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 $G 	o Y$ 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 $O_X$ is an $O_G$-comodule, and so it is also an $O_{G^*}$-module (see e.g. [11]). As an $O_{G^*}$-module, the structure sheaf $O_X$ is locally free of rank one, and so it gives a line bundle $\mathcal{M}_\pi$ on $G^*$. Set

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

Then the maps

$$\psi : H^1(Y, G) \to \text{Pic}(G^*), \quad [\pi] \mapsto [L_\pi];$$ (1.1)

$$\varphi : H^1(Y, G) \to \text{Pic}(\tilde{G}^*), \quad [\pi] \mapsto [i^*L_\pi]$$ (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 $Y = \text{Spec}(O_F)$. Write $G^* = \text{Spec}(A)$, $G = \text{Spec}(B)$, and $X = \text{Spec}(C)$. Then the algebra $C$ is a twisted form of $B$, and the homomorphisms $\psi$ and $\varphi$ measure the Galois module structure of this twisted form. The homomorphism $\psi$ was first introduced by W. Waterhouse (see [27]), and was further developed in the context of Galois module theory by M. Taylor (25). 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 [24], it was shown that, for elliptic curves with complex multiplication, the class invariant homomorphism $\psi$ vanishes on the classes of torsors obtained by dividing torsion points of order coprime to 6. This implies the existence of Galois generators for certain rings of integers of abelian extensions of imaginary quadratic fields, and it may be viewed as an integral version of the Kronecker Jugendtraum (see [26], [10]). This vanishing result was extended to all elliptic curves in [2] and [18].

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 $X$ is a projective curve over Spec($\mathbb{Z}$) which is equipped with a free action of a finite group. In [19], it is shown that the behaviour of the equivariant projective Euler characteristic of $\mathcal{O}_X$ is partly governed by class invariants of torsors arising from torsion points on the Jacobian of $X$. 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 [16]). 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. Let $V$ be a $d$-dimensional $\mathbb{Q}_p$-vector space. Let $F^c$ be an algebraic closure of $F$, and write $\Omega_F := \text{Gal}(F^c/F)$. Suppose that $\rho : \Omega_F \to \text{GL}(V)$ is a continuous representation of $\Omega_F$ that is ramified at only finitely many primes of $F$. Set $V^* := \text{Hom}_{\mathbb{Q}_p}(V, \mathbb{Q}_p(1))$, and let $\rho^* : \Omega_F \to \text{GL}(V^*)$ be the corresponding representation of $\Omega_F$. Suppose that $T \subseteq V$ is an $\Omega_F$-stable lattice, and write $T^* := \text{Hom}_{\mathbb{Z}_p}(T, \mathbb{Z}_p(1))$. (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 group schemes $G_n$ and $G^*_n$ over Spec($F$) by

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

Then $G^*_n$ is the Cartier dual of $G_n$, and we may write $G^*_n = \text{Spec}(A_n)$ for some Hopf algebra $A_n$ over $F$. Let $\mathfrak{A}_n$ be any $O_F$-algebra such that $\mathfrak{A}_n \otimes_{O_F} F = A_n$, and write $\text{Sp}(\mathfrak{A}_n) := \text{Spec}(\mathfrak{A}_n)$.

By using a description of $H^1(F,G_n)$ which arises via studying the Galois structure of $G_n$-torsors in terms of $A_n$, we 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 line bundle $L_\pi$ associated to $\pi$.) 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 $\pi : X \to \text{Spec}(F)$ 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 [8, 17] and [27] to construct a natural homomorphism

$$\phi_{\mathfrak{A}_n} : H^1_{\mathfrak{A}_n}(F, G_n) \to \text{Pic}(\text{Sp}(\mathfrak{A}_n)).$$ \hfill (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 $G_n$ over $\text{Spec}(O_F)$. If we choose $\mathfrak{A}_n$ to be the $O_F$-Hopf algebra representing the Cartier dual $G^*_n$ of $G_n$, then $H^1_{\mathfrak{A}_n}(F, G_n) = H^1(\text{Spec}(O_F), G_n)$, 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 $\text{Sp}(\mathfrak{A}_n)$ is equal to the normalisation $\tilde{G}^*_n$ of $G^*_n$. In this case, $H^1(\text{Spec}(O_F), G_n)$ is contained in $H^1_{\mathfrak{A}_n}(F, G_n)$, and the restriction of $\phi_{\mathfrak{A}_n}$ to $H^1(\text{Spec}(O_F), G_n)$ is the homomorphism (1.2). (See Example 3.5 below.)

In this paper we shall mainly be concerned with the cases

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

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

$$H^1_{f,(p)}(F_v, T) := \ker \left[ H^1(F_v, T) \to H^1(F^{nr}_v, T) \right].$$ \hfill (1.4)

Following [20 §3.1.4], we set

$$H^1_{f,(p)}(F, T) = \ker \left[ H^1(F, T) \to \bigoplus_{v \nmid p} H^1(F_v, T) \big/ H^1_{f,(p)}(F_v, T) \right].$$

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

The natural inclusions $G^*_n \to G^*_{n+1}$ induce pullback homomorphisms

$$\text{Pic}(\text{Sp}(\mathfrak{M}_{n+1})) \to \text{Pic}(\text{Sp}(\mathfrak{M}_n)), \quad \text{Pic}(\text{Sp}(\mathfrak{M}_{n+1})) \to \text{Pic}(\text{Sp}(\mathfrak{M}_n^{(p)})).$$

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

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

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 $\mathbb{Z}_p$-extension of $F$, and set

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

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 [13, p.131–132], and further studied by A. Plater in [21] and [22] (see also [15]).

Let

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

denote the natural localisation map. In [20, Section 3.1.4], Perrin-Riou constructs a $p$-adic height pairing

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

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

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

for the pairing induced by $B_F$. 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.

**Theorem 1.1.** Suppose that the pairing $\langle \langle , \rangle \rangle$ is non-degenerate modulo torsion. Then $x \in \mathfrak{G}_F(T)$ if and only if $\Phi^\{p\}_F(x)$ is of finite order.

Let $S$ be a finite set of places of $F$ containing the places lying over $p$, the places at which $\rho$ is ramified, and the set of infinite places. Let $F^S/F$ denote the maximal unramified outside $S$ extension of $F$. 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 1.2.** Suppose that the pairing $\langle \langle , \rangle \rangle$ is non-degenerate modulo torsion, and that

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

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

**Proof.** It follows from [20, Remark at the end of §3.4.3] that if (1.6) holds, then $\mathfrak{G}_F(T) \cap \text{Ker}(\text{Loc}_{F,T})$ is finite. The result now follows from Theorem 1.1. \qed
We now turn to the homomorphism $\Phi_F$.

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

$$\mathcal{C}_F(T) := \{ x \in H^1_u(F,T) \mid x \in \cap_n \text{Cores}_{F_n/F}(H^1_u(F_n^\ast, T)) \text{ for some integer } M > 0 \}.$$  

**Theorem 1.3.** Suppose that $x \in \mathcal{C}_F(T)$. Then $\Phi_F(x)$ is of finite order.

**Remark 1.4.** Whether or not the converse of Theorem 1.3 holds in general is an open question, and it appears to be a very delicate problem. If $T$ has $\mathbb{Z}_p$-rank one, then it may be shown that $G_F(T) = \mathcal{C}_F(T)$, and so the converse to Theorem 1.3 holds in this case. □

**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, and an anonymous referee for pointing some errors in an earlier version of this paper. 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.** In this paper, all modules are left modules unless explicitly stated otherwise.

For any field $L$, we write $L^c$ for an algebraic closure of $L$, and we set $\Omega_L := \text{Gal}(L^c/L)$. 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 $\Omega_{L_v}$ with a subgroup of $\Omega_L$. If $P$ is any $O_L$-module, then we shall usually write $P_v := P \otimes_{O_L} O_{L_v}$.

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

If $R$ and $S$ are rings with $R \subseteq S$, and if $A$ is any $R$-algebra, then we often write $A_S$ for $A \otimes_R S$. We shall also often write $\text{Sp}(A)$ for $\text{Spec}(A)$.

2. Resolvents and cohomology groups

Let $R$ be a Dedekind domain with field of fractions $K$, and write $R^c$ for the integral closure of $R$ in $K^c$. (In what follows we always allow the possibility that $R = K$ and $R^c = K^c$.) Assume that $K$ is of characteristic zero. In this section, we shall take $Y = \text{Spec}(R)$, and we shall explain how the cohomology group $H^1(Y, G)$ may be described in terms of the Hopf algebra $A$ representing $G^\ast$. Set $\Gamma := G(R^c)$ and $\Gamma^\ast := G^\ast(R^c)$.

