ON P-ADIC HEIGHT PAIRINGS AND LOCALLY FREE CLASSGROUPS OF HOPF ORDERS

A. Agboola

Version of April 30th, 1996

Let E be an elliptic curve with complex multiplication by the ring of integers $\mathfrak{O}$ of an imaginary quadratic field K. The purpose of this paper is to describe certain connections between the arithmetic of E on the one hand and the Galois module structure of certain arithmetic principal homogeneous spaces arising from E on the other. The present paper should be regarded as a complement to [AT]: we assume that the reader is equipped with a copy of the latter paper and that he is not averse to referring to it from time to time.

An outline of the contents of this paper is as follows. After setting up a certain amount of notation in §0, we give an account of the algebraic p-adic height pairing on E in §1. The pairing that we describe was first introduced by Bernadette Perrin-Riou (see [PR1], [PR2]). In §2 we describe the class invariant homomorphism. This homomorphism measures information regarding the module structure of certain principal homogeneous spaces of torsion sub-group schemes of E. In the next two sections, we describe what we call the modified classgroup of the Hopf algebra representing a certain torsion subgroup scheme of E, and we explain precisely how this group is related to the height pairing on E (see Theorem 4.2). This gives a

The author was partially supported by an NSF Postdoctoral Research Fellowship while the research described in this paper was carried out.

very direct and explicit link between the Galois module structure of the principal homogeneous spaces that we consider and the infinite descent on E described by Perrin-Riou in [PR1], [PR2]. Theorem 4.2 of the present paper therefore goes some way towards addressing the point raised in the introduction of [AT] concerning the precise nature of the connection between the algebraic p-adic height pairing and the class invariant homomorphism in the present setting. It seems quite likely to us that a similar relationship exists in the more general context of the p-adic height pairings described in [PR3]. It would be of some interest to obtain a better understanding of the relationship between class invariants and p-adic height pairings in general. (See [A3] for some further remarks on this.)

The final two sections of this paper are logically independent of the previous sections, although they involve a similar circle of ideas. Here we develop the bare beginings of an Iwasawa theory of classgroups of Hopf orders, using techniques of Kervaire-Murthy and Ullom (cf. [KM], [U1], [U2]). In particular, we prove an elliptic analogue of a result of Ullom (see Theorem 6.5).

§0. Notation.

We begin by fixing a certain amount of notation that will be in force for the rest of this paper. Let F/K be a finite extension over which E acquires everywhere good reduction. Set $\Delta = \mathrm{Gal}(F/K)$, and assume that all endomorphisms of E are defined over F. If $\alpha \in \mathfrak{O}$ we shall sometimes write $[\alpha]$ for the corresponding endomorphism of E. 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 $p\mathfrak{O} = \mathfrak{p}\mathfrak{p}^*$. 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

$q = \pi\pi^*$.

Let E_{π^n} (resp. $E_{\pi^{*n}}$) denote the subgroup of elements of $E(\mathbb{Q}^c)$ which are killed by π^n (resp. π^{*n}). (We shall also often write G_n (resp. G_n^*) instead of E_{π^n} (resp. $E_{\pi^{*n}}$).) Let

$$w_n : E_{\pi^n} \times E_{\pi^{*n}} \longrightarrow \mu_{q^n} \tag{0.1}$$

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

$$\chi_R^{(n)} = w_n(g, R) \qquad \forall g \in E_{\pi^{*n}} \tag{0.2}$$

This identifies $\hat{G_n}$ with $E_{\pi^{*n}}$. If $\omega \in \Omega_F$ and $\chi \in \hat{G_n}$, then ω acts on χ via $\chi^\omega(g) = \chi(g^{\omega^{-1}})^\omega$. The identification (2) preserves this action since the Weil pairing is Ω_F-equivariant.

