.

Iwasawa Theory of Elliptic Curves and Galois Module Structure

A. Agboola[1]

Mathematical Sciences Research Institute[2]
1000 Centennial Drive
Berkeley, CA 94720
U. S. A.

[1] Partially supported by an NSF Postdoctoral Research Fellowship.

[2] Current address: Department of Mathematics, University of California, Berkeley, CA 94720.

§0 Introduction

In this paper we apply techniques arising from Iwasawa theory to study the Galois module structure of principal homogeneous spaces constructed via points of infinite order on CM elliptic curves defined over a number field. This theory was introduced by M.J. Taylor in [T1] (see also [ST], [CN-S] and [CN-T]) and is motivated by the fact that such principal homogeneous spaces are very closely connected with certain rings of integers.

Let E be an elliptic curve with complex multiplication by $\mathfrak{O}$, the ring of integers of an imaginary quadratic field K. If $\alpha \in \mathfrak{O}$, we shall often (but not always) write $[\alpha]$ for the corresponding endomorphism of E. Let F/K be a finite extension over which E is defined and acquires everywhere good reduction. We write $\Delta = \mathrm{Gal}(F/K)$, and we assume that all endomorphisms of E are defined over F. For any field L, we write L^c for an algebraic closure of L, and we set $\Omega_L = \mathrm{Gal}(L^c/L)$.

Let p be an odd rational prime which splits in $\mathfrak{O}$, with $p\mathfrak{O} = \mathfrak{p}\mathfrak{p}^*$. Asssume that $p \not| |\Delta|$. Choose $\pi \in \mathfrak{p}$ with $\mathfrak{p}^h = \pi\mathfrak{O}$ for some $h \geq 1$ and write π^* for the complex conjugate of π. Set $q = \pi\pi^*$.

Write G_i for the subgroup of elements of $E(\mathbb{Q}^c)$ which are killed by $[\pi^{*i}]$. Let $\mathfrak{B}_i$ denote the $\mathfrak{O}_F$-Hopf algebra which represents the $\mathfrak{O}_F$-group scheme of $[\pi^{*i}]$-torsion on E, and let $\mathfrak{A}_i$ be the Cartier dual of $\mathfrak{B}_i$. A detailed description of these algebras is given in [T1] (see also [ST]). There it is shown that $\mathfrak{B}_i$ is an $\mathfrak{O}_F$-order in the algebra $\mathcal{B}_i = \mathrm{Map}_{\Omega_F}(G_i, \mathbb{Q}^c)$ and $\mathfrak{A}_i$ is an order in the algebra $\mathcal{A}_i = (F^c G_i)^{\Omega_F}$ (where here Ω_F acts upon both G_i and F^c). (Here and elsewhere we shall omit from our notation the dependence of our constructions upon the underlying field F unless there is some danger of ambiguity.)

Suppose that $Q \in E(F)$, and write

$$G_Q(i) = \{Q' \in E(\mathbb{Q}^c) : [\pi^{*i}]Q' = Q\}. \tag{0.1}$$

Define the Kummer algebra $F_Q(i)$ by

$$F_Q(i) = \mathrm{Map}_{\Omega_F}(G_Q(i), \mathbb{Q}^c). \tag{0.2}$$

Then $[F_Q(i) : F] = |G_i|$, and $\mathcal{A}_i$ acts on $F_Q(i)$ via

$$(f. \sum_{g \in G_i} a_g g)(Q') = \sum_{g \in G_i} a_g f(Q' + g) \tag{0.3}$$

for $f \in F_Q(i)$ and $\sum_{g \in G_i} a_g g \in \mathcal{A}_i$.

Let $\mathfrak{O}_Q(i)$ denote the integral closure of $\mathfrak{O}_F$ in $F_Q(i)$. In general, $\mathfrak{O}_Q(i)$ does not admit an action of $\mathfrak{A}_i$. We define the Kummer order $\mathfrak{C}_Q(i)$ to be the maximal $\mathfrak{A}_i$-stable submodule of $\mathfrak{O}_Q(i)$, i.e.

$$\mathfrak{C}_Q(i) = \{x \in \mathfrak{O}_Q(i) \mid x.\mathfrak{A}_i \subseteq \mathfrak{O}_Q(i)\}. \tag{0.4}$$

It is shown in [T1] that $\mathfrak{C}_Q(i)$ is a principal homogeneous space (phs) of $\mathfrak{B}_i$, and that $\mathfrak{C}_Q(i)$ is a locally free $\mathfrak{A}_i$-module. Thus $\mathfrak{C}_Q(i)$ defines an element $(\mathfrak{C}_Q(i))$ in the locally free classgroup $\mathrm{Cl}(\mathfrak{A}_i)$ of $\mathfrak{A}_i$. It follows from the definition of $\mathfrak{C}_Q(i)$ that $(\mathfrak{C}_Q(i))$ depends only upon the image of Q in $E(F)/\pi^{*i}E(F)$, and so we obtain a map

$$\psi_i : E(F)/\pi^{*i}E(F) \longrightarrow \mathrm{Cl}(\mathfrak{A}_i) \tag{0.5}$$

given by $\psi_i(Q) = (\mathfrak{C}_Q(i))$. The map ψ_i is in fact a homomorphism since E/F has everywhere good reduction (see Theorem 1 of [T1]), and $\psi_i(Q) = 0$ if and only if $\mathfrak{C}_Q(i)$ is a globally free $\mathfrak{A}_i$-module.

Let $\mathcal{M}_i$ be the maximal order in $\mathcal{A}_i$ containing $\mathfrak{A}_i$. By composing ψ_i with the natural surjection $e_i : \mathrm{Cl}(\mathfrak{A}_i) \to \mathrm{Cl}(\mathcal{M}_i)$ given by extension of scalars, we obtain a homomorphism

$$\varphi_i : E(F)/\pi^{*i}E(F) \longrightarrow \mathrm{Cl}(\mathcal{M}_i) \tag{0.6}$$

given by $\varphi_i(Q) = (\overline{\mathfrak{C}_Q(i)})$, where $\overline{\mathfrak{C}_Q(i)} = \mathfrak{C}_Q(i).\mathcal{M}_i$.

The phs $\mathfrak{C}_Q(i)$ is very closely related to the ring of integers of the field obtained by adjoining the coordinates of the the elements of $G_Q(i)$ to F. Thus a knowledge of the homorphisms ψ_i and φ_i yields important information on the Galois module structure of these rings of integers. (We refer the reader to [BT] for a good general account of applications of the theory of Hopf orders to the study of Galois module structure.)

While the behaviour of the homomorphism ψ_i on torsion points of $E(F)$ is quite well-understood (see [ST], [CN-S]), less is known about the Galois structure of phs arising from points of infinite order. The only general results in this direction of which we are aware are those contained in [T3] and [T4]. In [T3], the methods of [T1] and [Gr] are applied to Heegner points of certain modular elliptic curves. (See also the article by Ph. Cassou-Noguès et al. in [CT] for a brief account of this work.) In [T5], the kernel of ψ_1 is described (under suitable hypotheses) in terms of congruences satisfied by special values of certain p-adic L-functions attached to K. The purpose of this paper is to examine the behaviour of the homomorphisms φ_i on points of infinite order. For further results in this direction, see [AT].

We now give a brief description of the contents of this article. In §1 we show that we may take inverse limits of (0.6) to obtain a homomorphism

$$\Psi_{\mathcal{M}} : E(F) \otimes_{\mathfrak{O}} \mathfrak{O}_{\mathfrak{p}^*} \longrightarrow \varprojlim_i Cl(\mathcal{M}_i). \tag{0.7}$$

We then show that (assuming certain standard conjectures about elliptic curves) $\Psi_{\mathcal{M}}$ is closely related to the algebraic p-adic height pairing

$$\{.,.\}_{F,\mathfrak{p}} : E(F) \otimes_{\mathfrak{O}} \mathfrak{O}_{\mathfrak{p}} \times E(F) \otimes_{\mathfrak{O}} \mathfrak{O}_{\mathfrak{p}^*} \longrightarrow K_{\mathfrak{p}} \tag{0.8}$$

described in [PR1] and [PR2]. By exploiting this relationship, we are able to give a description of $\mathrm{Ker}(\Psi_{\mathcal{M}})$ up to $\mathbb{Z}_p$-pseudo-isomorphism (see §6). One application on of this description is as follows.

Suppose that K is of classnumber 1, that E is defined over K, and that F/K is abelian. Let $\hat{\Delta}$ denote the group of characters of Δ, and let $\mathfrak{O}_1$ (resp. $\mathfrak{O}_2$) denote the ring of integers in some finite extension of $K_{\mathfrak{p}}$ (resp. $K_{\mathfrak{p}^*}$) which contains all of the character values of Δ. Let $\overline{\chi}$ denote the contragredient of χ.

Define $r_\chi = \mathrm{rank}_{\mathfrak{O}_1}[(E(F) \otimes_{\mathfrak{O}} \mathfrak{O}_1)^{\chi})]$, where the superscript χ denotes the χ-equivariant eigenspace for the action of Δ. Let $\text{Ш}(F)(\mathfrak{p})$ be the $\mathfrak{p}$-primary component of the Tate-Shafarevitch group $\text{Ш}(F)$ of E/F.

THEOREM 0.1. *Suppose that $\{.,.\}_{F,\mathfrak{p}}$ is non-degenerate modulo torsion, and that $\text{Ш}(F)(\mathfrak{p})$ is finite. Suppose also that $r_\chi \geq 1$. Then*

$$\mathrm{rank}_{\mathfrak{O}_2}[(\mathrm{Ker}(\Psi_{\mathcal{M}}) \otimes_{\mathfrak{O}} \mathfrak{O}_2)^{\overline{\chi}}] = 1.$$

We remark that similar one-dimensional subspaces of the completed Mordell-Weil group have arisen in the work of several authors in different contexts (see [G1],

[P], [R]).

As a consequence of Theorem 0.1, we are able to deduce

THEOREM 0.2. *Suppose that the hypotheses of Theorem 0.1 hold and that* $r_\chi = 1$ *for some* $\chi \in \hat{\Delta}$. *Then there is a point* $Q \in E(F)$ *of infinite order such that* $\varphi_i(Q) = 0$ *for all* i.

It is interesting to note that the corresponding version of Theorem 0.2 is false in the analogous situation for CM abelian varieties defined over global function fields (see [A]).

The results contained in this paper formed a portion of my Ph.D. thesis (Columbia University, 1991). It is with the greatest of pleasure that I thank my advisor, Professor T.Chinburg, for all of his help, kindness and encouragement. I also wish to extend my warmest thanks to Professor M.J. Taylor for a great deal of extremely generous advice, and to Professor K. Rubin for many very helpful conversations and suggestions. I would like to acknowledge with thanks the hospitality of the MSRI, Berkeley, where this paper was written. Finally, I am very grateful to the referee for pointing out some mistakes in the original version of the manuscript.