Recall that there is a canonical isomorphism

$$H^1(Y, G) \simeq \text{Ext}^1(G^\ast, \mathbb{G}_m).$$
This implies that given any $G$-torsor $\pi : X \to Y$, we can associate to it a canonical commutative extension

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

The scheme $G(\pi)$ is a $\mathbb{G}_m$-torsor over $G^*$, and its associated $G^*$-line bundle is equal to $L_{\pi}$. (This construction is explained in detail by Waterhouse in [27].)

Over $\text{Spec}(R)$, the $G$-torsors $\pi_0$ and $\pi$ 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 [27], we obtain an isomorphism

$$\xi_{\pi} : L_{\pi} \otimes_R R_c \sim \to A_{R_c}.$$ 

We shall refer to $\xi_{\pi}$ as a splitting isomorphism for $\pi$.

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

$$A_{R_c} \xrightarrow{s_{\pi} \otimes_R R_c} L_{\pi} \otimes_R R_c \xrightarrow{\xi_{\pi}} A_{R_c}.$$ 

This is an isomorphism of $A_{R_c}$-modules, and so it is just multiplication by an element $r(s_{\pi})$ of $A_{R_c}$. We refer to $r(s_{\pi})$ as a resolvend of $s_{\pi}$ or as a resolvend associated to $\pi$. (This terminology is due to L. McCulloh, [17].) Note that $r(s_{\pi})$ depends upon the choice of $\xi_{\pi}$ as well as upon $s_{\pi}$.

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

$$H(A) := \{ \alpha \in A_{R_c}^\times | g_\omega \alpha = \alpha g_\omega \text{ for all } \omega \in \Omega_K, \text{ where } g_\omega \in \Gamma \},$$

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

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

The following result, in the case in which $G$ is a constant group scheme, is equivalent to certain results of L. McCulloh (see [17, 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 [8, Lemma 1.11 and Sections 2 and 3]) using techniques from the theory of Hopf algebras. We give a different approach to these ideas.
Theorem 2.2. Let $G$ be a finite, flat commutative group scheme over $\text{Spec}(R)$, and let $G^* = \text{Spec}(A)$ be the Cartier dual of $G$. Then the map
\[
\Upsilon_R : \text{Ker}(\psi) \to H(A); \quad [\pi] \mapsto r(\pi)
\]
is an isomorphism.

Proof. We first show that $\Upsilon_R$ is a homomorphism. Suppose that $\pi : X \to \text{Spec}(R)$ and $\pi' : X' \to \text{Spec}(R)$ are $G$-torsors satisfying $\psi(\pi) = \psi(\pi') = 0$. Let $s_\pi : A \to L_\pi$ and $s_{\pi'} : A \to L_{\pi'}$ be trivialisations of $L_\pi$ and $L_{\pi'}$ respectively. Write $s'' = s_\pi \cdot s_{\pi'}$. Then it follows via the functoriality of Waterhouse’s construction in [27] that there is a natural isomorphism $L_{\pi''} \simeq L_\pi \otimes L_{\pi'}$. Thus, if we set
\[
s_{\pi''} = s_\pi \otimes s_{\pi'} : A \simeq A \otimes_A A \to L_\pi \otimes_A L_{\pi'},
\]
then we see that $r(s_{\pi''}) = r(s_\pi) r(s_{\pi'})$. This implies that $r(\pi'') = r(\pi) r(\pi')$, as required.

We now show that $\Upsilon_R$ is surjective. For any scheme $S \to \text{Spec}(R)$, write $\text{Map}_S(G^*, G_m)$ for the set of scheme-theoretic morphisms $G^* \otimes_R S \to G_m \otimes_R S$. Since $G^*$ is affine, the functor $S \mapsto \text{Map}_S(G^*, G_m)$ is representable by the affine group scheme $G_{m,G^*} := G_m \otimes_R G^* \to \text{Spec}(R)$. The group scheme $G = \text{Hom}(G^*, G_m)$ is a closed subgroup scheme of $G_{m,G^*}$.

Suppose that $\alpha \in H(A)$. Then we may view $\alpha$ as being a $\text{Spec}(R^c)$-valued point of $G_{m,G^*}$. Let
\[
G_\alpha := \alpha \cdot [G \otimes_R R^c]
\]
(2.1)
denote the ‘translation-by-$\alpha$’ in $G_{m,G^*} \otimes_R R^c$ of $G \otimes_R R^c$. Then $G \otimes_R R^c$ acts on $G_\alpha$ via translation. Furthermore, translation by $\alpha$ induces an isomorphism
\[
\Xi_\alpha : G \otimes_R R^c \simeq G_\alpha
\]
(2.2)
of schemes with $G \otimes_R R^c$ action.

We now claim that $G_\alpha$ descends to $\text{Spec}(R)$, i.e. that there is a scheme $\pi_\alpha : Z_\alpha \to \text{Spec}(R)$ defined over $R$ which is such that $G_\alpha = Z_\alpha \otimes_R R^c$. Since $R$ is a Dedekind domain, and $G_\alpha$ is flat over $\text{Spec}(R^c)$, it suffices to check that the generic fibre $G_{\alpha/K^c}$ of $G_\alpha$ descends to a scheme over $\text{Spec}(K)$. This in turn follows via Galois descent, and may be seen as follows. We first note that the isomorphism $\Xi_\alpha$ 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 $z_\alpha$ is the $\Gamma$-valued cocycle of $\Omega_K$ associated to $\alpha$. Then it is easy to check that the action of $\Omega_K$ 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 $G_{\alpha/K^c}$ descends to $Z_{\alpha/K}$ over $\text{Spec}(K)$. A similar argument also shows that $\pi_\alpha : Z_\alpha \to \text{Spec}(R)$ is a $G$-torsor over $\text{Spec}(R)$.

We shall now show that $\psi(\pi_\alpha) = 0$. Let
\[
\xi_{\pi_\alpha} : L_{\pi_\alpha} \otimes_R R^c \simeq A_{R^c}
\]
denote the splitting isomorphism of $\pi_\alpha$ induced by $\Xi_\alpha$. Define an isomorphism

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

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 $\sigma_\alpha$ descends to an isomorphism $\sigma'_\alpha : A \rightarrow \mathcal{L}_{\pi_\alpha}$ over $R$. This will in turn follow if we show that

$$\sigma'^\omega(\alpha) = \sigma_\alpha(\alpha)$$

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

$$\sigma'^\omega(\alpha) = \omega[\sigma_\alpha(\alpha^{-1})] = \omega[\alpha \xi_{\pi_\alpha}^{-1}(a^{-1})] = \omega[\alpha z_\alpha(\omega^{-1}) \xi_{\pi_\alpha}^{-1}(a)^{\omega^{-1}}] = \omega[\alpha^{\omega^{-1}} \xi_{\pi_\alpha}^{-1}(a)^{\omega^{-1}}] = \alpha \xi_{\pi_\alpha}^{-1}(a) = \sigma_\alpha(\alpha).$$

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

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

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

$$\Xi_\beta \circ \Xi^{-1}_\alpha : G_\alpha \rightarrow G_\beta$$

induces an isomorphism $G_\alpha(K^c) \rightarrow G_\beta(K^c)$ of $\Omega_K$-modules. This implies that the $G$-torsors $\pi_\alpha : Z_\alpha \rightarrow \text{Spec}(R)$ and $\pi_\beta : Z_\beta \rightarrow \text{Spec}(R)$ are isomorphic. This completes the proof of the theorem. \hfill $\Box$

**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 $\Omega_K \rightarrow \Gamma$ defined by $\omega \mapsto r(s_\pi)^\omega r(s_\pi)^{-1}$ is an $\Omega_K$-cocycle representing $[\pi] \in H^1(K, G)$. \hfill $\Box$

If $R$ is a local ring, then $\text{Pic}(G^*) = 0$, and so $\text{Ker}(\psi) = H^1(R, G)$. The following result is a direct corollary of Theorem 2.2. It gives a description of the flat cohomology of $G$ over $\text{Spec}(R)$ in terms of resolvends. (Recall that $N$ denotes the exponent of $G$.)

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

(a) There is an isomorphism

$$\Upsilon_R : H^1(R, G) \rightarrow H(A).$$
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 $\gamma^*$. Let $\Gamma^* \setminus \Omega_K$ denote a set of representatives of $\Omega_K$-orbits of $\Gamma^*$. 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

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

(2.3)

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

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

Proof. See [3, Corollary 3.4].