For each $R \in E_{\pi^n}$ (resp. $R^* \in E_{\pi^{*n}}$), we let $F[R]$ (resp. $F[R^*]$) denote the field obtained by adjoining the coordinates of R (resp. R^*) to F. We write $F_n = \cup_{R \in E_{\pi^n}} F[R]$ (resp. $F_n^* = \cup_{R \in E_{\pi^{*n}}} F[R]$). Set $F_\infty = \cup_n F_n$ (resp. $F_\infty^* = \cup_n F_n^*$), and write $\Gamma_1 = Gal(F_\infty/F)$. Let N_∞/F be the unique $\mathbb{Z}_p$ extension contained in F_∞/F, and set $\Gamma = Gal(N_\infty/F)$.

§1. The algebraic p-adic height pairing.

In this section we shall describe the algebraic p-adic height pairing on E/F. The reader may refer to §3 of [PR1] or to Chapter IV of [PR2] for full details of the results we use.

We begin by recalling various elementary facts about Selmer groups. 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 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

$$0 \longrightarrow E_1(F) \longrightarrow E(F) \longrightarrow \prod_{\mathfrak{q}|\mathfrak{p}} \tilde{E}(k_{\mathfrak{q}}). \tag{1.1}$$

Let L be any extension of K over which E is defined. The Selmer group $S(L)^{\pi^{*n}}$ is defined to be the kernel of the natural homomorphism

$$\mathrm{H}^1(\Omega_L, E_{\pi^{*n}}) \longrightarrow \prod_{\mathfrak{q}} \mathrm{H}^1(\Omega_{L_{\mathfrak{q}}}, E). \tag{1.2}$$

(Here $L_{\mathfrak{q}}$ denotes the local completion of L at the prime $\mathfrak{q}$ of L.) The Selmer group $S(L)^{\pi^n}$ is defined similarly. We set $S(L) = \varinjlim S(L)^{\pi^n}$, and we write $Y(L)$ for the Pontryagin dual of $S(L)$.

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

$$0 \longrightarrow \Sigma(F)^{\pi^{*n}} \longrightarrow S(F)^{\pi^{*n}} \longrightarrow \prod_{\mathfrak{q}|\mathfrak{p}} \mathrm{H}^1(\Omega_{F_{\mathfrak{q}}}, E_{\pi^{*n}})$$

exact. Set $\Sigma(F) = \varprojlim \Sigma(F)^{\pi^{*n}}$. Then there is a natural injection

$$E_1(F) \otimes_{\mathfrak{O}} \mathfrak{O}_{\mathfrak{p}^*} \to \Sigma(F)$$

afforded by Kummer theory on E.

Let $J(F_n)$ denote the group of ideles of F_n, and write $U_n^{(\mathfrak{p})}$ for the subgroup of $J(F_n)$ consisting of ideles which are equal to 1 at all places above $\mathfrak{p}$ and which are units elsewhere. Set $\mathcal{C}_n = J(F_n)/U_n^{(\mathfrak{p})} F_n^x$, and let $W_n = \prod_{\mathfrak{q}|\mathfrak{p}} \mu_{q^n}(F_{n,\mathfrak{q}})$.

The first step in the construction of the p-adic height pairing is the following result (see Proposition 3.13 of [PR1]).

Proposition 1.1. *There is a natural exact sequence*

$$\mathrm{Hom}(E_{\pi^n}, W_n)^{\Omega_F} \longrightarrow \mathrm{Hom}(E_{\pi^n}, \mathcal{C}_n(p))^{\Omega_F} \xrightarrow{\eta_n} \Sigma(F)^{\pi^{*n}} \longrightarrow 0.$$

(Here $\mathcal{C}_n(p)$ denotes the p-primary part of $\mathcal{C}_n$.)

We refer the reader to [PR1] for a proof of this result. We shall give the definition of the homomorphism η_n in a moment. Before doing so, however, let us first explain how Proposition 1.1 is used to construct the p-adic height pairing.