§1 Classgroups

In this section we recall various facts we shall require concerning the Hom decsription of the locally free classgroups $\mathrm{Cl}(\mathfrak{A}_i)$ and $\mathrm{Cl}(\mathcal{M}_i)$ in terms of character maps.

We begin by giving a description of the group of characters $\hat{G}_i$ which will be particularly well-suited to certain calculations we shall carry out later. Recall that $q = \pi\pi^*$. Let

$$w_i : E_{\pi^{*i}} \times E_{\pi^i} \longrightarrow \mu_{q^i} \tag{1.1}$$

denote the Weil pairing on E. For each $R \in E_{\pi^i}$, we define a character $\chi_R^{(i)} \in \hat{G}_i$ by

$$\chi_R^{(i)}(g) = w_i(g, R) \qquad \forall g \in E_{\pi^{*i}}. \tag{1.2}$$

This identifies $\hat{G}_i$ with E_{π^i}. If $\omega \in \Omega_F$ and $\chi \in \hat{G}_i$, then ω acts on χ via $\chi^{\omega}(g) = \chi(g^{\omega^{-1}})^{\omega}$. The identification (1.2) preserves this action since the Weil pairing is Ω_F-equivariant.

Let $J(\mathbb{Q}^c)$ denote the group of finite ideles of $\mathbb{Q}^c$ (i.e. the direct limit of the finite idele groups of all finite extensions of $\mathbb{Q}$), and write $U(\mathbb{Q}^c)$ for the subgroup of finite unit ideles of $\mathbb{Q}^c$. Set $U(\mathfrak{A}_i) = \prod_{\mathfrak{q}<\infty} \mathfrak{A}_{i,\mathfrak{q}}^*$, where the direct product runs over all finite places of $\mathfrak{O}_F$. (Here and elsewhere we write $\mathfrak{C}_Q(i)_{\mathfrak{q}}$ (resp. $\mathfrak{A}_{i,\mathfrak{q}}$) for the semi-local completion of $\mathfrak{C}_Q(i)$ (resp. $\mathfrak{A}_i$) at $\mathfrak{q}$.)

Suppose that $u \in U(\mathfrak{A}_i)$. Then u determines a map $\mathrm{Det}(u) \in \mathrm{Map}_{\Omega_F}(E_{\pi^i}, J(\mathbb{Q}^c))$ which is defined by

$$\mathrm{Det}(u)(R)_{\mathfrak{q}} = \chi_R^{(i)}(u_{\mathfrak{q}}). \tag{1.3}$$

Using the identification (1.2) above in Fröhlich's Hom-description of classgroups (see [F] Ch. I §2 or [T2] Ch. I §3), we obtain isomorphisms

$$\mathrm{Cl}(\mathfrak{A}_i) = \frac{\mathrm{Map}_{\Omega_F}(E_{\pi^i}, J(\mathbb{Q}^c))}{\mathrm{Det}(U(\mathfrak{A}_i)).\mathrm{Map}_{\Omega_F}(E_{\pi^i}, \mathbb{Q}^{c*})} \tag{1.4}$$

and

$$\mathrm{Cl}(\mathcal{M}_i) = \frac{\mathrm{Map}_{\Omega_F}(E_{\pi^i}, J(\mathbb{Q}^c))}{\mathrm{Map}_{\Omega_F}(E_{\pi^i}, U(\mathbb{Q}^c)).\mathrm{Map}_{\Omega_F}(E_{\pi^i}, \mathbb{Q}^{c*})}. \tag{1.5}$$

We now recall a method for explicitly constructing a representing map for $(\mathfrak{C}_Q(i)) \in \mathrm{Cl}(\mathfrak{A}_i)$ and $(\overline{\mathfrak{C}_Q(i)}) \in \mathrm{Cl}(\mathcal{M}_i)$.

For each $a \in F_Q(i)$ and $\chi_R^{(i)} \in \hat{G}_i$, the $\chi_R^{(i)}$-resolvent $(a|\chi_R^{(i)}) \in \mathrm{Map}(G_Q(i), \mathbb{Q}^c)$ of a is defined by

$$(a|\chi_R^{(i)}) = \sum_{g \in G_i} \chi_R^{(i)}(g^{-1}) a^g. \tag{1.6}$$

Choose $d_Q^{(i)} \in F_Q(i)$ such that $F_Q(i) = d_Q^{(i)}.\mathcal{A}_i$, and for each prime $\mathfrak{q}$ of $\mathfrak{O}_F$, choose $m_{Q,\mathfrak{q}} \in \mathfrak{C}_Q(i)_\mathfrak{q}$ such that $\mathfrak{C}_Q(i)_\mathfrak{q} = m_{Q,\mathfrak{q}}.\mathfrak{A}_{i,\mathfrak{q}}$. Then the map $h_Q^{(i)} \in Map_{\Omega_F}(E_{\pi^i}, J(\mathbb{Q}^c))$ given by

$$h_Q^{(i)}(R)_\mathfrak{q} = (m_{Q,\mathfrak{q}}|\chi_R^{(i)})(d_Q^{(i)}|\chi_R^{(i)})^{-1} \tag{1.7}$$

represents both $(\mathfrak{C}_Q(i)) \in \mathrm{Cl}(\mathfrak{A}_i)$ and $(\overline{\mathfrak{C}_Q(i)}) \in \mathrm{Cl}(\mathcal{M}_i)$.

For any field L, we let $L(Q;i)$ denote the field obtained by adjoining the coordinates of all points in $G_Q(i)$ to L. We shall have need of the following result on the evaluation of local resolvents which is proved in [T1] (Theorem 3).

Proposition 1.1. *Let $\mathfrak{q}$ be a prime of $\mathfrak{O}_F$, and choose $m \in \mathfrak{C}_Q(i)$ such that $\mathfrak{C}_Q(i)_\mathfrak{q} = m.\mathfrak{A}_{i,\mathfrak{q}}$. Then, for all $Q' \in G_Q(i)$, $\pi^{*-i} \sum_{g \in G_i} m(Q'+g)g^{-1}$ is a unit in the ring $\mathfrak{A}_i(F(Q;i))_\mathfrak{q}$.* $\square$

We shall also require the following result regarding a change of basefield.

Proposition 1.2. *Let L/F be a finite extension. Then the following diagrams commute:*

$$\begin{array}{ccc} E(L) & \xrightarrow{\psi_{i,L}} & \mathrm{Cl}(\mathfrak{A}_i(L)) \\ {\scriptstyle Tr_{L/F}}\downarrow & & \downarrow{\scriptstyle Res} \\ E(F) & \xrightarrow[\psi_{i,F}]{} & \mathrm{Cl}(\mathfrak{A}_i(F)) \end{array} \tag{1.8}$$

$$
\begin{array}{ccc}
E(L) & \xrightarrow{\varphi_{i,L}} & \mathrm{Cl}(\mathcal{M}_i(L)) \\
{\scriptstyle Tr_{L/F}}\downarrow & & \downarrow{\scriptstyle Res} \\
E(F) & \xrightarrow[\varphi_{i,F}]{} & \mathrm{Cl}(\mathcal{M}_i(F))
\end{array}
\tag{1.9}
$$

Here $Tr_{L/F}$ is the usual trace map and Res is the restriction map on classgroups which is induced by the corestriction map

$$
\mathcal{N}: \mathrm{Map}_{\Omega_L}(E_{\pi^i}, J(\mathbb{Q}^c)) \longrightarrow \mathrm{Map}_{\Omega_F}(E_{\pi^i}, J(\mathbb{Q}^c)) \tag{1.10}
$$

defined by

$$
(\mathcal{N} f)(R) = \prod_{i=1}^{n} f(R^{\omega_i^{-1}})^{\omega_i} \qquad \forall R \in E_{\pi^i} \tag{1.11}
$$

where $\{\omega_1, \ldots, \omega_n\}$ is a transversal of $\Omega_L \backslash \Omega_F$.

Proof. See (1.2) of [T1] for a proof of (1.8). An identical argument also works for (1.9). $\square$

§2 Inverse Limits

In this section we shall construct the homomorphism $\Psi_{\mathcal{M}}$ of (0.7). To do this we shall first describe the relationship between $(\mathfrak{C}_Q(i)) \in \mathrm{Cl}(\mathfrak{A}_i)$ and $(\mathfrak{C}_Q(j)) \in \mathrm{Cl}(\mathfrak{A}_j)$ for $0 < j < i$ using the methods of §2 of [ST].

We begin by noting that the natural surjection $[\pi^{*i-j}] : G_i \to G_j$ induces a surjective homomorphism $\mathcal{A}_i \to \mathcal{A}_j$ of Hopf algebras (which we shall also denote by $[\pi^{*i-j}]$) given by

$$
[\pi^{*i-j}](\sum_{g \in G_i} \alpha_g g) = \sum_{g \in G_i} \alpha_g([\pi^{*i-j}]g). \tag{2.1}
$$

Similarly, the inclusion $G_j \to G_i$ induces an inclusion $\mathcal{A}_j \to \mathcal{A}_i$ of Hopf algebras. Passing to the integral level, we deduce that $\mathfrak{A}_j$ may be viewed either as a quotient algebra or as a subalgebra of $\mathfrak{A}_i$.

Next we observe that G_i acts on $\mathrm{Map}(G_i, \mathbb{Q}^c)$ via translations, i.e.

$$f^g(h) = f(g+h) \qquad \forall f \in \mathrm{Map}(G_i, \mathbb{Q}^c),\ g, h \in G_i. \tag{2.2}$$

For each $i \geq j \geq 0$, there is a group isomorphism $G_i/G_j \simeq G_{i-j}$. This induces identifications

$$\mathbb{Q}^c G_{i-j} = (\mathbb{Q}^c G_i)^{G_j} \tag{2.3}$$

and

$$\mathrm{Map}(G_{i-j}, \mathbb{Q}^c) = \mathrm{Map}(G_i, \mathbb{Q}^c)^{G_j}. \tag{2.4}$$

(2.3) and (2.4) in turn induce isomorphisms of $\mathfrak{A}_{i-j}$ with a subalgebra of $\mathfrak{A}_i$ and $\mathfrak{B}_{i-j}$ with a subalgebra of $\mathfrak{B}_i$. We also observe that the identification of of G_j with G_i/G_{i-j} induces an identification of $\hat{G}_j$ with E_{π^j} via the map $R \mapsto \chi_R^{(i)},\ R \in E_{\pi^j}$.

Proposition 2.1. *There are isomorphisms*

$$F_Q(j) \simeq \Sigma_{i-j} F_Q(i) \tag{2.5}$$

as $\mathcal{A}_j$-modules, and

$$\mathfrak{C}_Q(j) \simeq \frac{\Sigma_{i-j}}{\pi^{*i-j}} \mathfrak{C}_Q(i) \tag{2.6}$$

as $\mathfrak{A}_j$-modules.

