inverse limits over the diagrams (5.3), and applying Lemmas 5.1 and 5.2 yields a natural isomorphism

$$\beta : \varprojlim H^1(F_n^*, T) \xrightarrow{\sim} \mathrm{Hom}(T^*, \varprojlim \check{F}_n^{*\times}). \tag{5.4}$$

For each finite place v of F, similar arguments to those given above show that there is also a local isomorphism

$$\beta_v : \varprojlim H^1(F_{n,v}^*, T) \xrightarrow{\sim} \mathrm{Hom}(T^*, \varprojlim \check{F}_{n,v}^{*\times}). \tag{5.5}$$

Proposition 5.4. *(i) For each finite place v of F, the map β_v induces an isomorphism (which we denote by the same symbol)*

$$\beta_v : \varprojlim H^1_u(F_{n,v}^*, T) \xrightarrow{\sim} \mathrm{Hom}(T^*, \varprojlim \check{O}^{\times}_{F_{n,v}^*}). \tag{5.6}$$

(ii) The map β induces an isomorphism

$$\beta : \varprojlim H^1_u(F_n^*, T) \xrightarrow{\sim} \mathrm{Hom}(T^*, \varprojlim \check{O}^{\times}_{F_n^*}). \tag{5.7}$$

Proof. (i) It is easy to check that (5.2) induces an isomorphism

$$\varprojlim H^1_u(F_{n,v}^*, \Gamma_n) \xrightarrow{\sim} \varprojlim H^1_u(F_{n,v}^*, T).$$

The result now follows from the isomorphism

$$H^1_u(F_{n,v}^*, G_n) \xrightarrow{\sim} \mathrm{Hom}(\Gamma_n^*, O^{\times}_{F_{n,v}^*}/(O^{\times}_{F_{n,v}^*})^{p^n})$$

afforded by Proposition 3.9(i).

(ii) Suppose that $f \in \mathrm{Hom}(T^*, \varprojlim \check{F}_n^{*\times})$. For each finite place v of F, write f_v for the image of f in $\mathrm{Hom}(T^*, \varprojlim \check{F}_{n,v}^{*\times})$. Then $f_v \in \mathrm{Hom}(T^*, \varprojlim O^{\times}_{F_n^*,v})$ for all v if and only if $f \in \mathrm{Hom}(T^*, \varprojlim \check{O}^{\times}_{F_n^*})$. The result now follows from (i) above. □

Corollary 5.5. *There is a natural isomorphism*

$$\varprojlim H^1_u(F_n^*, T) \simeq \varprojlim \mathrm{Ker}(\Phi_{F_n^*}).$$

Proof. This follows directly from (5.6), Lemma 5.2, and Proposition 3.9(ii). □

Corollary 5.5 implies that we have

$$\cap_n \operatorname{Cores}_{F_n^*/F}(H^1_u(F_n^*,T)) \subseteq \operatorname{Ker}(\Phi_F).$$

Hence, if $x \in \mathfrak{C}_F(T)$, then for some integer $M > 0$, we have $\Phi_F(Mx) = M\Phi_F(x) = 0$, and so $\Phi_F(x)$ is of finite order. This proves Theorem 1.4.

6. Proof of Theorem 1.1

This section is devoted to the proof of Theorem 1.1.

Recall that $C_\infty = \cup_n C_n$ denotes the cyclotomic $\mathbf{Z}_p$-extension of F. We begin by showing that if $x \in \mathfrak{G}_F(T)$, then $\Phi_F^{\{p\}}(x)$ is of finite order.

Lemma 6.1. *Suppose that $m \geq 1$. Then*

$$\varprojlim \operatorname{Cl}(\mathfrak{M}^{\{p\}}_{m,O_{C_n}}) = 0,$$

where the inverse limit is taken with respect to the maps $\mathcal{N}_{C_n/C_{n-1}}$.

Proof. In order to ease notation somewhat, we write $\mathfrak{M}^{\{p\}}$ for $\mathfrak{M}^{\{p\}}_m$. Using the notation of Remark 2.5, we have

$$\mathfrak{M}^{\{p\}}_{C_n} \simeq \prod_{\gamma^* \in \Gamma_m \backslash \Omega_{C_n}} O_{C_n[\gamma^*]}[1/p],$$

and so

$$\operatorname{Cl}(\mathfrak{M}^{\{p\}}_{C_n}) \simeq \prod_{\gamma^* \in \Gamma_m \backslash \Omega_{C_n}} \operatorname{Cl}(O_{C_n[\gamma^*]}[1/p]).$$