Proposition 2.7. Suppose that $R = K$, and let $L$ be a (possibly infinite) extension of $K$. Then the following diagram is commutative:

$$\begin{align*}
H^1(K, G) \xrightarrow{\iota_K} H(A) \\
\downarrow \text{Res} & \quad \downarrow \\
H^1(L, G) \xrightarrow{\iota_L} H(A_L).
\end{align*}$$

(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 $i : H(A) \to H(A_L)$.

Proof. Let $\pi : X \to \text{Spec}(K)$ be any $G$-torsor, and let $s : A \xrightarrow{\sim} L_\pi$ be any trivialisation of $L_\pi$. Then it follows via a straightforward computation that the $\Omega_L$-cocycle associated to $i(r(s))$ is equal to the restriction of the $\Omega_K$-cocycle associated to $r(s)$ (cf. Remark 2.8).

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

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

Conversely, if $\pi \in \text{Res}_{K/K(\mu_N)}$, then for a suitable choice of $s_\pi$, we have $r(s_\pi) \in A_{F(\mu_N)}^\times$, and $r(s_\pi)^N \in A^\times$. Since $A$ is a semisimple $F$-algebra, this implies (via considering the Wedderburn decomposition (2.3) of $A$) that $r(s_\pi)^N \in A^\times N$, and so $\pi \in \text{Ker}(\eta_F)$. 

□
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 $\Omega_L$ in $\Omega_K$. Then we have a norm homomorphism
\[ N_{L/K} : A_L \rightarrow A_K; \quad a \mapsto \prod_{i=1}^{n} a^{\omega_i}. \] (2.5)
This induces homomorphisms (which we denote by the same symbol)
\[ N_{L/K} : H(A_L) \rightarrow H(A_K), \quad N_{L/K} : H(L) \rightarrow H(K). \]

**Theorem 2.9.** The following diagram is commutative:
\[
\begin{array}{ccc}
H^1(L, G) & \xrightarrow{\gamma_L} & H(A_L) \\
\text{Cores}_{L/K} \downarrow & & \downarrow N_{L/K} \\
H^1(K, G) & \xrightarrow{\gamma_K} & H(A_K)
\end{array}
\] (2.6)
where the left-hand vertical arrow is the corestriction map on cohomology.

**Proof.** Let $\pi_L : X_L \rightarrow \text{Spec}(L)$ 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 $\Omega_K$-cocycle associated to $N_{L/K}(r(s_{\pi_L}))$ is equal to the corestriction of the $\Omega_L$-cocycle associated to $r(s_{\pi_L})$ (cf. Remark 2.3). \qed

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

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

**Theorem 2.10.** Suppose that $R$ is a local ring. Then the following diagram is commutative:
\[
\begin{array}{ccc}
H^1(\text{Spec}(R), G_n) & \xrightarrow{\gamma_{R,n}} & H(A_n) \\
\downarrow p_n & & \downarrow q_n \\
H^1(\text{Spec}(R), G_{n-1}) & \xrightarrow{\gamma_{R,n-1}} & H(A_{n-1})
\end{array}
\] (2.7)

**Proof.** Suppose that $\pi_n : X_n \rightarrow \text{Spec}(R)$ 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 [27] 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 $s_{\pi_n}$ along $p_n^D$. We have
\[ \gamma_{R,n-1}(\pi_{n-1}) = [r(s_{\pi_{n-1}})] = [r((p_n^D)^* s_{\pi_n})] = [q_n(r(s_{\pi_n})]. \]
This establishes the result. \qed
Suppose now that \( R = K \). Fix a positive integer \( n \), and assume that \( G_n^* \) is a constant group scheme. Then we have

\[
A_n^\times / (A_n^\times)^p \simeq \text{Map}(\Gamma_n^*, K^\times / (K^\times)^p).
\]

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

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

Write

\[
ev_P : A_n^\times / (A_n^\times)^p \simeq \text{Map}(\Gamma_n^*, K^\times / (K^\times)^p) \to K^\times / (K^\times)^p
\]

for the map \( a \mapsto a(P) \) given by ‘evaluation at \( P \)’. The following result shows how to describe the map \( \eta_K \) of Corollary \( \text{2.4} \) in terms of Kummer theory.

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

\[
\begin{array}{ccc}
H^1(K, G_n) & \xrightarrow{\chi_P} & H^1(K, \mu_{p^n}) \\
\downarrow{\eta_K} & & \uparrow{\text{Kummer}} \\
A_n^\times / (A_n^\times)^p & \xrightarrow{\text{ev}_P} & K^\times / (K^\times)^p \\
\end{array}
\]

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

**Proof.** See [5, Proposition 3.2]. \( \Box \)

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

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

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

\[
\begin{array}{ccc}
H^1(K, G_n) & \xrightarrow{\chi_P} & \text{Hom}(\Gamma_n^*, K^\times / (K^\times)^p) \\
\downarrow{p_n} & & \downarrow{r_n} \\
H^1(K, G_{n-1}) & \xrightarrow{\eta_K} & \text{Hom}(\Gamma_{n-1}^*, K^\times / (K^\times)^{p^{n-1}}). \\
\end{array}
\]

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

\[
\begin{array}{ccc}
H^1(K, G_n) & \xrightarrow{\chi_P} & H^1(K, \mu_{p^n}) \simeq K^\times / (K^\times)^{p^n} \\
\downarrow{p_n} & & \downarrow{\text{red}} \\
H^1(K, G_{n-1}) & \xrightarrow{\chi_P} & H^1(K, \mu_{p^{n-1}}) \simeq K^\times / (K^\times)^{p^{n-1}}. \\
\end{array}
\]

(Here the right-hand vertical arrow denotes the natural reduction map.) The result now follows from Propositions \( \text{2.11} \) and \( \text{2.6} \) \( \Box \)
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 beginning 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 $\text{Spec}(F)$, and we let $G^* = \text{Spec}(A)$. Let $\mathfrak{A}$ denote any $O_F$-algebra in $A$ such that $A \otimes_{O_F} F = A$. Set

$$H(\mathfrak{A}) := \{ \alpha \in \mathfrak{A}^\times \mid \alpha^{\omega} = g \omega \alpha \text{ for all } \omega \in \Omega_K, \text{ where } g_\omega \in \Gamma \}.$$ 

We shall be interested in using the groups $H(\mathfrak{A})$ and $H(A)$ 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 $\Upsilon_F$ 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:

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

Hence a $G$-torsor $\pi : X \to \text{Spec}(F)$ lies in $H^1_{\mathfrak{A}}(F,G)$ if and only if there exists a trivialisation $s_\pi : A \xrightarrow{\sim} L_\pi$ with $r(s_\pi) \in H(\mathfrak{A}) \subseteq H(A)$. The resolvend $r(s_\pi)$ 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

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

□

**Remark 3.3.** Suppose that $F$ is either a number field or a local field, and let $\mathfrak{M}$ be the unique maximal $O_F$-order in $A$. Assume that $\pi \in H^1(F,G)$ lies in $\text{Ker}(\eta_F)$. Then it follows from the discussion in Remark 2.8 that there exists a resolvend $r(s_\pi) \in H(A)$ associated to $\pi$ such that $r(s_\pi)^N = 1$. Hence $r(s_\pi) \in H(\mathfrak{M})$, and so $\pi \in H^1_{\mathfrak{M}}(F,G)$. □

Now suppose that $F$ is a number field, and let $\mathfrak{M}$ be the unique maximal $O_F$-order in $A$. 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 $\text{Cl}(\mathfrak{A})$ for the locally free classgroup of $\mathfrak{A}$. Thus, $\text{Cl}(\mathfrak{A})$ is
the Grothendieck group of locally free \( \mathfrak{A} \)-modules of finite rank, and it may be identified with the group \( \text{Pic}(\text{Sp}(\mathfrak{A})) \). Then it is a standard result from the theory of classgroups (see e.g. [12 §52]) that there is a natural isomorphism

\[
\text{Cl}(\mathfrak{A}) \simeq \frac{J_f(A)}{\left( \prod_{v|\infty} \mathfrak{A}_v^\times \right) \cdot A^\times}.
\]

**Theorem 3.4.** Let \( F \) be a number field.

(a) There is a natural homomorphism

\[
\phi_{\mathfrak{A}} : H^1_{\mathfrak{A}}(F,G) \to \text{Cl}(\mathfrak{A}).
\]

(b) The isomorphism

\[
\Upsilon_F : H^1(F,G) \sim \to H(A)
\]

of Corollary 2.4 induces an isomorphism

\[
\Upsilon_{F,\mathfrak{A}} : \text{Ker}(\phi_{\mathfrak{A}}) \sim \to H(\mathfrak{A}) \subseteq H(A).
\]

(c) We have \( \text{Ker}(\eta_F) \subseteq \text{Ker}(\phi_{\mathfrak{A}}) \).