Here $\Sigma_{i-j} = \sum_{g \in G_{i-j}} g$ viewed as an element of $\mathcal{A}_i$, and $\mathcal{A}_j$ (resp. $\mathfrak{A}_j$) acts on *the right hand side of (2.5) (resp. (2.6)) via the homomorphism* $[\pi^{*i-j}]$.

Proof. See §2 of [ST], especially Proposition 1. $\square$

Lemma 2.2. *The homomorphism*

$$\rho'_{i,j} : \mathrm{Map}_{\Omega_F}(E_{\pi^i}, J(\mathbb{Q}^c)) \longrightarrow \mathrm{Map}_{\Omega_F}(E_{\pi^j}, J(\mathbb{Q}^c))$$

defined by $\rho'_{i,j}(f) = f|E_{\pi^j}$ *induces homomorphisms*

$$\mathrm{Cl}(\mathfrak{A}_i) \longrightarrow \mathrm{Cl}(\mathfrak{A}_j) \tag{2.7)(a}$$

and

$$\mathrm{Cl}(\mathcal{M}_i) \longrightarrow \mathrm{Cl}(\mathcal{M}_j). \tag{2.7)(b}$$

We denote both of these homomorphisms by $\rho_{i,j}$.

Proof. We shall just prove that (2.7)(a) holds, as the proof of (2.7)(b) is entirely similar.

We have to show that

$$\rho'_{i,j}(\mathrm{Det}(U(\mathfrak{A}_i)).\mathrm{Map}_{\Omega_F}(E_{\pi^i}, \mathbb{Q}^{c*})) \subseteq \mathrm{Det}(U(\mathfrak{A}_j)).\mathrm{Map}_{\Omega_F}(E_{\pi^j}, \mathbb{Q}^{c*}). \tag{2.8}$$

It is plain that $\rho'_{i,j}[\mathrm{Map}_{\Omega_F}(E_{\pi^i}, \mathbb{Q}^{c*})] \subseteq \mathrm{Map}_{\Omega_F}(E_{\pi^j}, \mathbb{Q}^{c*})$. Now suppose that $u \in \mathrm{Det}(U(\mathfrak{A}_j))$ and $R \in E_{\pi^j}$. Then

$$\chi_R^{(i)}(u_{\mathfrak{q}}) = \chi_R^{(j)}([\pi^{*i-j}]u_{\mathfrak{q}}) \tag{2.9}$$

and $[\pi^{*i-j}]u_{\mathfrak{q}} \in \mathfrak{A}^*_{j,\mathfrak{q}}$. Hence $\rho'_{i,j}(\mathrm{Det}(u)) = \mathrm{Det}([\pi^{*i-j}]u) \in \mathrm{Det}(U(\mathfrak{A}_j))$, and this establishes the result. $\square$

PROPOSITION 2.3. *Suppose that* $f \in \mathrm{Map}_{\Omega_F}(E_{\pi^i}, J(\mathbb{Q}^c))$ *is a representing map for* $(\mathfrak{C}_Q(i)) \in Cl(\mathfrak{A}_i)$*. Then* $f|E_{\pi^j}$ *is a representing map for* $(\mathfrak{C}_Q(j)) \in \mathrm{Cl}(\mathfrak{A}_j)$ *for all* $0 < j \leq i$*.*

Proof. Choose $d_Q^{(i)} \in F_Q(i)$ such that $F_Q(i) = d_Q^{(i)}.\mathfrak{A}_i$. Then (3.6) implies that $F_Q(j) \simeq (d_Q^{(i)}.(\Sigma_{i-j}/\pi^{*i-j})).\mathcal{A}_j$, (where $\mathcal{A}_j$ acts on the right-hand side of this last isomorphism via the homomorphism $[\pi^{*i-j}]$).

Let H_{ij} be a collection of coset representatives of G_i/G_{i-j}, and suppose that $R \in E_{\pi^j}$. Then

$$\begin{aligned}
\sum_{g \in G_j} (d_Q^{(i)}.\frac{\Sigma_{i-j}}{\pi^{*i-j}})^g \chi_R^{(i)}(g) &= \sum_{g \in G_j} (d_Q^{(i)}.\frac{\Sigma_{i-j}}{\pi^{*i-j}})^g w_i(g, R) \\
&= \sum_{h \in H_{ij}} (d_Q^{(i)}.\frac{\Sigma_{i-j}}{\pi^{*i-j}})^h w_i(h, R) \\
&= \pi^{*j-i} \sum_{g \in G_i} d_Q^{(i)g} w_i(g, R) \\
&= (d_Q^{(i)} | \chi_R^{(i)}) \pi^{*j-i}
\end{aligned}$$

Similarly, if for each place $\mathfrak{q}$ of F we choose $m_{Q,\mathfrak{q}}^{(i)} \in \mathfrak{C}_Q(i)_{\mathfrak{q}}$ such that $\mathfrak{C}_Q(i)_{\mathfrak{q}} = m_{Q,\mathfrak{q}}^{(i)}.\mathfrak{A}_{i,\mathfrak{q}}$, then we obtain

$$\sum_{g \in G_j} (m_{Q,\mathfrak{q}}^{(i)}.\frac{\Sigma_{i-j}}{\pi^{*i-j}}) \chi_R^{(i)}(g) = (m_{Q,\mathfrak{q}}^{(i)} | \chi_R^{(i)}) \pi^{*j-i}.$$

Hence,

$$h_Q^{(j)}(R)_{\mathfrak{q}} = \left[\sum_{g\in G_j}\left(m_{Q,\mathfrak{q}}^{(i)}\cdot\frac{\Sigma_{i-j}}{\pi^{*i-j}}\right)^g \chi_R^{(i)}(g)\right]\left[\sum_{g\in G_j}\left(d_Q^{(i)}\cdot\frac{\Sigma_{i-j}}{\pi^{*i-j}}\right)^g \chi_R^{(i)}(g)\right]^{-1}$$

$$= h_Q^{(i)}(R)_{\mathfrak{q}},$$

and now the result follows from (1.6). $\square$

Thus, if $red : E(F)/\pi^{*i}E(F) \to E(F)/\pi^{*i-1}E(F)$ denotes the natural reduction homomorphism, then we have commutative diagrams

$$\begin{array}{ccc} E(F)/\pi^{*i}E(F) & \xrightarrow{\psi_i} & \mathrm{Cl}(\mathfrak{A}_i) \\ {\scriptstyle red}\downarrow & & \downarrow{\scriptstyle \rho_{i,i-1}} \\ E(F)/\pi^{*i-1}E(F) & \xrightarrow[\psi_{i-1}]{} & \mathrm{Cl}(\mathfrak{A}_{i-1}) \end{array} \qquad (2.10)(a)$$

and

$$\begin{array}{ccc} E(F)/\pi^{*i}E(F) & \xrightarrow{\varphi_i} & \mathrm{Cl}(\mathcal{M}_i) \\ {\scriptstyle red}\downarrow & & \downarrow{\scriptstyle \rho_{i,i-1}} \\ E(F)/\pi^{*i-1}E(F) & \xrightarrow[\varphi_{i-1}]{} & \mathrm{Cl}(\mathcal{M}_{i-1}). \end{array} \qquad (2.10)(b)$$

Taking inverse limits yields homomorphisms

$$\Psi : E(F)\otimes_{\mathfrak{O}} \mathfrak{O}_{\mathfrak{p}^*} \longrightarrow \varprojlim_i \mathrm{Cl}(\mathfrak{A}_i) \qquad (2.11)(a)$$

and

$$\Psi_{\mathcal{M}} : E(F)\otimes_{\mathfrak{O}} \mathfrak{O}_{\mathfrak{p}^*} \longrightarrow \varprojlim_i \mathrm{Cl}(\mathcal{M}_i). \qquad (2.11)(b)$$

§3 The homomorphism $\Psi'_{\mathcal{M}}$

The purpose of this section is to describe certain technical results which will enable us to relate the homomorphism $\Psi_{\mathcal{M}}$ to the Iwasawa theory of E in §5.

We begin by establishing a useful property of a representing map for $(\mathfrak{C}_Q(i)) \in \mathrm{Cl}(\mathfrak{A}_i)$ (resp. $(\overline{\mathfrak{C}_Q(i)}) \in \mathrm{Cl}(\mathcal{M}_i)$.

PROPOSITION 3.1. *Let $h_Q^{(i)} \in \mathrm{Map}_{\Omega_F}(E_{\pi^i}, J(\mathbb{Q}^c))$ be as in (1.7). Then for each $r \in \mathbb{N}$, the Ω_F-map given by $R \mapsto h_Q^{(i)}(rR).h_Q^{(i)}(R)^{-r}$ represents the trivial class in $\mathrm{Cl}(\mathfrak{A}_i)$ (resp. in $\mathrm{Cl}(\mathcal{M}_i)$).*

Proof. Suppose that $Q' \in G_Q(i)$, and let $\omega \in \Omega_F$. Write ${Q'}^{\omega} = Q' + h_\omega$, with $h_\omega \in E_{\pi^{*i}}$. Choose $d_Q^{(i)} \in F_Q(i)$ such that $F_Q(i) = d_Q^{(i)}.\mathcal{A}_i$. Then for each $R \in E_{\pi^i}$ and $r \in \mathbb{N}$, both $\sum_{g\in G_i} d_Q^{(i)}(Q'-g)[r]g$ and $\sum_{g\in G_i} d_Q^{(i)}(Q'-g)g$ lie in $\mathcal{A}_i(F(Q;i)$. We have

$$
\begin{aligned}
&[(\sum_{g\in G_i} d_Q^{(i)}(Q'-g)[r]g)\big(\sum_{g\in G_i} d_Q^{(i)}(Q'-g)g\big)^{-r}]^{\omega}\\
&= \big(\sum_{g\in G_i} d_Q^{(i)}({Q'}^{\omega}-g^{\omega})[r]g^{\omega}\big) \times \big(\sum_{g\in G_i} d_Q^{(i)}({Q'}^{\omega}-g^{\omega})g^{\omega}\big)^{-r}\\
&= \big(\sum_{g\in G_i} d_Q^{(i)}(Q'-g^{\omega}+h_\omega)[r]g^{\omega}\big) \times \big(\sum_{g\in G_i} d_Q^{(i)}(Q'-g^{\omega}+h_\omega)g^{\omega}\big)^{-r}\\
&= \big(\sum_{g\in G_i} d_Q^{(i)}(Q'-g).[r](g+h_\omega)\big) \times \big(\sum_{g\in G_i} d_Q^{(i)}(Q'-g).(g+h_\omega)\big)^{-r}\\
&= \big(\sum_{g\in G_i} d_Q^{(i)}(Q'-g)[r]g\big) \times \big(\sum_{g\in G_i} d_Q^{(i)}(Q'-g)g\big)^{-r}.
\end{aligned}
$$

Thus

$$\Big(\sum_{g\in G_i} d_Q^{(i)}(Q'-g)[r]g\Big)\Big(\sum_{g\in G_i} d_Q^{(i)}(Q'-g)g\Big)^{-r} \in (\mathbb{Q}^c G_i)^{\Omega_F} = \mathcal{A}_i,$$

and similar reasoning also shows that this expression is independent of the choice of $Q' \in G_Q(i)$.