We first observe that Proposition 1.1 yields an isomorphism

$$\eta_n^{-1} : \Sigma(F)^{\pi^{*n}} \longrightarrow \frac{\mathrm{Hom}(E_{\pi^n}, \mathcal{C}_n(p))^{\Omega_F}}{\mathrm{Hom}(E_{\pi^n}, W_n)^{\Omega_F}}.$$

Define

$$\Xi_n : \Sigma(F)^{\pi^{*n}} \longrightarrow \frac{\mathrm{Hom}(E_{\pi^n}, \mathcal{C}_n(p))^{\Omega_F}}{\mathrm{Hom}(E_{\pi^n}, W_n)^{\Omega_F}}$$

by $\Xi_n(s)(R) = \eta_n^{-1}(\pi^{*-n}R)$. For each n, let $\mathcal{X}_n/F_n$ be the maximal abelian pro-p extension of F_n which is unramified away from primes dividing $\mathfrak{p}$, and set $X_n = \mathrm{Gal}(\mathcal{X}_n/F_n)$, $X_\infty = \varinjlim X_n$. The global Artin map yields a surjection

$$(-, \mathcal{X}_n/F_n) : \mathcal{C}_n(p) \longrightarrow X_n,$$

and this induces a homomorphism

$$\Xi_n' : \Sigma(F)^{(\pi^{*n})} \longrightarrow \mathrm{Hom}(E_{\pi^n}, X_n)^{\Gamma_1} \tag{1.3}$$

which is defined by $\Xi_n' = (-, \mathcal{X}_n/F_n) \circ \Xi_n(s)$.

It is shown in §3.2 of [PR1] that we may take inverse limits of (1.3) to obtain a homorphism

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

(Here T_π denotes the π-adic Tate module of E.) Φ_F is an isomorphism if the weak $\mathfrak{p}$-adic Leopoldt conjecture holds for F.

It is an immediate consequence of a theorem of Coates (see Theorem 12 of [C]) that there is an isomorphism

$$f : \mathrm{Hom}(T_\pi, X_\infty)^{\Gamma_1} \longrightarrow Y(F_\infty)^{\Gamma_1},$$

and it may easily be shown via Pontryagin duality (see [PR1] p. 378-379) that there is a natural homomorphism

$$\alpha_F : Y(F_\infty)^{\Gamma_1} \longrightarrow \mathrm{Hom}(E(F) \otimes \mathfrak{O}_\mathfrak{p}, \mathfrak{O}_\mathfrak{p}).$$

Hence we obtain a pairing

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

given by $\{x, y\} = (\alpha_F \circ f \circ \Phi_F(x))(y)$; this extends to a pairing (which we shall also denote by $\{,\}$)

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

This pairing $\{,\}$ is the algebraic p-adic height pairing on E.

We shall now give a description of the homomorphism η_n.

Suppose that $f \in \mathrm{Hom}(E_{\pi^n}, \mathcal{C}_n(p))^{\Omega_F}$. Let $\bar{f} \in \mathrm{Map}(E_{\pi^n}, J(F_n))$ be a representative of f. Write $d_n : U_n^{(\mathfrak{p})} F_n^x \to F_n^x$ for the natural projection map.

Consider the sequence of homomorphisms

$$\mathrm{Hom}(E_{\pi^n}, \mathcal{C}_n(p))^{\Omega_F} \longrightarrow \mathrm{Ext}^1(E_{\pi^n}, U_n^{(\mathfrak{p})} F_n^x)^{\Omega_F} \xrightarrow{d_n} \mathrm{Ext}^1(E_{\pi^n}, F_n^x)^{\Omega_F}. \qquad (1.4)$$

Let $f_1 \in \mathrm{Ext}^1(E_{\pi^n}, F_n^x)^{\Omega_F}$ denote the image of f under this sequence of homomorphisms. It follows via standard theory (see e.g. [R] p.211) that f_1 is represented by the map

$$(R, S) \longmapsto d_n\left(\frac{\bar{f}(R+S)}{\bar{f}(R)\bar{f}(S)}\right), \qquad R, S \in E_{\pi^n}.$$

Next, consider the exact sequence

$$0 \longrightarrow F_n^x \longrightarrow \bar{F}^x \longrightarrow \bar{F}^x/F_n^x \longrightarrow 0;$$

this gives the Ω_F-equivariant exact sequence

$$\mathrm{Hom}(E_{\pi^n}, \bar{F}^x) \longrightarrow \mathrm{Hom}(E_{\pi^n}, \bar{F}^x/F_n^x) \longrightarrow \mathrm{Ext}^1(E_{\pi^n}, F_n^x) \longrightarrow \mathrm{Ext}^1(E_{\pi^n}, \bar{F}_n^x).$$