**Proof.** (a) Suppose that \( \pi : X \to \text{Spec}(F) \) is a \( G \)-torsor with \([\pi] \in H^1_{\mathfrak{A}}(F,G)\). Fix a trivialisation \( s_\pi : A \sim \to \mathcal{L}_\pi \). Note that \( r(s_\pi) \in H(A) \) is well-defined up to multiplication by an element of \( \Gamma \cdot A^\times \).

For each finite place \( v \) of \( F \), write \( \pi_v \) for the torsor \( X \otimes_F F_v \to \text{Spec}(F_v) \). Since \([\pi_v] \in H^1_{\mathfrak{A}_v}(F_v,G)\), we may choose a trivialisation \( t_{\pi_v} : A_v \sim \to \mathcal{L}_{\pi_v} \) satisfying \( r(t_{\pi_v}) \in H(\mathfrak{A}_v) \). Then \( r(t_{\pi_v}) \) is well-defined up to multiplication by an element of \( \Gamma \cdot \mathfrak{A}_v^\times \), and \( r(t_{\pi_v}) r(s_\pi^{-1}) \in \Gamma \cdot \mathfrak{A}_v^\times \). Furthermore, for all but finitely many places \( v \), we have that \( r(s_\pi) \in H(M_v) \), and so \( r(t_{\pi_v}) r(s_\pi^{-1}) \in \Gamma \cdot \mathfrak{M}_v^\times \) for all such \( v \).

It therefore follows that the element \((r(t_{\pi_v}) r(s_\pi^{-1}))_v \) lies in \( \left( \prod_{v|\infty} \Gamma \right) \cdot J_f(A) \), and that its image in

\[
\frac{\left( \prod_{v|\infty} \Gamma \right) \cdot J_f(A)}{\left( \prod_{v|\infty} \mathfrak{A}_v^\times \right) \cdot A^\times} \simeq \text{Cl}(\mathfrak{A})
\]

is well-defined. We define

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

We now show that \( \phi_{\mathfrak{A}} \) is a homomorphism. Suppose that \( \pi' : X' \to \text{Spec}(F) \) is another \( G \)-torsor, and let \( s_{\pi'} \) and \( t_{\pi'_v} \) \( (v \nmid \infty) \) be trivialisations defined analogously to \( s_\pi \) and \( t_{\pi_v} \) above. Write \( \pi'' := \pi \cdot \pi' \). Then it follows from the functoriality of Waterhouse’s construction in [27] that there is a natural isomorphism \( \mathcal{L}_{\pi''} \simeq \mathcal{L}_\pi \otimes \mathcal{L}_{\pi'} \). Thus, if we set

\[
s_{\pi''} := s_\pi \otimes s_{\pi'} : \mathcal{L}_\pi \otimes \mathcal{L}_{\pi'} \sim \to A, \quad t_{\pi''_v} := t_{\pi_v} \otimes t_{\pi'_v} : \mathcal{L}_{\pi_v} \otimes \mathcal{L}_{\pi'_v} \sim \to A_v,
\]
then \( r(s''_v) = r(s_v) r(s'_v) \), and \( r(t''_v) = r(t_v) r(t'_v) \). Hence it follows that
\[
\phi_{\mathfrak{A}}(\pi'') = [(r(t''_v) r(s''_v))^{-1}]_v = [(r(t_v) r(s_v))^{-1}]_v \cdot [(r(t'_v) r(s'_v))^{-1}]_v \\
= \phi_{\mathfrak{A}}(\pi) \cdot \phi_{\mathfrak{A}}(\pi'),
\]
as asserted.

(b) Suppose that \( \pi : X \to \text{Spec}(F) \) is a \( G \)-torsor satisfying \( r(s_v) \in H(\mathfrak{A}) \) for some choice of trivialisation \( s_v : A \to \mathcal{L}_v \) of \( \mathcal{L}_v \). Write \( s_{\pi,v} : A_v \to \mathcal{L}_{\pi,v} \) for the trivialisation of \( \mathcal{L}_{\pi,v} \) induced by \( s_v \). Then \( r(s_{\pi,v}) \in H(\mathfrak{A}_v) \) for all finite places \( v \) of \( F \). Hence \( \pi \in H^1_{\mathfrak{A}}(F,G) \), and we may take \( t_v = s_{\pi,v} \) 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 suitable choices of \( s_v \) and \( r(t_v) \), we have that
\[
(r(t_v) r(s_v))^{-1} \in \prod_{v \mid \infty} \mathfrak{A}_v^* \subseteq \prod_{v \mid \infty} H(\mathfrak{A}_v).
\]
This implies that \( r(s_v) \in H(\mathfrak{A}_v) \) for each place \( v \mid \infty \), and so it follows that \( r(s_v) \in H(\mathfrak{A}) \).

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

**Example 3.5.** Suppose that \( F \) is a number field. Let \( G \) be a finite, flat, commutative group scheme over \( \text{Spec}(O_F) \), with generic fibre \( G \). Let \( G^* = \text{Spec}(\mathfrak{A}) \) denote the Cartier dual of \( G^* \); then \( G^* = \text{Spec}(A) \) is the generic fibre of \( G^* \). 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
\[
H^1_{\mathfrak{A}}(F,G) = H^1(O_F,G).
\]
Hence we obtain a description of the flat Selmer group of \( G \) in terms of resolvends. In this case, the map
\[
\phi_{\mathfrak{A}} : H^1(O_F,G) \to \text{Cl}(\mathfrak{A}) \simeq \text{Pic}(G^*)
\]
is the same as the class invariant homomorphism \((1.1)\) for the group \( G \).

Also, we have
\[
H^1(O_F,G) = H^1_{\mathfrak{A}}(F,G) \subseteq H^1_{\mathfrak{M}}(F,G),
\]
and \( \text{Sp}(\mathfrak{M}) \) is the normalisation of \( G^* \). The restriction of the homomorphism
\[
\phi_{\mathfrak{M}} : H^1_{\mathfrak{M}}(F,G) \to \text{Cl}(\mathfrak{M}) \simeq \text{Pic}(\text{Sp}(\mathfrak{M}))
\]
to \( H^1(O_F,G) \) 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
\[
H^1_v(F_v,G) := \ker \left[ H^1(F_v,G) \to H^1(F_v^{nr},G) \right],
\]
where \( F_v^{nr} \) is the maximal unramified extension of \( F_v \) in a fixed algebraic closure of \( F_v \).
If \( \pi \in H_1^1(F_v, G) \), and \( r(s_\pi) \) is any resolvent associated to \( \pi \), then Proposition 2.7 implies that \( r(s_\pi) \in A_v^{\times} \). 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 \( \alpha^{-1}r(s_\pi) = r(\alpha^{-1}s_\pi) \in M_{r,F_v^{nr}}^{\times} \). This implies that \( \pi \in H_{2M}(F, G) \), and so

\[
H_1^1(F_v, G) \subseteq H_{2M}(F_v, G).
\]

Suppose further that \( G \) is unramified at \( v \). Then \( G := \text{Sp}(M_v) \) is a finite, flat, commutative \( O_{F_v} \)-group scheme, and it is a standard result that \( H_1^1(F_v, G) = H^1(O_{F_v}, G) \). We therefore deduce that in this case, we have \( H_1^1(F_v, G) = H_{2M}(F_v, G) \).

\[\square\]

**Remark 3.7.** It is not difficult to define refinements of the homomorphism \( \phi_A \) taking values in relative algebraic \( K \)-groups as in [11], or in Arakelov Picard groups as in [3]. 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 \( N_{L/F} \) of [2,5] induces a homomorphism

\[ N_{L/K} : \text{Cl}(A_{OL}) \to \text{Cl}(A). \]

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

\[
\begin{array}{ccc}
H_1^{\text{A}_{OL}}(F, G) & \xrightarrow{\phi_{A_{OL}}} & \text{Cl}(A_{OL}) \\
\text{Cores}_{L/F} \downarrow & & \downarrow N_{L/F} \\
H_1^{\text{A}}(F, G) & \xrightarrow{\phi_A} & \text{Cl}(A).
\end{array}
\] (3.2)