For each place $\mathfrak{q}$ of $\mathfrak{O}_F$ choose $m_{Q,\mathfrak{q}}^{(i)} \in \mathfrak{C}_Q(i)_{\mathfrak{q}}$ such that $\mathfrak{C}_Q(i)_{\mathfrak{q}} = m_{Q,\mathfrak{q}}^{(i)}\mathfrak{A}_{i,\mathfrak{q}}$. Proposition 1.1 implies that

$$\pi^{*-i}\sum_{g\in G_i} m_{Q,\mathfrak{q}}^{(i)}(Q'-g)g, \quad \pi^{*-i}\sum_{g\in G_i} m_{Q,\mathfrak{q}}^{(i)}(Q'-g)[r]g \quad \in \mathfrak{A}_i(F(Q;i))_{\mathfrak{q}}^{*}.$$

Reasoning exactly as above, we conclude that

$$\Big(\pi^{*-i}\sum_{g\in G_i} m_{Q,\mathfrak{q}}^{(i)}(Q'-g)[r]g\Big)\Big(\pi^{*-i}\sum_{g\in G_i} m_{Q,\mathfrak{q}}^{(i)}(Q'-g)g\Big)^{-r} \in [\mathfrak{A}_i(F(Q;i))_{\mathfrak{q}}^{*}]^{\Omega_F} \subseteq \mathfrak{A}_{\mathfrak{q}}^{*}.$$

Thus, it now follows from (1.4) (resp. (1.5)) that the map $R \mapsto h_Q^{(i)}([r]R).h_Q^{(i)}(R)^{-r}$ represents the trivial class in $\mathrm{Cl}(\mathfrak{A}_i)$ (resp. $\mathrm{Cl}(\mathcal{M}_i)$. $\square$

Remark 3.2. It may in fact easily be shown that if $f \in \mathrm{Map}_{\Omega_F}(E_{\pi^i}, J(\mathbb{Q}^c))$ is any representing map for $(\mathfrak{C}_Q(i)) \in \mathrm{Cl}(\mathfrak{A}_i)$, then $f = h_Q^{(i)}$ for suitable choices of $d_Q^{(i)}$ and $m_{Q,\mathfrak{q}}^{(i)}$.

For each $R \in E_{\pi^i}$, we let $F[R]$ denote the field obtained by adjoining the coordinates of R to F (with similar notation $F[R']$ for $R' \in E_{\pi^{*i}}$). We write $F_i = \bigcup_{R\in E_{\pi^i}} F[R]$ and $F_i' = \bigcup_{R'\in E_{\pi^{*i}}} F[R']$. We shall now give a description of $\mathrm{Cl}(\mathcal{M}_i)$ in terms of certain ideal classgroups.

LEMMA 3.3. *Let $E_{\pi^i}\backslash\Omega_F$ denote a set of representatives of Ω_F-orbits of E_{π^i}. Then we have isomorphisms*

(a) $\mathcal{A}_i \simeq \prod_{R\in E_{\pi^i}\backslash\Omega_F} F[R]$

(b) $\mathcal{M}_i \simeq \prod_{R\in E_{\pi^i}\backslash\Omega_F} \mathfrak{O}_{F[R]}$

(c) $\mathrm{Cl}(\mathcal{M}_i) \simeq \prod_{R\in E_{\pi^i}\backslash\Omega_F} Cl(\mathfrak{O}_{F[R]})$.

Proof. (b) and (c) follow immediately from (a), which we shall now prove. Let $\{\omega_1,\dots,\omega_n\}$ be a transversal of $\Omega_F\backslash\Omega_{F_i'}$. then $\mathcal{A}_i = (\mathbb{Q}^c G_i)^{\Omega_F} = (F_i' G_i)^{\Omega_F}$ is generated over F by all elements of the form $\sum_\omega l^\omega g^\omega$, where $l\in F_i'$ and $g\in G_i$. Suppose that $R\in E_{\pi^i}$ and $\lambda\in\Omega_F$. Then,

$$\begin{aligned}\Big(\sum_\omega l^\omega \chi_R^{(i)}(g^\omega)\Big)^\lambda &= \Big(\sum_\omega l^\omega w_i(R,g^\omega)\Big)^\lambda\\ &= \sum_\omega l^{\omega\lambda} w_i(R^\lambda, g^{\omega\lambda})\\ &= \sum_\omega l^\omega \chi_{R^\lambda}^{(i)}(g^\omega)\end{aligned}$$

Hence $(F_i' G_i)^{\Omega_F} \subseteq \prod_{R\in E_{\pi^i}\backslash\Omega_F} F[R]$. Since both sides of the inclusion have the same dimension over F as F-vector spaces, it follows that (a) holds. $\square$

If $\alpha\in\mathrm{Cl}(\mathcal{M}_i)$ is represented by $f\in\mathrm{Map}_{\Omega_F}(E_{\pi^i}, J(\mathbb{Q}^c))$, then the image of α under the isomorphism 3.3(b) is obtained by evaluating f on elements of $E_{\pi^i}\backslash\Omega_F$ and then taking ideal content. Thus every element of $\mathrm{Cl}(\mathcal{M}_i)$ may be represented by a map $R\mapsto I_R$, with $I_R\in\mathrm{Cl}(\mathfrak{O}_{F[R]})$ satisfying $I_{R^\omega} = I_R^\omega$ for all $\omega\in\Omega_F$. Conversely, every such map defines an element of $\mathrm{Cl}(\mathcal{M}_i)$.

LEMMA 3.4. *Choose $d_Q^{(i)}\in F_Q(i)$ such that $F_Q(i)\in d_Q^{(i)}.\mathcal{A}_i$. Suppose that $Q'\in G_Q(i)$, and let $R\in E_{\pi^r}$ with $0<r\le i$. Then*

(a) $\sum_{g\in G_i}[d_Q^{(i)g^{-1}}(Q')\chi_R^{(i)}(g)] \in F[R](Q;i)$

(b) $\big(\sum_{g\in G_i}[d_Q^{(i)g^{-1}}(Q')\chi_R^{(i)}(g)]\big)^{q^r} \in F[R]$.

(Recall that $F[R](Q;i)$ denotes the field obtained by adjoining the coordinates of all points in $G_Q(i)$ to $F[R]$.)

Proof. We shall just prove (b), since the proof of (a) is very similar. Let $\omega \in \Omega_{F[R]}$, and write $Q'^{\omega} = Q' + h_\omega$, with $h_\omega \in E_{\pi^{*i}}$. Recall that $q = \pi\pi^*$. Then,

$$\begin{aligned}
\Big(\Big[\sum_{g\in G_i} d_Q^{(i)g^{-1}}(Q')\chi_R^{(i)}(g)\Big]^{q^r}\Big)^{\omega} &= \Big[\sum_{g\in G_i} d_Q^{(i)}(Q'^{\omega} - g^{\omega}).w_i(g^{\omega}, R^{\omega})\Big]^{q^r} \\
&= \Big[w_i(h_\omega, R^\omega)\sum_{g\in G_i} d_Q^{(i)}(Q'-g).w_i(g, R^\omega)\Big]^{q^r} \\
&= \Big[\sum_{g\in G_i} d_Q^{(i)}(Q'-g).w_i(g, R)\Big]^{q^r}.
\end{aligned}$$

Hence $\big[\sum_{g\in G_i} d_Q^{(i)}(Q'-g).w_i(g,R)\big]^{q^r} \in F[R]$, and is independent of the choice of Q'. $\square$

Now Proposition 1.1 implies that

$$c(h_Q^{(i)}(R)).\mathfrak{O}_{F[R](Q;i)} = (d_Q^{(i)}|\chi_R^{(i)})(Q').\pi^{*-1}.\mathfrak{O}_{F[R](Q;i)} \qquad (3.1),$$

where c denotes ideal content. If $d_Q^{(i)}$ is chosen to be an $\mathfrak{A}_{i,\mathfrak{q}}$-basis of $\mathfrak{C}_Q(i)_{\mathfrak{q}}$ for all primes $\mathfrak{q}|\pi^*$ then (from Proposition 1.1 again), $(d_Q^{(i)}|\chi_R^{(i)})(Q').\pi^{*-i}$ is a unit at all such $\mathfrak{q}$. Since we have assumed that E/F has everywhere good reduction, it follows from the criterion of Néron-Ogg-Shafarevitch that $F[R](Q;i)/F[R]$ is unramified at all primes away from $\mathfrak{p}^*$. As $(d_Q^{(i)}|\chi_R^{(i)})(Q')^{q^r} \in F[R]$ (see Lemma 3.4(b)), it follows that $(d_Q^{(i)}|\chi_R^{(i)})(Q').\mathfrak{O}_{F[R](Q;i)}$ is an ambiguous ideal, i.e. that we have

$$(d_Q^{(i)}|\chi_R^{(i)})(Q').\mathfrak{O}_{F[R](Q;i)} = \vartheta_R.\mathfrak{O}_{F[R](Q;i)} \tag{3.2}$$

where ϑ_R is an $\mathfrak{O}_{F[R]}$-ideal.

Hence, in the notation of the remarks following Lemma 3.3, we deduce that $(\overline{\mathfrak{C}_Q(i)}) \in \mathrm{Cl}(\mathcal{M}_i)$ is represented by the map

$$R \mapsto (\vartheta_R)^{-1} \tag{3.3}$$

where (ϑ_R) denotes the class of the ideal ϑ_R in $\mathfrak{O}_{F[R]}$.

For each $R \in E_{\pi^i}$, it follows from (3.1) and (3.2), together with Proposition 3.1, that

$$(\vartheta_R)^q = (\vartheta_{qR}\mathfrak{O}_{F[R]}) \tag{3.4}$$

in $Cl(\mathfrak{O}_{F[R]})$. Now $[F[R] : F[qR]] = [F[R] : F[\pi R]] = q$ if the order of R is sufficiently large. Thus, if $[F[R] : F[qR]] = q$, then

$$(\vartheta_{qR}) = N_{F[R]/F[qR]}(\vartheta_R) \tag{3.5}$$

in $Cl(\mathfrak{O}_{F[qR]})$, where $N_{F[R]/F[qR]}$ is the norm from $F[R]$ to $F[qR]$.