Now $\mathrm{Ext}^1(E_{\pi^n}, \bar{F}_n^x) = 0$ since $\bar{F}^x$ is divisible. Hence there exists $\beta \in \mathrm{Hom}(E_{\pi^n}, \bar{F}^x/F_n^x)$ which maps onto $f_1 \in \mathrm{Ext}^1(E_{\pi^n}, F_n^x)$. Any two different choices of β differ by an element of $\mathrm{Hom}(E_{\pi^n}, \bar{F}^x) = \mathrm{Hom}(E_{\pi^n}, \mu_{q^n}) \simeq E_{\pi^{*n}}$. Since f_1 is fixed by Ω_F, it follows that for each $\sigma \in \Omega_F$, we have $\beta^\sigma = h_\sigma \beta$, where $h_\sigma \in \mathrm{Hom}(E_{\pi^n}, \mu_{q^n}) \simeq E_{\pi^{*n}}$. The element $\eta_n(f) \in \mathrm{H}^1(\Omega_F, E_{\pi^n})$ is defined to be the cohomology class represented by the cocycle $\{\sigma \mapsto h_\sigma\}$. It may be easily checked from the description that $\eta_n(f)$ is trivial at all places $\mathfrak{q}$ with $\mathfrak{q}|\mathfrak{p}$. Hence $\eta_n(f) \in \Sigma(F)^{(\pi^{*n})}$, as claimed.

We conclude this section by remarking that it is the homomorphism η_n that lies at the heart of the construction of the p-adic height pairing. In §4, we shall relate η_n to the Galois module structure of principal homogeneous spaces arising from points on E.

§2. The class invariant homomorphism.

The purpose of this section is to recall various facts that we shall require concerning the class invariant homomorphism. For full details, we refer the reader to [A1], [AT], [BT] and [T1].

Let $\mathfrak{B}_n$ denote the $\mathfrak{O}_F$-Hopf algebra which represents the $\mathfrak{O}_F$-group scheme of $[\pi^{*n}]$-torsion on E, and let $\mathfrak{A}_n$ denote the Cartier dual of $\mathfrak{B}_n$. Then $\mathfrak{B}_n$ is an $\mathfrak{O}_F$-order in the algebra $B_n = \mathrm{Map}_{\Omega_F}(G_n, \mathbb{Q}^c)$, and $\mathfrak{A}_n$ is an order in the algebra

$A_n = (F^c G_n)^{\Omega_F}$ (where Ω_F acts upon both G_n and F^c). Let $E_{\pi^n} \backslash \Omega_F$ denote a set of representatives of Ω_F orbits of E_{π^n}. Then the Wedderburn decomposition of A_n is given by

$$A_n = \prod_{R \in E_{\pi^n} \backslash \Omega_F} F[R]$$

(see e.g. [A1] lemma 3.3). It is shown in [T1] that

$$A_n = \{ \sum_{g \in G_n} f(g) g^{-1} | f \in B_n \}$$

and

$$\mathfrak{A}_n = \{ (\pi^*)^{-n} \sum_{g \in G_n} f(g) g^{-1} | f \in \mathfrak{B}_n \}.$$

Let $\mathcal{E}/\mathfrak{O}_F$ denote the Néron model of E/F. The endomorphism π^{*n} of E yields the exact Kummer sequence of commutative group schemes

$$0 \longrightarrow \mathcal{E}_{\pi^{*n}} \longrightarrow \mathcal{E} \xrightarrow{\pi^{*n}} \mathcal{E} \longrightarrow 0.$$

This in turn yields the following exact sequence of flat cohomology:

$$0 \longrightarrow \mathcal{E}_{\pi^{*n}} \longrightarrow \mathcal{E}(\mathfrak{O}_F) \xrightarrow{\pi^{*n}} \mathcal{E}(\mathfrak{O}_F) \longrightarrow \mathrm{H}^1(\mathfrak{O}_F, \mathcal{E}_{\pi^{*n}}).$$