**Proof.** Let \( \pi : X \to \text{Spec}(L) \) be a \( G \)-torsor with \( [\pi] \in H_1^{\text{A}_{OL}}(L, G) \), and let \( s_\pi : A_L \sim \mathcal{L}_\pi \) be any trivialisation of \( \mathcal{L}_\pi \). For each finite place \( v \) of \( L \), let \( t_{\pi_v} : A_{L_v} \sim \mathcal{L}_{\pi_v} \) be a trivialisation of \( \mathcal{L}_{\pi_v} \) satisfying \( r(t_{\pi_v}) \in H(A_{OL_v}) \). Then

\[ \phi_{A_{OL}}(\pi) = [(r(t_{\pi_v}) r(s_\pi^{-1}))_v] \in \text{Cl}(A). \]

The result now follows via a similar argument to that used in the proof of Theorem 2.9. \[\square\]

For the rest of this paper, we shall mainly be concerned with the special cases in which \( A = \mathbb{M} \) or \( A = \mathbb{M} \otimes \mathbb{O}_F \mathbb{O}_{F}[1/p] : = \mathbb{M}^{(p)} \). We identify \( \text{Pic}(\text{Sp}(\mathbb{M})) \) and \( \text{Pic}(\text{Sp}(\mathbb{M}^{(p)})) \) with the locally free classgroups \( \text{Cl}(\mathbb{M}) \) and \( \text{Cl}(\mathbb{M}^{(p)}) \) of \( \mathbb{M} \) and \( \mathbb{M}^{(p)} \) respectively. We set

\[
H_1^1(F, G) : = H_{2M}^1(F, G), \quad H_1^{1, (p)}(F, G) : = H_{2M}^1(F, G),
\]

and we write

\[
\phi : H_1^1(F, G) \to \text{Cl}(\mathbb{M}), \quad \phi^{(p)} : H_1^{1, (p)}(F, G) \to \text{Cl}(\mathbb{M}^{(p)})
\]

for the homomorphisms given by Theorem 3.4.
**Proposition 3.9.** Let $F$ be a number field, and suppose that $G^*$ is constant over $\text{Spec}(F)$.

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

$$H^1_u(F_v, G) \cong \text{Hom}(\Gamma^*, O^*_F/(O^*_F)^N).$$

(ii) The isomorphism $\eta_F$ induces isomorphisms

$$\text{Ker}(\phi) \cong \text{Hom}(\Gamma^*, O^*_F/(O^*_F)^N),$$

$$\text{Ker}(\phi^{(p)}) \cong \text{Hom}(\Gamma^*, O^*_{F[1/p]}/(O^*_{F[1/p]})^N).$$

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

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

Proposition 2.6 implies that we have isomorphisms

$$H^1(F, G) \simeq \text{Hom}(\Gamma^*, F^*/(F^*)^N), \quad \text{(3.3)}$$

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

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). 

□

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 $\mathbb{Q}_p$-vector space. Suppose that $\rho : \Omega_F \to \text{GL}(V)$ is a continuous representation which is ramified at only finitely many primes of $F$. We set $V^* := \text{Hom}_{\mathbb{Q}_p}(V, \mathbb{Q}_p(1))$, and we write $\rho^* : \Omega_F \to \text{GL}(V^*)$ for the corresponding representation of $\Omega_F$. Let $T \subseteq V$ be any $\Omega_F$-stable lattice, and write $T^* := \text{Hom}_{\mathbb{Z}_p}(T, \mathbb{Z}_p(1))$. For each positive integer $n$, we define finite group schemes $G_n$ and $G^*_n$ over $\text{Spec}(F)$ by

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

Then $G^*_n$ is the Cartier dual of $G_n$ with $G^*_n = \text{Spec}(A_n)$ 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 $p^D_n$ 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 $\mathfrak{A}_n = \subseteq A_n$ such that $\mathfrak{A}_n \otimes_{O_F} F = A_n$, and $q_n(\mathfrak{A}_n) = \mathfrak{A}_{n-1}$. 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
\[
H(\mathfrak{A}_v(T)) := \{ \alpha \in \mathfrak{A}_v(T)_{OF_v}^\times | \alpha^\omega = t_\omega \alpha \text{ for all } \omega \in \Omega_{F_v}, \text{ where } t_\omega \in T \},
\]
\[
H(\mathfrak{A}_v(T)) := \frac{H(\mathfrak{A}_v(T))}{T \cdot \mathfrak{A}_v(T)^\times}.
\]

Define \( H(\mathfrak{A}(T)) \) and \( H(\mathfrak{A}(T)) \) in a similar way. Write
\[
H^1_{\mathfrak{A}_v(T)}(F_v, T) := \varprojlim H^1_{\mathfrak{A}_{n,v}}(F_v, G_n), \quad H^1_{\mathfrak{A}_v(T)}(F, T) := \varprojlim H^1_{\mathfrak{A}_n}(F, G_n).
\]

**Proposition 4.1.** For each finite place \( v \) of \( F \), we have
\[
H^1_{\mathfrak{A}_v(T)}(F_v, T) \simeq \frac{H(\mathfrak{A}_v(T))}{T \cdot \mathfrak{A}_v(T)^\times}.
\]

**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
\[
1 \to G_n \cdot \mathfrak{A}_{n,v}^\times \to H(\mathfrak{A}_{n,v}) \to H^1_{\mathfrak{A}_{n,v}}(F_v, G_n) \to 0.
\]
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
\[
H^1_{\mathfrak{A}_v(T)}(F_v, T) \simeq \varprojlim H(\mathfrak{A}_{n,v})_{T \cdot \mathfrak{A}_v(T)^\times}.
\]

It follows easily from the definitions that
\[
H(\mathfrak{A}_v(T)) = \varprojlim H(\mathfrak{A}_{n,v}),
\]
and this implies the result. \( \square \)

It is easy to check that \( p_n^D \) induces pullback homomorphisms
\[
(p_n^D)^* : \text{Cl}(\mathfrak{A}_n) \to \text{Cl}(\mathfrak{A}_{n-1}).
\]

Let
\[
\phi_{\mathfrak{A}_n} : H^1_{\mathfrak{A}_n}(F, G_n) \to \text{Cl}(\mathfrak{A}_n)
\]
denote the natural homomorphism afforded by Theorem 3.4.
Theorem 4.2. The following diagram is commutative:

\[
\begin{array}{ccc}
H^1_{\mathfrak{A}_n}(F,G_n) & \xrightarrow{\phi_{\mathfrak{A}_n}} & \text{Cl}(\mathfrak{A}_n) \\
p_n \downarrow & & \downarrow (p^n)^* \\
H^1_{\mathfrak{A}_n}(F,G_{n-1}) & \xrightarrow{\phi_{\mathfrak{A}_{n-1}}} & \text{Cl}(\mathfrak{A}_{n-1}),
\end{array}
\] (4.1)

Proof. The proof of this is similar to that of Theorem 2.10. Let \( \pi_n : X_n \to \text{Spec}(F) \) be a \( \mathfrak{G}_n \)-torsor with \([\pi_n] \in H^1_{\mathfrak{A}_n}(F,G_n)\), and write \( \pi_{n-1} := p_n(\pi_n) \). Let \( s_{\pi_n} : A_n \to L_{\pi_n} \) be any trivialisation of \( L_{\pi_n} \), and for each finite place \( v \) of \( F \), let \( t_{\pi_n,v} : A_{n,v} \to L_{\pi_n,v} \) be a trivialisation of \( L_{\pi_n,v} \) satisfying \( r(t_{\pi_n,v}) \in H(A_{n,v}) \).

Then, via functoriality, we have that \((p^n)^* L_{\pi_n} \simeq L_{\pi_{n-1}}\). The pullbacks \((p^n)^* s_{\pi_n} \) and \((p^n)^* t_{\pi_n,v}\) of \( s_{\pi_n} \) and \( t_{\pi_n,v} \) along \( p^n \) give trivialisations of \( L_{\pi_{n-1}} \) and \( L_{\pi_{n-1},v} \) respectively, and we have that

\[ r((p^n)^* t_{\pi_n,v}) = q_{n,v}(t_{\pi_n,v}) \in H(\mathfrak{A}_{n-1,v}). \]

The result now follows from the definitions of \( \phi_{\mathfrak{A}_n} \) and \( \phi_{\mathfrak{A}_{n-1}} \).