Choose $d \geq 1$ sufficiently large that

$$\Gamma_m^* \backslash \Omega_{C_d} = \Gamma_m^* \backslash \Omega_{C_i}$$

for all $i \geq d$. Then, for each $\gamma^* \in \Gamma_m^* \backslash \Omega_{C_d}$

$$C_\infty[\gamma^*] := \cup_{i \geq d} C_i[\gamma^*]$$

is the cyclotomic $\mathbf{Z}_p$-extension of $C_d[\gamma^*]$, and the map

$$\mathcal{N}_{C_i/C_d} : \operatorname{Cl}(\mathfrak{M}^{\{p\}}_{O_{C_i}}) \to \operatorname{Cl}(\mathfrak{M}^{\{p\}}_{C_d})$$

is induced by the usual norm maps

$$\operatorname{Cl}(O_{C_i[\gamma^*]}[1/p]) \to \operatorname{Cl}(O_{C_d[\gamma^*]}[1/p])$$

for each $\gamma^* \in \Gamma_m^* \backslash \Omega_{C_i} = \Gamma_m^* \backslash \Omega_{C_d}$.

However, if L is any number field, and $L_\infty = \cup_j L_j$ is the cyclotomic $\mathbf{Z}_p$-extension of L, then it is easy to show that $\varprojlim \operatorname{Cl}(O_{L_j}[1/p]) = 0$. Hence we have

$$\varprojlim \operatorname{Cl}(O_{C_i[\gamma^*]}[1/p]) = 0 \quad (i \geq d),$$

and so it follows that

$$\varprojlim \mathrm{Cl}(\mathfrak{M}^{\{p\}}_{O_{C_n}}) = 0,$$

as claimed. □

Corollary 6.2. *We have* $\varprojlim \mathrm{Cl}(\mathfrak{M}^{\{p\}}_{O_{C_n}}(T)) = 0$, *where the inverse limit is taken with respect to the maps* $\mathcal{N}_{C_n/C_{n-1}}$. □

Proposition 6.3. *Suppose that* $x \in \mathfrak{G}_F(T)$. *Then* $\Phi^{\{p\}}_F(x)$ *is of finite order.*

Proof. Taking inverse limits over (4.3) yields a homomorphism

$$\varprojlim \Phi^{\{p\}}_{C_n} : \varprojlim H^1_{\mathfrak{M}(T)_{O_{C_n}}}(C_n, T) \to \varprojlim \mathrm{Cl}(\mathfrak{M}^{\{p\}}_{O_{C_n}}(T)),$$

and Corollary 6.2 implies that this is the zero map. Hence

$$\cap_n \mathrm{Cores}_{C_n/F}(H^1_{\mathfrak{M}(T)_{O_{C_n}}}(C_n, T)) \subseteq \mathrm{Ker}(\Phi^{\{p\}}_F).$$

Thus, if $x \in \mathfrak{G}_F(T)$, then $M\Phi^{\{p\}}_F(x) = \Phi^{\{p\}}_F(Mx) = 0$ for some integer $M > 0$. This establishes the result. □

We now 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 [22, 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

$$0 \to T^* \to T'_y \to \mathbf{Z}_p \to 0. \tag{6.1}$$

Taking $\mathbf{Z}_p(1)$-duals of (6.1) yields an exact sequence

$$1 \to \mathbf{Z}_p(1) \to T_y \to T \to 0. \tag{6.2}$$

We may consider the global and local Galois cohomology of (6.2) for each finite place v of F:

$$\begin{array}{ccccccc} H^1(F, \mathbf{Z}_p(1)) & \xrightarrow{i} & H^1(F, T_y) & \xrightarrow{j} & H^1(F, T) & \longrightarrow & H^2(F, \mathbf{Z}_p(1)) \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ H^1(F_v, \mathbf{Z}_p(1)) & \xrightarrow{i_v} & H^1(F_v, T_y) & \xrightarrow{j_v} & H^1(F_v, T) & \longrightarrow & H^2(F_v, \mathbf{Z}_p(1)). \end{array} \tag{6.3}$$

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 (6.2) splits locally at v because $y \in \mathrm{Ker}(\mathrm{Loc}_{F,T^*})$, and so we have a corresponding splitting

$$H^1(F_v, T_y) = H^1(F_v, \mathbf{Z}_p(1)) \oplus H^1(F_v, T) \tag{6.4}$$

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 (6.3) 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 (6.4). 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

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

(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 [22, 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 $\Phi_{\mathfrak{M}^{\{p\}}(T)}$ by interpreting the pairing B_F in terms of resolvends.