We now observe that $F[R] \subseteq F_i$, and so via the natural homomorphism $\mathrm{Cl}(\mathfrak{O}_{F[R]}) \to \mathrm{Cl}(\mathfrak{O}_{F_i})$, $(\vartheta_R) \in \mathrm{Cl}(\mathfrak{O}_{F[R]})$ defines an element of $\mathrm{Cl}(\mathfrak{O}_{F_i})$. Thus φ_i induces a homomorphism

$$\varphi_i^{(e)} : E(F)/\pi^{*i}E(F) \longrightarrow \mathrm{Map}_{\Omega_F}(E_{\pi^i}, \mathrm{Cl}(\mathfrak{O}_{F_i})) \tag{3.6}$$

defined by

$$\varphi_i^{(e)}(Q)(R) = (\vartheta_R.\mathfrak{O}_{F_i}). \tag{3.6)(a}$$

Now Proposition 3.1 implies that $c(h_Q^{(i)}(rR)h_Q^{(i)}(R)^{-r})$ is a principal ideal for each $r \in \mathbb{N}$. Hence

$$(\vartheta_{rR}.\mathfrak{O}_{F_i}) = (\vartheta_R.\mathfrak{O}_{F_i})^r$$

and so we in fact have

$$\varphi_i^{(e)} : E(F)/\pi^{*i}E(F) \longrightarrow \mathrm{Hom}_{\Omega_F}(E_{\pi^i}, \mathrm{Cl}(\mathfrak{O}_{F_i})_p) \tag{3.7}$$

where $\mathrm{Cl}(\mathfrak{O}_{F_i})_p$ denotes the p-primary part of $\mathrm{Cl}(\mathfrak{O}_{F_i})$.

We next observe that the restriction of $[\pi^*]$ to E_{π^i} is an automorphism. For each $Q \in E(F)$, define $\varphi'_i(Q) \in \mathrm{Hom}_{\Omega_F}(E_{\pi^i}, \mathrm{Cl}(\mathfrak{O}_{F_i})_p)$ by

$$\varphi'_i(Q)(R) = \varphi_i^{(e)}(Q)([\pi^*]^{-i}R). \tag{3.8}$$

Let $Tr_{F_i/F_{i-1}}$ denote the trace map from F_i to F_{i-1}. Since $Tr_{F_i/F_{i-1}}(R) = [q]R$ for all sufficiently large i, it follows that

$$N_{F_i/F_{i-1}}(\varphi'_i(Q)(R)) = \varphi'_{i-1}(Q)([\pi]R) \tag{3.9}$$

(for i sufficiently large), where $N_{F_i/F_{i-1}}$ is the norm from F_i to F_{i-1}. In other words, the following diagram commutes

$$\begin{array}{ccc} E(F)/\pi^{*i}E(F) & \xrightarrow{\varphi_i'} & \mathrm{Hom}_{\Omega_F}(E_{\pi^i}, \mathrm{Cl}(\mathfrak{O}_{F_i})_p) \\ {\scriptstyle red}\downarrow & & \downarrow{\scriptstyle N_{i/i-1}} \\ E(F)/\pi^{*i-1}E(F) & \xrightarrow[\varphi_{i-1}']{} & \mathrm{Hom}_{\Omega_F}(E_{\pi^{i-1}}, \mathrm{Cl}(\mathfrak{O}_{F_{i-1}})_p). \end{array} \tag{3.10}$$

Here $N_{i/i-1}$ is defined by

$$N_{i/i-1}(\varphi_i'(Q)(R)) = N_{F_i/F_{i-1}}(\varphi_i'(Q)(R')) \tag{3.11}$$

where R' is any element of E_{π^i} satisfying $[\pi]R' = R$. It is easily checked that this is well-defined.

Taking inverse limits of (3.10), we obtain a homomorphism

$$\Psi'_{\mathcal{M}} : E(F) \otimes_{\mathfrak{O}} \mathfrak{O}_{\mathfrak{p}^*} \longrightarrow \mathrm{Hom}_{\Omega_F}(T_\pi, \varprojlim_i \mathrm{Cl}(\mathfrak{O}_{F_i})_p) \tag{3.12}$$

where T_π is the π-adic Tate module of E and the inverse limit $\varprojlim_i \mathrm{Cl}(\mathfrak{O}_{F_i})_p$ is taken with respect to the norm maps $N_{F_i/F_{i-1}}$.

It is clear that the homomorphism $\Psi'_{\mathcal{M}}$ completely determines $\Psi_{\mathcal{M}}$. In particular, we have

LEMMA 3.5. $\mathrm{Ker}(\Psi'_{\mathcal{M}}) = \mathrm{Ker}(\Psi_{\mathcal{M}})$. □

§4. Selmer Groups

In this section we recall various results we shall require concerning Selmer groups.

Set $F_\infty = \bigcup_i F_i$ and $F'_\infty = \bigcup_i F'_i$. Let N_∞/F be the unique $\mathbb{Z}_p$-extension contained in F_∞/F, and write $\Gamma = \mathrm{Gal}(N_\infty/F)$. We may identify Γ with $\mathrm{Gal}(F_\infty/F(E_\mathfrak{p}))$, and $\mathrm{Gal}(F(E_\mathfrak{p})/F)$ with $\mathrm{Gal}(N_\infty/F_\infty)$. Let $\chi_\infty : \mathrm{Gal}(F_\infty/F) \to \mathfrak{O}_\mathfrak{p}^*$ denote the character giving the action of $\mathrm{Gal}(F_\infty/F)$ on E_{π^∞}. We have

$$\begin{aligned}\mathrm{Gal}(F_\infty/F) &\simeq \mathrm{Gal}(F_\infty/F(E_\mathfrak{p})) \times \mathrm{Gal}(F(E_\mathfrak{p})/F)\\ &\simeq \Gamma \times \mathrm{Gal}(F(E_\mathfrak{p})/F).\end{aligned}$$

Write ε (resp. κ) for the restriction of χ_∞ to $\mathrm{Gal}(F(E_\mathfrak{p})/F)$ (resp. Γ).

Choose a topological generator γ of Γ, and write Λ for the power series ring $\mathbb{Z}_p[\![T]\!]$. Then we may identify Λ with the completed group ring $\mathbb{Z}_p[\![\Gamma]\!]$ in the usual manner via the map $\gamma \mapsto T+1$.

For each i, let $\mathcal{H}_i/F_i$ be the maximal everwhere unramified abelian pro-p extension of F_i, and let $\mathcal{X}_i/F_i$ be the maximal abelian pro-p extension of F_i which is unramified away from primes dividing $\mathfrak{p}$. Set $H_i = \mathrm{Gal}(\mathcal{H}_i/F_i)$, $X_i = \mathrm{Gal}(\mathcal{X}_i/F_i)$, and write H_∞ (resp. X_∞) for the inverse limit of the $\mathcal{H}_i$ (resp. $\mathcal{X}_i$).

If $\mathfrak{q}$ is a prime of F, we write $k_\mathfrak{q}$ for the residue field of F at $\mathfrak{q}$, and we let $\tilde{E}(k_\mathfrak{q})$ denote the reduction of $E(F)$ at $\mathfrak{q}$. Write $E_{1,\mathfrak{q}}(F)$ for the kernel of reduction of $E(F)$ at $\mathfrak{q}$, and define $E_{1,\mathfrak{p}}(F) = E_1(F)$ via exactness of the sequence

$$0 \longrightarrow E_1(F) \longrightarrow E(F) \longrightarrow \prod_{\mathfrak{q}|\mathfrak{p}} \tilde{E}(k_\mathfrak{q}). \tag{4.1}$$

We now recall the definitions of the Selmer and the Tate-Shafarevitch groups of E. Let L be any extension of K over which E is defined. The Selmer group $S(L)^{\pi^{*i}}$ is defined to be the kernel of the natural homomorphism

$$H^1(\Omega_L, E_{\pi^{*i}}) \longrightarrow \prod_{\mathfrak{q} \ of \ L} H^1(\Omega_{L_\mathfrak{q}}, E). \tag{4.2}$$

The enlarged Selmer group $S'(L)^{\pi^{*i}}$ is the kernel of the homomorphism

$$H^1(\Omega_L, E_{\pi^{*i}}) \longrightarrow \prod_{\mathfrak{q} \ \nmid \mathfrak{p}^*} H^1(\Omega_{L_\mathfrak{q}}, E). \tag{4.3}$$

The Selmer groups $S(L)^{\pi^i}$ and $S'(L)^{\pi^i}$ are defined similarly. We set $S(L) = \varinjlim_i S(L)^{\pi^i}$ and we write $Y(L)$ for the Pontryagin dual of $S(L)$

The Tate-Shafarevitch group $\text{Ш}(L)$ of E/L is defined to be the kernel of the map

$$H^1(\Omega_L, E) \longrightarrow \prod_{\mathfrak{q} \ of \ L} H^1(\Omega_{L_\mathfrak{q}}, E). \tag{4.4}$$

Define $\Sigma(F)^{(\pi^{*i})}$ to be the subgroup of $S(F)^{\pi^{*i}}$ which makes the following sequence exact

$$0 \longrightarrow \Sigma(F)^{(\pi^{*i})} \longrightarrow S(F)^{\pi^{*i}} \longrightarrow \prod_{v|\mathfrak{p}} H^1(\Omega_{F_v}, E_{\pi^{*i}}),$$

and set $\Sigma(F) = \varprojlim_i \Sigma(F)^{\pi^{*i}}$. Then there is a natural injection $E_1(F) \otimes_{\mathfrak{O}} \mathfrak{O}_{\mathfrak{p}^*} \longrightarrow \Sigma(F)$. The following result is shown in Corollaire 3.3 of [PR1].

Lemma 4.1. *If $|\text{Ш}(F)(\mathfrak{p}^*)| < \infty$, then $E_1(F) \otimes_{\mathfrak{O}} \mathfrak{O}_{\mathfrak{p}^*} = \Sigma(F)$.* $\square$

Proposition 4.2. (J.Coates). *There are Λ-module isomorphisms*

(a) $S(N_\infty) \simeq Hom(X_\infty^{(\varepsilon)}, E_{\pi^\infty})$.

(b) $Y(N_\infty) \simeq Hom(T_\pi, X_\infty^{(\varepsilon)})$

Proof. (a) See Theorems 12 and 9 of [Co].

(b) Write $D_\mathfrak{p} = K_\mathfrak{p}/\mathfrak{O}_\mathfrak{p}$. Choosing a generator t of T_π over $\mathfrak{O}_\mathfrak{p}$ is equivalent to fixing an isomorphism $\mathfrak{O}_\mathfrak{p} \to T_\pi$ such that $1 \mapsto t$. This in turn induces an isomorphism $\phi : D_\mathfrak{p} \to E_{\pi^\infty}$. Via such a choice of t, we may define a pairing

$$(.,.) : Hom(T_\pi, X_\infty^{(\varepsilon)}) \times Hom(X_\infty^{(\varepsilon)}, E_{\pi^\infty}) \longrightarrow D_\mathfrak{p} \tag{4.5}$$

by $(f_1, f_2) = \phi^{-1}(f_2(f_1(t)))$. It is easy to check that $(.,.)$ is independent of the choice of t, is non-degenerate, and is Ω_F-equivariant, which gives the result. $\square$

We conclude this section with a description of the weak $\mathfrak{p}$-adic Leopoldt conjecture for F. Let L/K be a finite extension, and for each prime $\mathfrak{q}$ of L, let $U(L_\mathfrak{q})$ denote the group of units of the local completion $L_\mathfrak{q}$ of L at $\mathfrak{q}$. Write $U(L)$ for the group of global units of L. Then there is a natural injection

$$i_L : U(L) \longrightarrow \prod_{\mathfrak{q}|\mathfrak{p}} U(L_\mathfrak{q}) \tag{4.6}$$

given by the diagonal embedding $i(x) = (x, x, \ldots, x)$.