Set

\[ \text{Cl}(\mathfrak{A}(T)) := \lim_{\leftarrow} \text{Cl}(\mathfrak{A}_n). \]

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

\[
\Phi_{\mathfrak{A}(T)} : H^1_{\mathfrak{A}(T)}(F,T) \to \text{Cl}(\mathfrak{A}(T)).
\] (4.2)

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

\[ N_{L/K} : \text{Cl}(\mathfrak{A}(T)_{O_L}) \to \text{Cl}(\mathfrak{A}(T)), \]

and the following diagram is commutative:

\[
\begin{array}{ccc}
H^1_{\mathfrak{A}(T)_{O_L}}(F,G) & \xrightarrow{\phi_{\mathfrak{A}(T)_{O_L}}} & \text{Cl}(\mathfrak{A}(T)_{O_L}) \\
\text{Cores}_{L/F} \downarrow & & \downarrow N_{L/F} \\
H^1_{\mathfrak{A}(T)}(F,G) & \xrightarrow{\phi_{\mathfrak{A}(T)}} & \text{Cl}(\mathfrak{A}(T)).
\end{array}
\] (4.3)

Proof. This follows from Theorem 3.8. □

Proposition 4.4. There is an isomorphism

\[ \Upsilon_{F,\mathfrak{A}(T)} : \text{Ker}(\Phi_{\mathfrak{A}(T)}) \simeq H(\mathfrak{A}(T)) \subseteq H(A(T)). \]

Proof. This follows easily from Theorem 3.4(b). □
Write
\[ H^1_u(F, T) := \lim_{\leftarrow} H^1_u(F, G_n), \quad H^1_{u,(p)}(F, T) := \lim_{\leftarrow} H^1_{u,(p)}(F, G_n). \]
Then (4.2) yields a homomorphism
\[ \Phi_F := \Phi_{2\mathfrak{M}(T)} : H^1_u(F, T) \to \varprojlim \text{Cl}(\mathfrak{M}(T)). \] (4.4)
From Remark 3.6, we see that
\[ H^1_{f,(p)}(F, T) \subseteq H^1_u,(p)(F, T). \]
Hence, restricting \( \Phi_{2\mathfrak{M}(p)}(T) \) to \( H^1_{f,(p)}(F, T) \) yields a homomorphism
\[ \Phi^{(p)}_F : H^1_{f,(p)}(F, T) \to \varprojlim \text{Cl}(\mathfrak{M}^{(p)}(T)). \]

**Remark 4.5.** If \( v \mid p \), then \( H^1_u(F_v, T) \) is not in general equal to the group \( H^1_f(F_v, T) \) introduced by Bloch and Kato in [7]. For example, it follows from the definitions that \( H^1_u(F_v, T) \) is always infinite. On the other hand, if \( v \mid p \), then \( H^1_f(F_v, \mathbb{Z}_p(r)) \) is finite for all \( r \leq 0 \) (see e.g. [7, Example 3.9]).

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 \( \mathbb{Z}_p \)-module. \( \Box \)

**Remark 4.6.** Suppose that \( \mathcal{A} \) is an abelian scheme over \( \text{Spec}(O_F) \), and let \( T \) denote its \( p \)-adic Tate module. For each positive integer \( n \), let \( G_n \) denote the \( O_F \)-group scheme of \( p^n \)-torsion on \( \mathcal{A} \), and write \( G_n^\ast \) for its Cartier dual. Then taking inverse limits of the homomorphisms
\[ \psi_n : H^1(\text{Spec}(O_F), G_n) \to \text{Pic}(G_n^\ast) \]
yield a homomorphism
\[ \Psi_F : H^1_f(F, T) \to \varprojlim \text{Pic}(G_n^\ast) \]
(see [1], [6], [5]). It seems reasonable to conjecture that \( \Psi_F \) 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. \( \Box \)

5. **Proof of Theorem 1.3**

In this section we give the proof of Theorem 1.3.

For each integer \( n \) the action of \( \Omega_F \) on \( \Gamma_n^\ast \) yields a representation
\[ \rho_n^\ast : \Omega_F \to \text{Aut}(\Gamma_n^\ast). \]
Write \( F_n^* \) for the fixed field of \( \rho_n^* \); then \( F_n^* = \bigcup_n F_n^* \), where \( F_n^* \) is the extension of \( F \) cut out by \( \rho^* \). The group scheme \( G_n^* \) is constant over \( \text{Spec}(F_n^*) \), and we write

\[
\eta_{n,F_n^*} : \text{Ker}(\phi_{n,F_n^*}) \xrightarrow{\sim} \text{Hom}(\Gamma_n^*, O_{F_n^*}/(O_{F_n^*})^p_n)
\]

for the isomorphism afforded by Proposition 3.9(ii).

Consider the map

\[
d_n : H^1(F_n^*, \Gamma_n) \xrightarrow{\phi_{n,F_n^*}} H^1(F_n^*, \Gamma_{n-1}) \xrightarrow{\text{Cores}_{F_n^*/F_{n-1}^*}} H^1(F_{n-1}^*, \Gamma_{n-1}).
\]

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

\[
d_n : H^1(F_n^*, \Gamma_n) \rightarrow H^1(F_{n-1}^*, \Gamma_{n-1})
\]

induces isomorphisms

\[
\lim_{\leftarrow} H^1(F_n^*, \Gamma_n) \xrightarrow{\sim} \lim_{\leftarrow} H^1(F_n^*, T),
\]

\[
\lim_{\leftarrow} H^1(F_n^*, \Gamma_n) \xrightarrow{\sim} \lim_{\leftarrow} H^1(F_{n-1}^*, T)
\]

(5.1)

(5.2)

**Proof.** See e.g. [23, Lemma B.3.1].

Let \( h_n \) denote the composition

\[
h_n : \text{Hom}(\Gamma_n^*, F_n^{*x}/(F_n^{*x})^p_n) \xrightarrow{r_n} \text{Hom}(\Gamma_n^*, F_{n-1}^*/(F_n^{*x})^p_{n-1}) \xrightarrow{N_{F_n^*/F_n^{*x}}} \text{Hom}(\Gamma_{n-1}^*, F_{n-1}^*/(F_{n-1}^{*x})^{p_{n-1}}),
\]

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

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

\[
h_n : \text{Hom}(\Gamma_n^*, F_n^{*x}/(F_n^{*x})^p_n) \rightarrow \text{Hom}(\Gamma_n^*, F_{n-1}^*/(F_{n-1}^{*x})^{p_{n-1}})
\]

induces isomorphisms

\[
\lim_{\leftarrow} \text{Hom}(\Gamma_n^*, F_n^{*x}/(F_n^{*x})^p_n) \xrightarrow{\sim} \text{Hom}(T^*, \lim_{\leftarrow} F_n^{*x}),
\]

\[
\lim_{\leftarrow} \text{Hom}(\Gamma_n^*, O_{F_n^*}/(O_{F_n^*})^p_n) \xrightarrow{\sim} \text{Hom}(T^*, O_{F_n^*}).
\]
Proof. This is proved by applying Lemma 5.1 to the $p$-divisible group schemes $(\mathbb{Z}/p^n\mathbb{Z})_{n \geq 1}$ and $(\mu_{p^n})_{n \geq 1}$. We have

$$\lim_{\leftarrow} \left[ \text{Hom}(\Gamma^*_n, F^*_n/(F^*_n)^{p^n}) \right] = \lim_{\leftarrow} \left[ \text{Hom}(\Gamma^*_n, \mathbb{Z}/p^n \mathbb{Z}) \otimes \mathbb{Z}_p (F^*_n/(F^*_n)^{p^n}) \right]$$

$$= \left[ \lim_{\leftarrow} \text{Hom}(\Gamma^*_n, \mathbb{Z}/p^n \mathbb{Z}) \right] \otimes \mathbb{Z}_p \left[ \lim_{\leftarrow} (F^*_n/(F^*_n)^{p^n}) \right]$$

$$= \text{Hom}(T^*, \mathbb{Z}_p) \otimes \mathbb{Z}_p \lim_{\leftarrow} H^1(F^*_n, \mu_{p^n})$$

$$= \text{Hom}(T^*, \mathbb{Z}_p) \otimes \mathbb{Z}_p \lim_{\leftarrow} H^1(F^*_n, \mathbb{Z}_p(1))$$

$$= \text{Hom}(T^*, \mathbb{Z}_p) \otimes \mathbb{Z}_p \lim_{\leftarrow} \tilde{F}_n^{\times}$$

$$= \text{Hom}(T^*, \lim_{\leftarrow} \tilde{F}_n^{\times}).$$

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

Lemma 5.3. The following diagram is commutative:

$$\begin{align*}
H^1(F^*_n, \Gamma_n) & \xrightarrow{\eta_n, F^*_n} \text{Hom}(\Gamma^*_n, F^*_n/(F^*_n)^{p^n}) \\
\downarrow d_n & \quad \downarrow h_n \\
H^1(F^*_{n-1}, \Gamma_{n-1}) & \xrightarrow{\eta_{n-1}, F^*_{n-1}} \text{Hom}(\Gamma^*_{n-1}, F^*_{n-1}/(F^*_{n-1})^{p^{n-1}}).
\end{align*}$$