Since $E(F) \simeq \mathcal{E}(\mathfrak{O}_F)$ (via the universal property of the Néron model), we obtain a homomorphism

$$\frac{E(F)}{\pi^{*n} E(F)} \simeq \frac{\mathcal{E}(\mathfrak{O}_F)}{\pi^{*n} \mathcal{E}(\mathfrak{O}_F)} \longrightarrow \mathrm{H}^1(\mathfrak{O}_F, \mathcal{E}_{\pi^{*n}}).$$

Thus each point $Q \in E(F)$ yields an element of $\mathrm{H}^1(\mathfrak{O}_F, \mathcal{E}_{\pi^{*n}})$; this element is represented by an algebra $\mathfrak{C}_Q(n)$ which is a principal homogeneous space of $\mathfrak{B}_n$. It may be shown that $\mathfrak{C}_Q(n)$ is a locally free $\mathfrak{A}_n$-module, and so determines an element $(\mathfrak{C}_Q(n))$ in the locally free classgroup $\mathrm{Cl}(\mathfrak{A}_n)$ of $\mathfrak{A}_n$. Hence we obtain a map

$$\psi_n : E(F) \longrightarrow \mathrm{Cl}(\mathfrak{A}_n)$$

defined by $\psi_n(Q) = (\mathfrak{C}_Q(n))$. It is shown in [T1] that if E/F has everywhere good reduction, then ψ_n is a homomorphism. (For a discussion of ψ_n in terms of the geometry of $\mathcal{E}$, we refer the reader to [A2].)

Let us now make a remark on Galois action. Write $C_Q(n) = \mathfrak{C}_Q(n) \otimes_{\mathfrak{O}_F} F$; then $C_Q(n)$ is a principal homogeneous space of B_n, and so determines an element $s_Q(n) \in \mathrm{H}^1(F, E_{\pi^{*n}})$. In general, $C_Q(n)$ is not stable under the action of G_n. However, $C_Q(n) \otimes F_n/F$ is a Galois algebra with Galois group isomorphic to $\mathrm{Gal}(F_n/F) \ltimes G_n$, where for $g \in G_n$ and $\gamma \in \mathrm{Gal}(F_n/F)$, we have

$$\gamma^{-1} g \gamma = \gamma(g)$$

(i.e. Galois action of γ on G_n). If $c \in C_Q(n) \otimes F^c$ and $\sigma \in \Omega_F$, then it follows from Galois descent (cf. [BT] pages 181-183) that

$$c^{\sigma} = c^{s_Q(n)(\sigma)}.$$

We shall write $\mathrm{PH}(\mathfrak{B}_n)$ (resp. $\mathrm{PH}(B_n)$) for the group of principal homogeneous spaces of $\mathfrak{B}_n$ (resp. B_n), and we let $\mathrm{PH}_{\mathfrak{p}}(\mathfrak{B}_n)$ (resp. $\mathrm{PH}_{\mathfrak{p}}(B_n)$) denote the group of principal homogeneous spaces of $\mathfrak{B}_n$ (resp. B_n) that are locally trivial at all places dividing $\mathfrak{p}$. There are natural injections $\mathrm{PH}(\mathfrak{B}_n) \hookrightarrow \mathrm{PH}(B_n)$ and $\mathrm{PH}_{\mathfrak{p}}(\mathfrak{B}_n) \hookrightarrow \mathrm{PH}_{\mathfrak{p}}(B_n)$.