Let $\overline{i_L(U(L))}$ denote the closure of $i_L(U(L))$ with respect to the $\mathfrak{p}$-adic topology. Write $\delta(L)$ for the difference between the $\mathbb{Z}_p$-rank of $U(L)$ and the $\mathbb{Z}_p$-rank of $\overline{i_L(U(L))}$. Then the weak $\mathfrak{p}$-adic Leopoldt conjecture for F asserts that the numbers $\delta(L)$ are bounded independently of L as L runs through the set of all finite extensions of F which are contained in F_∞.

We shall assume for the rest of this paper that the weak $\mathfrak{p}$-adic Leopoldt conjecture holds for F. This is known to be the case if F/K is abelian, via work of A. Brumer (see [Br]). We shall also assume that $|\text{Ш}(F)(\mathfrak{p}^*)| < \infty$, and so in particular that Lemma 4.1 holds.

§5 The algebraic $\mathfrak{p}$-adic height pairing.

In this section we describe the $\mathfrak{p}$-adic height pairing on E/F and explain its relationship to the homomorphism $\Psi'_{\mathcal{M}}$. We refer the reader to §3 of [PR1] or Chapter IVof [PR2] for full details of the results we use concerning $\mathfrak{p}$-adic heights.

Let $J(F_i)$ denote the ideles of F_i. Write $U_i^{(\mathfrak{p})}$ for the subgroup of $J(F_i)$ consisting of ideles which are equal to 1 at all places above $\mathfrak{p}$, and which are units elsewhere. Set $\mathcal{C}_i = J(F_i)/U_i^{(\mathfrak{p})} F_i^*$, and let $W_i = \prod_{\mathfrak{q}|\mathfrak{p}} \mu_{q^i}(F_{i,\mathfrak{q}})$. It is shown in §3.2 of [PR1] that there is an isomorphism

$$\eta_i^{-1} : \Sigma(F)^{(\pi^{*i})} \longrightarrow \frac{\mathrm{Hom}(E_{\pi^i}, \mathcal{C}_i(p))^{\Gamma_1}}{\mathrm{Hom}(E_{\pi^i}, W_i)^{\Gamma_1}} \tag{5.1}$$

where $\mathcal{C}_i(p)$ denotes the p-primary part of $\mathcal{C}_i$ and $\Gamma_1 = \mathrm{Gal}(F_\infty/F)$.

Suppose that $T \in E_{1,\mathfrak{p}}(F) \otimes_{\mathfrak{O}} \mathfrak{O}_{\mathfrak{p}^*}$, and let T_i denote the image of T in $\Sigma(F)^{\pi^{*i}}$ under projection. Then it follows from the construction of η_i given in §3.2 of [PR] that

$$(c(\eta_i^{-1}(T_i)(R))) = \varphi_i^{(e)}(T_i)(R). \tag{5.2}$$

Define

$$\Xi_i : \Sigma(F)^{(\pi^{*i})} \longrightarrow \frac{\mathrm{Hom}(E_{\pi^i}, \mathcal{C}_i(p))^{\Gamma_1}}{\mathrm{Hom}(E_{\pi^i}, W_i)^{\Gamma_1}} \tag{5.3}$$

by $\Xi_i(s)(R) = \eta_i(s)(\pi^{*-i}R)$. For each i, the global Artin map yields a surjection

$$(-, \mathcal{X}_i/F_i) : \mathcal{C}_i(p) \longrightarrow X_i,$$

and this induces a homomorphism

$$\gamma_i : \Sigma(F)^{\pi^{*i}} \longrightarrow \mathrm{Hom}(E_{\pi^{*i}}, X_i)^{\Gamma_1} \tag{5.4}$$

which is defined by $\gamma_i(s) = (-, \mathcal{X}_i/F_i) \circ \Xi_i(s)$.

It is shown in §3.2 of [PR1] that we may take inverse limits of (5.4) to obtain an isomorphism

$$\Phi_F : \Sigma(F) \longrightarrow \mathrm{Hom}(T_\pi, X_\infty)^{\Gamma_1}. \tag{5.5}$$

(The reader should note that our Φ_F is slightly different from the Φ_F of [PR1], because there Ξ_i is defined by $\Xi_i(s)(R) = \Xi_i(s)(R) = \eta_i(s)(\delta^{-1}\pi^{*-i}R)$, where $\delta = [F(E_\mathfrak{p}) : F]$.)

We shall now use the isomorphism Φ_F to construct a pairing

$$\{.,.\}'_{F,\mathfrak{p}} : E(F) \otimes_\mathfrak{O} \mathfrak{O}_\mathfrak{p} \times E_1(F) \otimes_\mathfrak{O} \mathfrak{O}_{\mathfrak{p}^*} \longrightarrow \mathfrak{O}_\mathfrak{p} \tag{5.6}$$

as follows.

Suppose that $S \in E_{1,\mathfrak{p}}(F) \otimes_\mathfrak{O} \mathfrak{O}_{\mathfrak{p}^*}$ and $P \in E(F) \otimes_\mathfrak{O} \mathfrak{O}_\mathfrak{p}$. Let t be a generator of of T_π (as an $\mathfrak{O}_\mathfrak{p}$-module). Set $x_S = \Phi_F(S)(t) \in X_\infty$. For each $j \in \mathbb{N}$, let $P_j \in E(F)$ be such that the image of P_j under the projection $E(F) \to E(F)/\pi^j E(F)$ is equal to the image of P under the projection $E(F) \otimes_\mathfrak{O} \mathfrak{O}_\mathfrak{p} \to E(F)/\pi^j E(F)$. Choose any $P'_j \in E(F^c)$ such that $[\pi^j]P'_j = P_j$. Then the map $\pi^{-j} \mapsto \phi^{-1}(P_j'^{x_S} - P'_j)$ induces an element $\tau \in Hom(D_{\mathfrak{p}}, D_{\mathfrak{p}})$. There is an isomorphism

$$\xi : \mathfrak{O}_{\mathfrak{p}} \longrightarrow \mathrm{Hom}(D_{\mathfrak{p}}, D_{\mathfrak{p}})$$

given by $\xi(a)(\alpha) = a.\alpha$, where $a \in \mathfrak{O}_{\mathfrak{p}}$ and $\alpha \in D_{\mathfrak{p}}$. We set $\{P, S\}'_{F,\mathfrak{p}} = \xi^{-1}(\tau)$.

As $[E(F) : E_1(F)] < \infty$, $\{.,.\}'_{F,\mathfrak{p}}$ may be extended to a pairing

$$\{.,.\}_{F,\mathfrak{p}} : E(F) \otimes_{\mathfrak{O}} \mathfrak{O}_{\mathfrak{p}} \times E(F) \otimes_{\mathfrak{O}} \mathfrak{O}_{\mathfrak{p}^*} \longrightarrow K_{\mathfrak{p}}. \tag{5.7}$$

$\{.,.\}_{F,\mathfrak{p}}$ is the algebraic $\mathfrak{p}$-adic height pairing on E/F and is conjectured to be non-degenerate modulo torsion. One of the main results of [PR1] (p.370; see also Chapter IV, Thèoréme 22 of [PR2]) asserts that if this is the case, and if in addition $|\text{Ш}(F)(\mathfrak{p}^*)| < \infty$, then the $\mathfrak{p}$-adic L-function $\mathcal{L}_{\mathfrak{p}}(E/F, s)$ associated to E/F vanishes to order $\mathrm{rank}_{\mathfrak{O}}(E(F))$ at $s = 1$.

Let

$$\Phi_{\mathcal{M}} : \Sigma(F) \longrightarrow \mathrm{Hom}(T_\pi, H_\infty)^{\Gamma_1} \tag{5.8}$$

be the map obtained by composing Φ_F with the projection $\mathrm{Hom}(T_\pi, X_\infty)^{\Gamma_1} \to \mathrm{Hom}(T_\pi, H_\infty)^{\Gamma_1}$. Write Φ'' for the map obtained by composing $\Psi'_{\mathcal{M}}$ with the natural map $\varprojlim_i \mathrm{Cl}(\mathfrak{O}_{F_i})(p) \to H_\infty$ arising from classfield theory. The link between the Galois structure of phs and the $\mathfrak{p}$-adic height pairing on E/F is given by the following lemma.

LEMMA 5.1. $\mathrm{Ker}(\Phi''|\Sigma(F)) = \mathrm{Ker}(\Phi_{\mathcal{M}})$.

Proof. This follows immediately from the definition of $\Psi'_{\mathcal{M}}$ together with (5.2) and the definition of Φ_F. $\square$

§6. Unramified points

In this section we shall obtain a description of $\mathrm{Ker}\Phi_{\mathcal{M}}$ in terms of the pairing is $\{.,.\}_{F,\mathfrak{p}}$. We begin by introducing some notation. We shall say that two $\mathbb{Z}_p$-modules A, B are pseudo-isomorphic (as $\mathbb{Z}_p$-modules), and write $A \sim B$, if there is a homomorphism $A \to B$ with finite kernel and cokernel. Thus, if A and B are finitely generated, then $A \sim B$ if and only if $\mathrm{rank}_{\mathbb{Z}_p}(A) = \mathrm{rank}_{\mathbb{Z}_p}(B)$; in particular, $A \sim B$ if and only if $B \sim A$.

Let $Z_\infty = \mathrm{Gal}(\mathcal{X}_\infty/\mathcal{H}_\infty)$. Then $\mathrm{Hom}(T_\pi, X_\infty)^{\Gamma_1} = \mathrm{Hom}(T_\pi, X_\infty^{(\chi_\infty)})$, and so $\Phi_{\mathcal{M}}$ is simply the composition of Φ_F with the natural projection

$$\mathrm{Hom}(T_\pi, X_\infty^{(\chi_\infty)}) \to \mathrm{Hom}(T_\pi, (X_\infty/Z_\infty)^{(\chi_\infty)}).$$

The following proposition immediately implies that this projection is in fact surjective up to finite index. I would like to thank Karl Rubin for showing me the proof of this result.

Proposition 6.1. $X_\infty^{(\chi_\infty)}/Z_\infty^{(\chi_\infty)} \sim (X_\infty/Z_\infty)^{(\chi_\infty)}$.