(5.3)

Proof. Note that $G^*_n$ is constant over $\text{Spec}(F^*_n)$. The result now follows from Theorem 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

$$\beta : \lim_{\leftarrow} H^1(F^*_n, T) \xrightarrow{\sim} \text{Hom}(T^*, \lim_{\leftarrow} \tilde{F}_n^{\times}).$$

(5.4)

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

$$\beta_v : \lim_{\leftarrow} H^1(F^*_n, T) \xrightarrow{\sim} \text{Hom}(T^*, \lim_{\leftarrow} \tilde{F}_n^{\times}).$$

(5.5)

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

$$\beta_v : \lim_{\leftarrow} H^1(F^*_n, T) \xrightarrow{\sim} \text{Hom}(T^*, \lim_{\leftarrow} \tilde{F}_n^{\times}).$$

(5.6)

(ii) The map $\beta$ induces an isomorphism

$$\beta : \lim_{\leftarrow} H^1(F^*_n, T) \xrightarrow{\sim} \text{Hom}(T^*, \lim_{\leftarrow} \tilde{O}_{F_n}^{\times}).$$

(5.7)

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

$$\lim_{\leftarrow} H^1(F^*_n, \Gamma_n) \xrightarrow{\sim} \lim_{\leftarrow} H^1(F^*_n, T).$$
The result now follows from the isomorphism
\[ H^1\left( F^*_n, G_n \right) \cong \text{Hom}( \Gamma^*_n, O^\times_{F^*_n, v} / (O^\times_{F^*_n, v})^{p^n} ) \]
afforded by Proposition 3.9(i).

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

**Corollary 5.5.** There is a natural isomorphism
\[ \varprojlim H^1\left( F^*_n, T \right) \cong \varprojlim \ker( \Phi_{F^*_n} ). \]

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

Corollary 5.5 implies that we have
\[ \bigcap_n \text{Cores}_{F^*_n/F}( H^1\left( F^*_n, T \right)) \subseteq \ker( \Phi_{F^*_n} ). \]
Hence, if \( x \in \mathcal{G}_F(T) \), 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 1.3.

6. **Proof of Theorem 1.1**

This section is devoted to the proof of Theorem 1.1.

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

**Lemma 6.1.** Suppose that \( m \geq 1 \). Then
\[ \varprojlim \text{Cl}( \mathcal{M}^{(p)}_{m, O_{C_n} } ) = 0, \]
where the inverse limit is taken with respect to the maps \( N_{C_n/C_{n-1}} \).

**Proof.** In order to ease notation somewhat, we write \( \mathcal{M}^{(p)} \) for \( \mathcal{M}^{(p)}_m \). Using the notation of Remark 2.6 we have
\[ \mathcal{M}^{(p)}_{C_n} \cong \prod_{\gamma^* \in \Gamma_m \setminus \Omega_{C_n}} O_{C_n[\gamma^*]}[1/p], \]
and so
\[ \text{Cl}( \mathcal{M}^{(p)}_{C_n} ) \cong \prod_{\gamma^* \in \Gamma_m \setminus \Omega_{C_n}} \text{Cl}( O_{C_n[\gamma^*]}[1/p] ). \]
Choose \( d \geq 1 \) sufficiently large that
\[ \Gamma_m \setminus \Omega_{C_d} = \Gamma_m \setminus \Omega_{C_i} \]
for all \( i \geq d \). Then, for each \( \gamma^* \in \Gamma_m^* \setminus \Omega_{C_d} \)

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

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

\[
\mathcal{N}_{C_i/C_d} : \text{Cl}(\mathfrak{m}_{O_{C_i}}^{(p)}) \to \text{Cl}(\mathfrak{m}_{C_d}^{(p)})
\]

is induced by the usual norm maps

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

for each \( \gamma^* \in \Gamma_m^* \setminus \Omega_{C_i} = \Gamma_m^* \setminus \Omega_{C_d} \).

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

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

and so it follows that

\[
\varprojlim \text{Cl}(\mathfrak{m}_{O_{C_n}}^{(p)}) = 0,
\]

as claimed. \( \square \)

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

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

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

\[
\varprojlim \Phi_C^{(p)} : \varprojlim H^1_{\mathfrak{m}(T)_{O_{C_n}}}(C_n, T) \to \varprojlim \text{Cl}(\mathfrak{m}_{O_{C_n}}^{(p)}(T)),
\]

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

\[
\bigcap_n \text{Cores}_{C_n/F}(H^1_{\mathfrak{m}(T)_{O_{C_n}}}(C_n, T)) \subseteq \text{Ker}(\Phi_F^{(p)}).
\]

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

We now recall the definition of the pairing

\[
B_F : H^1_{f,(p)}(F, T) \times \text{Ker}(\text{Loc}_{F,T^*}) \to \mathbb{Q}_p
\]

given in [20, Section 3.1.4].

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

\[
0 \to T^* \to T'_y \to \mathbb{Z}_p \to 0.
\] (6.1)
Taking $\mathbb{Z}_p(1)$-duals of (6.1) yields an exact sequence

$$1 \to \mathbb{Z}_p(1) \to T_y \to T \to 0.$$  \hspace{1cm} (6.2)

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

$$H^1(F, \mathbb{Z}_p(1)) \xrightarrow{i} H^1(F, T_y) \xrightarrow{j} H^1(F, T) \xrightarrow{} H^2(F, \mathbb{Z}_p(1))$$

$$H^1(F_v, \mathbb{Z}_p(1)) \xrightarrow{i_v} H^1(F_v, T_y) \xrightarrow{j_v} H^1(F_v, T) \xrightarrow{} H^2(F_v, \mathbb{Z}_p(1)).$$ \hspace{1cm} (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 $v \not| p$.

At places $v | p$ the extension (6.2) splits locally at $v$ because $y \in \text{Ker}(\text{Loc}_{F,T}^*)$, and so we have a corresponding splitting

$$H^1(F_v, T_y) = H^1(F_v, \mathbb{Z}_p(1)) \oplus H^1(F_v, T)$$ \hspace{1cm} (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

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

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 $v \not| p$, choose any local lifting $\lambda_v \in H^1_F(F_v, T_y)$ of $x_v \in H^1(F_v, T)$. For places $v$ with $v | p$, 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 $\tilde{x}_v - \lambda_v \in i_v(H^1(F_f, \mathbb{Z}_p(1)))$. If $v | p$, then $i_v$ is injective, and so we may in fact identify $i_v(H^1(F_v, \mathbb{Z}_p(1)))$ with $H^1(F_v, \mathbb{Z}_p(1))$.

Let

$$l_x : \bigoplus_v H^1(F_v, \mathbb{Z}_p(1)) \to \mathbb{Q}_p$$

denote the composition

$$\bigoplus_v H^1(F_v, \mathbb{Z}_p(1)) \simeq \bigoplus_v \mathbb{F}_v^\times \xrightarrow{L_x} \mathbb{Q}_p,$$
where \( L_\chi \) is defined by

\[
L_\chi((u_v)_v) = \sum_{v|p} \log_p N_{F_v/Q_p}(u_v) - \sum_{v|p} (\log_p q_v) \text{ord}_v(u_v).
\]

(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 \( L_\chi \) induces a well-defined map on \( \oplus_v i_v(H^1(F_v, \mathbb{Z}_p(1))) \). We define

\[
B_F(x, y) = L_\chi \left( \bar{x}_v - \sum_v \lambda_v \right) \in \mathbb{Q}_p.
\]

It is shown in \([20, \text{Section 3.1.4}]\) that \( B_F \) induces a pairing

\[
\langle \langle , \rangle \rangle : \frac{H^1_{f,(p)}(F, T)}{\mathcal{G}_F(T)} \times \text{Ker}(\text{Loc}_{F,T'}) \to \mathbb{Q}_p,
\]

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 \( \Phi_{\mathfrak{M}(p),(1)} \), \( \Phi_{T_y}^{(p)} \) and \( \Phi_T^{(p)} \) for \( \Phi_{\mathfrak{M}(p),(\mathfrak{M}(1))} \), \( \Phi_{\mathfrak{M}(p),(T_y)} \), and \( \Phi_{\mathfrak{M}(p),(T)} \) respectively.