In order to ease notation in what follows, we shall write $\Phi^{\{p\}}_{\mathbf{Z}_p(1)}$, $\Phi^{\{p\}}_{T_y}$ and $\Phi^{\{p\}}_{T}$ for $\Phi_{\mathfrak{M}^{\{p\}}(\mathbf{Z}_p(1))}$, $\Phi_{\mathfrak{M}^{\{p\}}(T_y)}$, and $\Phi_{\mathfrak{M}^{\{p\}}(T)}$ respectively.

Proposition 6.4. *Set $h_F := |\operatorname{Cl}(O_F[1/p])|$, and suppose that $\Phi^{\{p\}}_T(x) = 0$. Then there exists $\tilde{x} \in H^1_{f,\{p\}}(F, T_y)$ such that $j(\tilde{x}) = h_F x$ and $\Phi^{\{p\}}_{T_y}(\tilde{x}) = 0$.*

Proof. It is not hard to check that (6.2) yields sequences (which are exact in the middle, and where we denote maps on resolvends by the same symbols as the corresponding maps on cohomology groups):

$$\mathbf{H}(A(\mathbf{Z}_p(1))) \xrightarrow{i} \mathbf{H}(A(T_y)) \to \mathbf{H}(A(T)),$$
$$\mathbf{H}(A_v(\mathbf{Z}_p(1))) \xrightarrow{i_v} \mathbf{H}(A_v(T_y)) \to \mathbf{H}(A_v(T)),$$
$$\mathbf{H}(\mathfrak{M}(\mathbf{Z}_p(1))) \xrightarrow{i} \mathbf{H}(\mathfrak{M}(T_y)) \to \mathbf{H}(\mathfrak{M}(T)),$$
$$\mathbf{H}(\mathfrak{M}_v(\mathbf{Z}_p(1))) \xrightarrow{i_v} \mathbf{H}(\mathfrak{M}_v(T_y)) \to \mathbf{H}(\mathfrak{M}_v(T)).$$

It therefore follows from (3.1) that (6.2) induces a sequence

$$\operatorname{Cl}(\mathfrak{M}^{\{p\}}(\mathbf{Z}_p(1))) \to \operatorname{Cl}(\mathfrak{M}^{\{p\}}(T_y)) \to \operatorname{Cl}(\mathfrak{M}^{\{p\}}(T))$$

of classgroups which is exact in the middle. We therefore deduce via functoriality that the following diagram (whose rows are exact in the middle) commutes:

$$\begin{array}{ccccc} \operatorname{Cl}(\mathfrak{M}^{\{p\}}(\mathbf{Z}_p(1))) & \longrightarrow & \operatorname{Cl}(\mathfrak{M}^{\{p\}}(T_y)) & \longrightarrow & \operatorname{Cl}(\mathfrak{M}^{\{p\}}(T)) \\ \Phi^{\{p\}}_{\mathbf{Z}_p(1)}\Big\uparrow & & \Phi^{\{p\}}_{T_y}\Big\uparrow & & \Phi^{\{p\}}_{T}\Big\uparrow \\ H^1_{f,\{p\}}(F, \mathbf{Z}_p(1)) & \xrightarrow{\ i\ } & H^1_{f,\{p\}}(F, T_y) & \xrightarrow{\ j\ } & H^1_{f,\{p\}}(F, T). \end{array} \tag{6.5}$$

For each integer $n > 0$, the Wedderburn decomposition of $\mathfrak{M}^{\{p\}}(\mu_{p^n})$ (cf. (2.3)) is given by

$$\mathfrak{M}^{\{p\}}(\mu_{p^n}) \simeq \bigoplus_{i=0}^{p^n-1} O_F[1/p].$$

Hence $h_F \cdot \operatorname{Cl}(\mathfrak{M}^{\{p\}}(\mu_{p^n})) = 0$ for each n, and so it follows that $h_F \cdot \operatorname{Cl}(\mathfrak{M}^{\{p\}}(\mathbf{Z}_p(1))) = 0$ also. The result now follows from the commutativity of (6.5). □

Proposition 6.5. *Assume that the pairing $\langle\langle\,,\,\rangle\rangle$ is non-degenerate, and suppose that $\Phi^{\{p\}}_T(x)$ is of finite order. Then $x \in \mathfrak{G}_F(T)$.*

Proof. We first observe from the definition of $\mathfrak{G}_F(T)$ that if $M_1 x \in \mathfrak{G}_F(T)$ for any integer $M_1 > 0$, then $x \in \mathfrak{G}_F(T)$ also. Hence, we see from Proposition 6.4 that, without loss of generality, we may assume that there exists a lift $\tilde{x} \in H^1_{f,\{p\}}(F, T_y)$ of $x \in H^1_{f,\{p\}}(F, T)$ such that $\Phi^{\{p\}}_{T_y}(\tilde{x}) = 0$. We shall make this assumption from now on.