Proof. The exact sequence

$$0 \longrightarrow Z_\infty \longrightarrow X_\infty \longrightarrow X_\infty/Z_\infty \longrightarrow 0 \tag{6.1}$$

yields

$$0 \longrightarrow Z_\infty^{(\chi_\infty)} \longrightarrow X_\infty^{(\chi_\infty)} \longrightarrow (X_\infty/Z_\infty)^{(\chi_\infty)} \tag{6.2}$$

and

$$0 \longrightarrow Z_\infty^{(\varepsilon)} \longrightarrow X_\infty^{(\varepsilon)} \longrightarrow (X_\infty/Z_\infty)^{(\varepsilon)} \tag{6.2)(a}$$

Since Δ is a finite group, we deduce from (6.2)(a) that

$$\mathrm{rank}_{\mathbb{Z}_p}(X_\infty^{(\varepsilon)}) = \mathrm{rank}_{\mathbb{Z}_p}(X_\infty/Z_\infty)^{(\varepsilon)} + \mathrm{rank}_{\mathbb{Z}_p}(Z_\infty^{(\varepsilon)}).$$

We claim that the right-hand arrow of (6.2) is surjective up to finite index. For, if this were not the case, then we would have

$$\mathrm{rank}_{\mathbb{Z}_p}(X_\infty/Z_\infty)^{(\chi_\infty)} + \mathrm{rank}_{\mathbb{Z}_p}(Z_\infty^{(\chi_\infty)}) > \mathrm{rank}_{\mathbb{Z}_p}(X_\infty^{(\chi_\infty)}). \tag{6.3}$$

Now $\mathrm{Hom}(T_\pi, X_\infty^{(\chi_\infty)}) \simeq E_1(F) \otimes_{\mathfrak{O}} \mathfrak{O}_{\mathfrak{p}^*}$ (from (5.5) and Lemma 4.1), and so

$$\mathrm{rank}_{\mathbb{Z}_p}(X_\infty^{(\chi_\infty)}) = \mathrm{rank}_{\mathbb{Z}_p}(E_1(F) \otimes_{\mathfrak{O}} \mathfrak{O}_{\mathfrak{p}^*}) = n_{E/F}, \tag{6.4}$$

say. (Here we have identified $\mathfrak{O}_{\mathfrak{p}^*}$ with $\mathbb{Z}_p$.) Hence we obtain

$$\begin{aligned} \mathrm{rank}_{\mathbb{Z}_p}(X_\infty^{(\varepsilon)}) &= \mathrm{rank}_{\mathbb{Z}_p}(X_\infty/Z_\infty)^{(\varepsilon)} + \mathrm{rank}_{\mathbb{Z}_p}(Z_\infty^{(\varepsilon)}) \\ &\geq \mathrm{rank}_{\mathbb{Z}_p}(X_\infty/Z_\infty)^{(\chi_\infty)} + \mathrm{rank}_{\mathbb{Z}_p}(Z_\infty^{(\chi_\infty)}) \\ &> \mathrm{rank}_{\mathbb{Z}_p}(X_\infty^{(\chi_\infty)}) \\ &= n_{E/F}. \end{aligned}$$

This implies that the $\mathfrak{p}$-adic L-function $\mathcal{L}_{\mathfrak{p}}(E/F, s)$ associated to E/F vanishes to order strictly greater than $n_{E/F}$ at $s = 1$. Since we have assumed that $|\text{Ш}(F)(\mathfrak{p})| < \infty$ and $\{.,.\}_{F,\mathfrak{p}}$ is non-degenerate modulo torsion, this is a contradiction (see [PR1] p.370). $\square$

We now introduce a certain subgroup U of $E(F) \otimes_{\mathfrak{O}} \mathfrak{O}_{\mathfrak{p}}$ which we shall call the group of unramified points of $E(F) \otimes_{\mathfrak{O}} \mathfrak{O}_{\mathfrak{p}}$. Suppose that $P \in E(F) \otimes_{\mathfrak{O}} \mathfrak{O}_{\mathfrak{p}}$, and for each $j \in \mathbb{N}$, choose $P_j \in E(F)$ such that the image of P_j under the projection $E(F) \to E(F)/\pi^j E(F)$ is equal to the image of P under the projection $E(F) \otimes_{\mathfrak{O}} \mathfrak{O}_{\mathfrak{p}} \to E(F)/\pi^j E(F)$. Choose any $P'_j \in E(F^c)$ such that $[\pi^j]P'_j = P_j$. Then we may define a homomorphism

$$h_j : X_\infty^{(\chi_\infty)} \longrightarrow E_{\pi^\infty} \tag{6.5}$$

by $h_j(\omega) = P_j'^{\omega} - P'_j$. We say that P is an *unramified point* if h_j vanishes on $Z_\infty^{(\chi_\infty)}$ for all $j \in \mathbb{N}$.

Proposition 6.3. *The orthogonal complement* $[\Phi_F^{-1}(\mathrm{Hom}(T_\pi, Z_\infty^{(\chi_\infty)})]^\perp$ *of* $\Phi_F^{-1}(\mathrm{Hom}(T_\pi, Z_\infty^{(\chi_\infty)})$ *with respect to the pairing* $\{.,.\}_{F,\mathfrak{p}}$ *is equal to* U.

Proof. It is clear from the definitions that

$$U \subseteq [\Phi_F^{-1}(\mathrm{Hom}(T_\pi, Z_\infty^{(\chi_\infty)})]^\perp.$$

Suppose conversely that $P \in E(F) \otimes_{\mathfrak{O}} \mathfrak{O}_{\mathfrak{p}}$ is orthogonal to all points S which lie in $\Phi_F^{-1}(\mathrm{Hom}(T_\pi, Z_\infty^{(\chi_\infty)}) \subseteq E_1(F) \otimes_{\mathfrak{O}} \mathfrak{O}_{\mathfrak{p}^*}$. Then, (using the notation of §5)

$$P_j'^{x_S} - P'_j = 0 \qquad \forall j \in \mathbb{N}, \quad \forall S \in [\Phi_F^{-1}(\mathrm{Hom}(T_\pi, Z_\infty^{(\chi_\infty)})].$$

Let $\omega \in Z_\infty$. Since Φ_F is an isomorphism, it follows that (again using the notation of §5)

$$x_S = \Phi_F(S)(t) = \omega$$

for some $S \in [\Phi_F^{-1}(\mathrm{Hom}(T_\pi, Z_\infty^{(\chi_\infty)})]$. Thus we deduce that

$$P_j^{'\omega} - P' = 0 \qquad \forall j \in \mathbb{N}, \quad \forall \omega \in Z_\infty^{(\chi_\infty)}.$$

Hence $P \in U$, and this establishes the result. $\square$

Corollary 6.4. *$\mathrm{Ker}(\Psi_{\mathcal{M}}) \sim U^\perp$ and $(\mathrm{Ker}(\Psi_{\mathcal{M}}))^\perp \sim U$.*

Proof. We deduce from Lemmas 3.5, 5.1, and the remarks immediately preceding Proposition 6.1 that $\mathrm{Ker}\Psi_{\mathcal{M}} = [\Phi_F^{-1}(\mathrm{Hom}(T_\pi, Z_\infty^{(\chi_\infty)})]$. The result now follows from Proposition 6.3 together with the fact that $\{.,.\}_{F,\mathfrak{p}}$ is non-degenerate modulo torsion. $\square$

We shall now give another description of the group U up to pseudo-isomorphism. For each prime $\mathfrak{P}$ of F lying above $\mathfrak{p}$, we write $E_1(F_\mathfrak{P})$ for the kernel of reduction of $E(F_\mathfrak{P})$. Then $E_1(F_\mathfrak{P})$ is an $\mathfrak{O}_\mathfrak{p}$-module, and we have a natural homomorphism

$$f_\mathfrak{P} : E_{1,\mathfrak{p}}(F) \otimes_\mathfrak{O} \mathfrak{O}_\mathfrak{p} \longrightarrow E_1(F_\mathfrak{P}) \tag{6.6}$$

which induces

$$f : E_{1,\mathfrak{p}}(F) \otimes_\mathfrak{O} \mathfrak{O}_\mathfrak{p} \longrightarrow \prod_{\mathfrak{P}|\mathfrak{p}} E_1(F_\mathfrak{P}) \qquad (6.7).$$

Proposition 6.5. *$U \sim \mathrm{Ker}(f)$.*

Proof. We shall show that $(U \cap E_1(F) \otimes_\mathfrak{O} \mathfrak{O}_\mathfrak{p}) \sim \mathrm{Ker}(f)$. (This will suffice since $[E(F) \otimes_\mathfrak{O} \mathfrak{O}_\mathfrak{p} : E_1(F) \otimes_\mathfrak{O} \mathfrak{O}_\mathfrak{p}] < \infty$.) Suppose that $P \in E_1(F) \otimes_\mathfrak{O} \mathfrak{O}_\mathfrak{p}$. For each $i \in \mathbb{N}$ and $\mathfrak{P}|\mathfrak{p}$, let $F_{\infty,\mathfrak{P}}(\frac{1}{\pi^i} f_\mathfrak{P}(P))$ be the field obtained by adjoining π^ith roots of $f_\mathfrak{P}(P)$ (taken with respect to the formal group law on E) to $F_{\infty,\mathfrak{P}}$. Then P is unramified if and only if the extension $F_{\infty,\mathfrak{P}}(\frac{1}{\pi^i} f_{\mathfrak{P}}(P))/F_{\infty,\mathfrak{P}}$ is unramified for all $\mathfrak{P}|\mathfrak{p}$ and all $i \in \mathbb{N}$. As we are only concerned with modules up to pseudo-isomorphism, we may assume that either $f_{\mathfrak{P}}(P) = 0$ or that $f_{\mathfrak{P}}(P)$ is of infinite order. However, if $f_{\mathfrak{P}}(P)$ is of infinite order, then $F_{\infty,\mathfrak{P}}(\frac{1}{\pi^i} f_{\mathfrak{P}}(P))/F_{\infty,\mathfrak{P}}$ is non-trivial and ramified for all sufficiently large i (see [CW] Th. 11), and so $f(P) \notin U$. The result follows. $\square$

Let us now give an application of this result. Suppose now that $\mathrm{rank}_{\mathfrak{O}} E(F) = 1$. Then $\mathrm{rank}_{\mathfrak{O}_{\mathfrak{p}}}(\mathrm{Im}(f)) = 1$, and so from Proposition 6.5 implies that the group U is finite. It therefore follows from Corollary 6.4 (together with the non-degeneracy of the pairing $\{.,.\}_{F,\mathfrak{p}}$) that $\mathrm{rank}_{\mathfrak{O}_{\mathfrak{p}^*}}(\mathrm{Ker}(\Psi_{\mathcal{M}})) = 1$, which in turn implies that the image of $\Psi_{\mathcal{M}}$ is finite. Hence we have

THEOREM 6.6. *Suppose that* $\mathrm{rank}_{\mathfrak{O}} E(F) = 1$. *Then* $\mathrm{Im}(\Psi_{\mathcal{M}})$ *is finite, and so if* $Q \in |\mathrm{Im}(\Psi_{\mathcal{M}})|.E(F)$ *is a point of infinite order, then* $\varphi_i(Q) = 0$ *for all* $i \geq 1$. *Hence* $\overline{\mathfrak{C}_Q(i)}$ *is a globally free* $\mathcal{M}_i$*-module for all* $i \geq 1$. $\square$

We remark that Theorem 6.6 does not hold in the analogous situation over global function fields (see [A]).