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

**Proof.** It is not hard to check that \([62] \) 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):

\[
\begin{align*}
\mathbf{H}(A(\mathfrak{M}(1))) & \xrightarrow{i} \mathbf{H}(A(T_y)) \to \mathbf{H}(A(T)), \\
\mathbf{H}(A_v(\mathfrak{M}(1))) & \xrightarrow{i_v} \mathbf{H}(A_v(T_y)) \to \mathbf{H}(A_v(T)), \\
\mathbf{H}(\mathfrak{M}(\mathfrak{M}(1))) & \xrightarrow{i} \mathbf{H}(\mathfrak{M}(T_y)) \to \mathbf{H}(\mathfrak{M}(T)), \\
\mathbf{H}(\mathfrak{M}_v(\mathfrak{M}(1))) & \xrightarrow{i_v} \mathbf{H}(\mathfrak{M}_v(T_y)) \to \mathbf{H}(\mathfrak{M}_v(T)).
\end{align*}
\]

It therefore follows from \([6,1] \) that \([62] \) induces a sequence

\[
\text{Cl}(\mathfrak{M}^{(p)}(\mathfrak{M}(1))) \to \text{Cl}(\mathfrak{M}^{(p)}(T_y)) \to \text{Cl}(\mathfrak{M}^{(p)}(T))
\]

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:

\[
\begin{array}{ccc}
\text{Cl}(\mathfrak{M}^{(p)}(\mathfrak{M}(1))) & \xrightarrow{\Phi_{\mathfrak{M}(1)}^{(p)}} & \text{Cl}(\mathfrak{M}^{(p)}(T_y)) & \xrightarrow{\Phi_{T_y}^{(p)}} & \text{Cl}(\mathfrak{M}^{(p)}(T)) \\
\Phi_{\mathfrak{M}(1)}^{(p)} & & \Phi_{T_y}^{(p)} & & \Phi_T^{(p)} \\
H^1_{f,(p)}(F, \mathfrak{M}(1)) & \xrightarrow{i} & H^1_{f,(p)}(F, T_y) & \xrightarrow{j} & H^1_{f,(p)}(F, T).
\end{array}
\]
For each integer \( n > 0 \), the Wedderburn decomposition of \( \mathfrak{M}^{(p)}(\mu_{p^n}) \) (cf. (6.3)) is given by

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

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

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

**Proof.** We first observe from the definition of \( \mathfrak{S}_F(T) \) that if \( M_1x \in \mathfrak{S}_F(T) \) for any integer \( M_1 > 0 \), then \( x \in \mathfrak{S}_F(T) \) 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 \( \Phi^{(p)}_T(\tilde{x}) = 0 \). We shall make this assumption from now on.

It follows from the standard identification of \( H^1(F, T^*) \) with \( \text{Ext}^1_{\Omega_F}(Z_p, T^*) \) that we may write

\[
T_y = Z_p(1) \times T
\]

with \( \Omega_F \)-action given by

\[
(\zeta, t)^\sigma = (\zeta^\sigma \cdot \{f(\sigma^{-1})(t)\}^\sigma, t^\sigma)
\]

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

\[
A_{F^c}(T_y) \xrightarrow{\sim} A_{F^c}(Z_p(1)) \otimes_{F^c} A_{F^c}(T); \quad \alpha \mapsto k_1(\alpha) \otimes k_2(\alpha),
\]

(6.7)

where \( k_1 \) and \( k_2 \) are induced by the projection maps \( Z_p(1) \times T \to Z_p(1) \) and \( Z_p(1) \times T \to T \) respectively.

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

\[
\nu_v = (1 \otimes k_2(\alpha))_v
\]

(cf. (6.4)); this is a resolvend associated to \( \lambda_v \) since \( y \) is locally trivial at \( v \). Then, for each place \( v \) of \( F \), we have

\[
\tau_v := \alpha_v \nu_v^{-1} \in i_v(\text{H}(\mathfrak{M}^{(p)}(Z_p(1)))),
\]

and \( \tau_v \) is a resolvend associated to \( \tilde{x}_v - \lambda_v \in i_v(H^1(F_v, Z_p(1))) \).

If \( v \nmid p \), then \( Z_p(1) \) is unramified at \( v \), and so Remark 3.6 implies that we have

\[
H(\mathfrak{M}^{(p)}_v(Z_p(1))) = H(\mathfrak{M}_v(Z_p(1))) \simeq H^1(F_v, Z_p(1)) \simeq \hat{O}^\times_{F_v}.
\]

Hence it follows that \( (\log_p(q_v)) \text{ord}_v(\tilde{x}_v - \lambda_v) = 0 \).
If $v \mid p$, then $\tau_v = (k_1(\alpha) \otimes 1)_v$, and so $\bigoplus_{v \mid p} \tau_v$ is the image of $k_1(\alpha) \in \mathcal{M}_v^{(p)}(\mathbb{Z}_p(1))_{\mathbb{O}_F^c}$ under the localisation map

$$\delta : \mathcal{M}_v^{(p)}(\mathbb{Z}_p(1))_{\mathbb{O}_F^c} \to \bigoplus_{v \mid p} \mathcal{M}_v^{(p)}(\mathbb{Z}_p(1))_{\mathbb{O}_F^c}.$$  

For each integer $n \geq 1$, write

$$\delta_n : \mathcal{M}_v^{(p)}(\mu_{p^n})_{\mathbb{O}_F^c} \to \bigoplus_{v \mid p} \mathcal{M}_v^{(p)}(\mu_{p^n})_{\mathbb{O}_F^c}$$

for the localisation map, and let $\tau_{v,n}$ denote the image of $\tau_v$ in $\mathcal{M}_v^{(p)}(\mu_{p^n})_{\mathbb{O}_F^c}$ under the natural map $\mathcal{M}_v^{(p)}(\mathbb{Z}_p(1))_{\mathbb{O}_F^c} \to \mathcal{M}_v^{(p)}(\mu_{p^n})_{\mathbb{O}_F^c}$. 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 $H^1(F_v, \mathbb{Z}_p(1)) \to H^1(F_v, \mu_{p^n})$.  

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

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

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

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

This in turn implies that

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

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

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

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

$$\sum_{v \mid p} \log_p\left(N_{F_v/Q_p}(\tilde{x}_v - \lambda_v)\right) = 0.$$

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*, preprint.
[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 Festschrift (Vol. I), P. Cartier, et al., eds, *Prog. in Math.*, 86, Birkhäuser, 1990, 333–400.
[8] N. P. Byott, *Tame realisable classes over Hopf orders*, J. Algebra, 201, (1998), 284–316.
[9] 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.
[10] Ph. Cassou-Noguès, M. J. Taylor, *Elliptic functions and rings of integers*, Prog. in Math. 66 Birkhäuser, 1987.
[11] T. Chinburg, B. Erez, G. Pappas, M. J. Taylor, *Tame actions for group schemes: integrals and slices*, Duke Math. Journal, 82, (1996), 269–308.
[12] C. Curtis, I. Reiner, *Methods of Representation Theory, Volume II*, Wiley, 1987.
[13] R. Greenberg, *Iwasawa theory for p-adic representations*, Adv. Stud. Pure. Math. 17, 97–137.
[14] A. Grothendieck et al., *Groupes de monodromie en géométrie algébrique*, Lecture Notes in Mathematics, Vol. 288, Springer-Verlag, Berlin-New York, 1970.
[15] J. W. Jones, *Plater’s p-adic orthogonality relation for abelian varieties*, Houston J. Math. 21, (1995), 261–282.
[16] 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.
[17] L. R. McCulloh, *Galois module structure of abelian extensions*, Crelle, 375/376, (1987), 259-306.
[18] G. Pappas, *On torsion line bundles and torsion points on abelian varieties*, Duke Math. J., 91 (1998), 215–224.
[19] G. Pappas, *Galois modules and the theorem of the cube*, Invent. Math., 133 (1998), 193–225.
[20] 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).)
[21] A. Plater, *Height pairings on elliptic curves*, Cambridge University Ph.D. thesis, 1991.
[22] A. Plater, *An orthogonality relation on the points of an elliptic curve*, J. London Math. Soc (2), 44 (1991), 227–249.
[23] K. Rubin, *Euler Systems*, Annals of Mathematics Studies 147, Princeton University Press, 2000.
[24] A. Srivastav, M. J. Taylor, *Elliptic curves with complex multiplication and Galois module structure*, Invent. Math., 99, (1990), 165–184.
[25] M. J. Taylor, *Mordell-Weil groups and the Galois module structure of rings of integers*, Ill. J. Math. 32 (1988), 428–452.
[26] M. J. Taylor, *Relative Galois module structure of rings of integers and elliptic functions II*, Ann. Math. (2) 121, (1985), no. 3, 519–535.
[27] 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