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

$$T_y = \mathbf{Z}_p(1) \times T \tag{6.6}$$

with Ω_F-action given by

$$(\zeta, t)^\sigma = \left(\zeta^\sigma \cdot \{f(\sigma^{-1})(t)\}^\sigma, t^\sigma\right)$$

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

$$A_{F^c}(T_y) \xrightarrow{\sim} A_{F^c}(\mathbf{Z}_p(1)) \otimes_{F^c} A_{F^c}(T); \qquad \alpha \mapsto k_1(\alpha) \otimes k_2(\alpha), \tag{6.7}$$

where k_1 and k_2 are induced by the projection maps $\mathbf{Z}_p(1) \times T \to \mathbf{Z}_p(1)$ and $\mathbf{Z}_p(1) \times T \to T$ respectively.

We now make a choice of resolvends associated to $\tilde{x}$ and λ_v for each v. Since $\tilde{x} \in \mathrm{Ker}(\Phi^{\{p\}}_{T_y})$, we may choose a resolvend $\alpha \in \mathbf{H}(\mathfrak{M}^{\{p\}}(T_y))$ associated to $\tilde{x}$. For each place $v \nmid p$, we choose an arbitrary resolvend $\nu_v \in \mathbf{H}(\mathfrak{M}^{\{p\}}_v(T_y))$ associated to λ_v. For each place $v \mid p$, we set

$$\nu_v = (1 \otimes k_2(\alpha))_v$$

(cf. (6.7)); this is a resolvend associated to λ_v since y is locally trivial at v. Then, for each place v of F, we have

$$\tau_v := \alpha_v \nu_v^{-1} \in i_v(\mathbf{H}(\mathfrak{M}^{\{p\}}_v(\mathbf{Z}_p(1)))),$$

and τ_v is a resolvend associated to $\tilde{x}_v - \lambda_v \in i_v(H^1(F_v, \mathbf{Z}_p(1)))$.

If $v \nmid p$, then $\mathbf{Z}_p(1)$ is unramified at v, and so Remark 3.6 implies that we have

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

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

If $v \mid p$, then $\tau_v = (k_1(\alpha) \otimes 1)_v$, and so $\oplus_{v|p} \tau_v$ is the image of $k_1(\alpha) \in \mathfrak{M}^{\{p\}}(\mathbf{Z}_p(1))^\times_{O_{F^c}}$ under the localisation map

$$\delta : \mathfrak{M}^{\{p\}}(\mathbf{Z}_p(1))^\times_{O_{F^c}} \to \bigoplus_{v|p} \mathfrak{M}^{\{p\}}_v(\mathbf{Z}_p(1))^\times_{O_{F^c_v}}.$$

For each integer $n \geq 1$, write

$$\delta_n : \mathfrak{M}^{\{p\}}(\mu_{p^n})^\times_{O_{F^c}} \to \bigoplus_{v|p} \mathfrak{M}^{\{p\}}_v(\mu_{p^n})^\times_{O_{F^c_v}}$$

for the localisation map, and let $\tau_{v,n}$ denote the image of τ_v in $\mathfrak{M}^{\{p\}}_v(\mu_{p^n})^\times_{O_{F^c_v}}$ under the natural map $\mathfrak{M}^{\{p\}}_v(\mathbf{Z}_p(1))^\times_{O_{F^c_v}} \to \mathfrak{M}^{\{p\}}_v(\mu_{p^n})^\times_{O_{F^c_v}}$. Let $(\tilde{x}_v - \lambda_v)_n$ denote the image of $(\tilde{x}_v - \lambda_v)$ in $H^1(F_v, \mu_{p^n})$ under the natural map $H^1(F_v, \mathbf{Z}_p(1)) \to H^1(F_v, \mu_{p^n})$.

Since $\bigoplus_{v|p} \tau_v$ lies in the image of δ, we have that $\bigoplus_{v|p} \tau_{v,n}$ lies in the image of δ_n. It therefore follows that

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

lies in the image of $O_F[1/p]^\times F^{\times p^n}/F^{\times p^n}$ 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 $B_F(x, y) = 0$. Hence $x \in \mathfrak{G}_F(T)$, since by hypothesis $\langle\langle\, , \rangle\rangle$ is non-degenerate. $\square$

Theorem 1.1 now follows immediately from Propositions 6.3 and 6.5.

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

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

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

[7] 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.

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

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

[10] 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.

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

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

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

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

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

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

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

[18] 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.

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

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

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

[22] 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).)

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

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

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

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

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

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

[31] 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