Let L/F be any finite extension. It is shown in Theorem 2 of [ST] that if $E(F)$ is finite and $P \in E(L)$, then $\mathfrak{C}_P(i; L) \simeq \mathfrak{A}_i(L)$ as $\mathfrak{A}_i(F)$-modules for all i. We have a similar result in our situation if $\mathrm{rank}_{\mathfrak{O}} E(F) = 1$.

THEOREM 6.7. *Suppose that* $\mathrm{rank}_{\mathfrak{O}} E(F) = 1$, *and let* $P \in |\mathrm{Im}(\Psi_{\mathcal{M},F})|.E(L)$. *Then there is an isomorphism*

$$\overline{\mathfrak{C}_P(i; L)(L)} \simeq \mathcal{M}_i(L) \tag{6.8}$$

of $\mathcal{M}_i(F)$-modules for all $i \geq 1$.

Proof. This follows immediately from Theorem 6.6 together with the trace-restriction diagram (1.9). $\square$

§7. Galois action on $\mathrm{Ker}(\boldsymbol{\Psi}_{\mathcal{M}})$

We shall now give a proof of Theorem 0.1. Hence, in this section we assume that K has classnumber 1 and that E is defined over K.

Write $\mathcal{E}_{1,\mathfrak{p}}(F) = \prod_{\mathfrak{P}|\mathfrak{p}} E_1(F_{\mathfrak{P}})$, and recall that we have a natural homomorphism $f : E_1(F) \otimes_{\mathfrak{O}} \mathfrak{O}_{\mathfrak{p}} \to \mathcal{E}_{1,\mathfrak{p}}(F)$. It is clear that f is a Δ-homomorphism. For each character $\chi \in \hat{\Delta}$, set $r_{\chi} = \mathrm{rank}_{\mathfrak{O}_1}(E(F) \otimes_{\mathfrak{O}} \mathfrak{O}_1)^{\chi}$. Suppose that $\chi_1 \in \hat{\Delta}$ with $r_{\chi_1} \geq 1$. Let $\{\chi_1, \ldots, \chi_m\}$ be the set of all characters in $\hat{\Delta}$ lying in the Ω_K-orbit of χ_1. Then $r_{\chi_j} = r_{\chi_1} \geq 1$ for all $1 \leq j \leq m$, and so it follows that $E(F) \cap (\oplus_{j=1}^{m}(E_1(F) \otimes_{\mathfrak{O}} \mathfrak{O}_1)^{\chi_j})$ contains a point Q of infinite order. Since f is a Δ-homomorphism and $f(Q)$ is of infinite order, we deduce that $\prod_{j=1}^{m}(\mathcal{E}_{1,\mathfrak{p}}(F) \otimes_{\mathfrak{O}} \mathfrak{O}_1)^{\chi_j}$ has $\mathfrak{O}_1$-rank at least 1. But this implies that

$$s_{\chi_j} = \mathrm{rank}_{\mathfrak{O}_1}(\mathcal{E}_{1,\mathfrak{p}}(F) \otimes_{\mathfrak{O}} \mathfrak{O}_1)^{\chi_j} \geq 1 \tag{7.1}$$

for all $1 \leq j \leq m$, since $s_{\chi_j} = s_{\chi_1}$ for all such j.

However in fact $s_{\chi} = 1$ for all $\chi \in \hat{\Delta}$. This latter assertion holds because $\mathcal{E}_{1,\mathfrak{p}}(F)$ contains a subgroup of finite index which is isomorphic to $\prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{O}_{F_{\mathfrak{P}}}$ (see e.g. [Si] Chapter VII, Proposition 6.3). It follows from the above remarks that we have shown

$$\begin{aligned}\operatorname{rank}_{\mathfrak{O}_1}(Ker(f)\otimes_{\mathfrak{O}}\mathfrak{O}_1)^{\chi} &= \operatorname{rank}_{\mathfrak{O}_1}(U\otimes_{\mathfrak{O}}\mathfrak{O}_1)^{\chi} \\ &= r_{\chi}-1\end{aligned} \tag{7.2}$$

for all $\chi \in \hat{\Delta}$ with $r_{\chi} \geq 1$.

Now since we have assumed that E is defined over K, it may be shown that the pairing $\{.,.\}_{F,\mathfrak{p}}$ is Ω_K-equivariant. Hence (7.1) implies that if $r_{\chi} \geq 1$, then

$$\operatorname{rank}_{\mathfrak{O}_2}(U^{\perp}\otimes_{\mathfrak{O}}\mathfrak{O}_2)^{\overline{\chi}} = 1. \tag{7.3}$$

But $U^{\perp} \sim \operatorname{Ker}(\Psi_{\mathcal{M}})$ (Corollary 6.4), and now the result follows. $\square$

We remark that the proof of Theorem 0.1 in fact shows that if $\operatorname{rank}_{\mathfrak{O}_2}[(E(F)\otimes_{\mathfrak{O}}\mathfrak{O}_2)^{\chi}] \geq 1$, then $\operatorname{rank}_{\mathfrak{O}_2}[(\operatorname{Ker}(\Psi_{\mathcal{M}})\otimes_{\mathfrak{O}}\mathfrak{O}_2)^{\chi}] = 1$.

Corollary 7.1. *Suppose that* $\operatorname{rank}_{\mathfrak{O}_2}[(E(F)\otimes_{\mathfrak{O}}\mathfrak{O}_2)^{\chi}] = 1$ *for some* $\chi \in \hat{\Delta}$. *Then there is a point* $Q \in E(F)$ *of infinite order with* $\Psi_{\mathcal{M}}(Q) = 0$.

Proof. Let $\{\chi = \chi_1, \dots, \chi_m\}$ be the set of all characters lying in the Ω_K orbit of χ. Then

$$\operatorname{rank}_{\mathfrak{O}_2}[(E(F)\otimes_{\mathfrak{O}}\mathfrak{O}_2)^{\chi_j}] = 1 \qquad 1 \leq j \leq m.$$

Hence $E(F) \cap \oplus_{j=1}^{m}(E(F)\otimes_{\mathfrak{O}}\mathfrak{O}_2)^{\chi_j}$ contains a point of infinite order.

Theorem 0.1 implies that

$$[\oplus_{j=1}^{m}(E(F)\otimes_{\mathfrak{O}}\mathfrak{O}_2)^{\chi_j} : \oplus_{j=1}^{m}(\operatorname{Ker}(\Psi_{\mathcal{M}})\otimes_{\mathfrak{O}}\mathfrak{O}_2)^{\chi_j}] < \infty.$$

Therefore $E(F) \cap \oplus_{j=1}^{m}(\operatorname{Ker}(\Psi_{\mathcal{M}})\otimes_{\mathfrak{O}}\mathfrak{O}_2)^{\chi_j}$ also contains a point of infinite order, which proves the result. $\square$

References

[A] A. Agboola, 'Abelian varieties and Galois module structure in global function fields', preprint.

[AT] A. Agboola, M. J. Taylor, 'Class invariants of Mordell-Weil groups', preprint.

[B] A. Brumer, 'On the units of algebraic number fields', *Mathematika* **14**, 121-124, (1967)

[BT] N. P. Byott, M.J. Taylor, 'Hopf orders and Galois module structure'. In: K. W. Roggenkamp, M. J. Taylor, *Group rings and class groups'*, DMV Seminar Band 18, Birhauser, (1992).

[CN-S] Ph. Cassou-Noguès, A. Srivastav, 'On Taylor's conjecture for Kummer orders', Séminaire de Théorie des Nombres, Bordeaux **2**, (1990), 349-363.

[CN-T] Ph. Cassou-Noguès, M.J. Taylor, *Elliptic functions and rings of integers*, Birkhauser, Boston, (1987).

[Co] J. Coates, 'Infinite descent on elliptic curves with complex multiplication'. In: *Arithmetic and Geometry*, Birkhauser, Progress in Math. **35**, 107-137, (1983).

[CT] J. Coates, M. J. Taylor (eds.), *L-functions and arithmetic: Proceedings of the Durham Symposium, July 1989*, Cambridge University Press, Cambridge, (1991).

[CW] J. Coates, A. Wiles, 'On the conjecture of Birch and Swinnerton-Dyer', *Inv. Math.,* **39**, 223-251, (1977).

[F] A. Fröhlich, *Galois module structure of algebraic integers*, Springer Verlag, New York, (1983).

[G] R. Greenberg, 'Iwasawa theory for p-adic representations'. In: J.Coates et al. (eds) *Algebraic number theory—in honour of K. Iwasawa*, Adv. Studies in Pure Math. **17**, Academic Press, 1989.

[Gr] B. H. Gross, 'Heegner points on $X_0(N)$'. In: E. Rankin (ed.), *Modular forms*, Ellis-Horwood, Chichester, (1984).

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

[PR1] B. Perrin-Riou, 'Déscente infinie et hauteur p-adique sur les courbes elliptiques à multiplication complexe', *Inv. Math.,* **70**, 369-398, (1983).

[PR2] B. Perrin-Riou, 'Arithmétique des courbes elliptiques et théorie d'Iwasawa', *Bull. Soc. Math. de France Suppl.*, Mémoire **17**, (1984).

[R] K. Rubin, 'p-adic L-functions and rational points on elliptic curves with complex multiplication, *Inv. Math.*, **107**, (1992), 323-350.

[Si] J. Silverman, *The arithmetic of elliptic curves*, Springer Verlag, New York, (1986).

[ST] A. Srivastav, M. J. Taylor, 'Elliptic curves with complex multiplication and Galois module structure', *Inv. Math.,* **99**, 165-184, (1990).

[T1] M. J. Taylor, 'Mordell-Weil groups and the Galois module structure of rings of integers', *Ill. J. Math.,* **32**, 428-452, (1988).

[T2] M. J. Taylor, *Classgroups of group rings*, Cambridge University Press, Cambridge, (1984).

[T3] M. J. Taylor, 'Rings of integers of fields obtained by the division of Heegner points', handwritten manuscript.

[T4] M. J. Taylor, 'The Galois module structure of certain arithmetic principal homogeneous spaces', to appear in *J. Algebra*.