We now turn our attention to locally free classgroups. Let $J(A_n)$ denote the group of finite ideles of A_n. The theory of classgroups (see e.g. Chapter VI of [CR]) furnishes us with isomorphisms

$$\mathrm{Cl}(\mathfrak{A}_n) \simeq \frac{J(A_n)}{(\prod_{\mathfrak{q}} \mathfrak{A}_{n,\mathfrak{q}}^x).A_n^x} \simeq \frac{\mathrm{Map}(E_{\pi^n}, J(\mathbb{Q}^c))^{\Omega_F}}{\prod_{\mathfrak{q}}(\mathrm{Det}(\mathfrak{A}_{n,\mathfrak{q}}^x)).\,\mathrm{Map}(E_{\pi^n}, (F^c)^x)^{\Omega_F}}. \tag{2.1}$$

This notation may be explained as follows. Suppose that $u \in J(A_n)$. Then u determines a map $\mathrm{Det}(u) \in \mathrm{Map}(E_{\pi^n}, J(\mathbb{Q}^c))^{\Omega_F}$ which is defined by

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

The second isomorphism in (2.1) is induced by the map $u \mapsto \mathrm{Det}(u)$ from $J(A_n)$ to $\mathrm{Map}(E_{\pi^n}, J(\mathbb{Q}^c))^{\Omega_F}$.

We shall now describe the construction of an idele in $J(A_n)$ representing the class $(\mathfrak{C}_Q(n)) \in \mathrm{Cl}(\mathfrak{A}_n)$. Define the resolvend map

$$r : C_Q(n) \longrightarrow (C_Q(n) \otimes F_n)[G_n]$$

by

$$r(c) = \sum_{g \in G_n} c^g g^{-1}.$$

Then r is a homomorphism of A_n-modules (but not of algebras, since it does not preserve multiplication). It is a standard result in Galois theory that $r(c)$ is invertible if and only if $C_Q(n) = c.A_n$.

For each prime $\mathfrak{q}$ of F, choose a local generator $c_{\mathfrak{q}} \in \mathfrak{C}_Q(n)_{\mathfrak{q}}$ such that $\mathfrak{C}_Q(n)_{\mathfrak{q}} = c_{\mathfrak{q}}.\mathfrak{A}_{n,\mathfrak{q}}$, and let $c \in C_Q(n)$ satisfy $C_Q(n) = c.A_n$. Then we have that $r(c) = r(c_{\mathfrak{q}}).u_{\mathfrak{q}}$, with $u_{\mathfrak{q}} \in A_{n,\mathfrak{q}}^x$. The idele $(u_{\mathfrak{q}}) \in J(A_n)$ represents the class $(\mathfrak{C}_Q(n)) \in \mathrm{Cl}(\mathfrak{A}_n)$.

§2. The modified class invariant homomorphism.

In this section we shall describe a map that we call the modified class invariant homomorphism. It is this map that gives the link between the module structure of principal homogeneous spaces and the algebraic p-adic height pairing.

Let $J_{\mathfrak{p}}(\mathfrak{A}_n)$ denote the subgroup of $\prod_{\mathfrak{q}} \mathrm{Det}(\mathfrak{A}_{n,\mathfrak{q}}^x)$ consisting of those elements that are equal to 1 at all places dividing $\mathfrak{p}$. If $\mathfrak{q}$ is a prime of F, we write $G_n(F_{\mathfrak{q}})$ for the subgroup of elements of G_n that are rational over $F_{\mathfrak{q}}$. The modified classgroup $\mathrm{Cl}'(\mathfrak{A}_n)$ of $\mathfrak{A}_n$ is defined as follows:

$$\mathrm{Cl}'(\mathfrak{A}_n) = \frac{J(A_n)}{J_{\mathfrak{p}}(\mathfrak{A}_n).(\prod_{\mathfrak{q}|\mathfrak{p}} G_n(F_{\mathfrak{q}})).A_n^x}.$$

We remark that (unlike $\mathrm{Cl}(\mathfrak{A}_n)$) $\mathrm{Cl}'(\mathfrak{A}_n)$ is an infinite group, and there is a natural surjection

$$e_n : \mathrm{Cl}'(\mathfrak{A}_n) \longrightarrow \mathrm{Cl}(\mathfrak{A}_n).$$

Now suppose that $\mathfrak{C} \in \mathrm{PH}_{\mathfrak{p}}(\mathfrak{B}_n)$, with $C := \mathfrak{C} \otimes F$. For each $\mathfrak{q}|\mathfrak{p}$, there is a natural isomorphism of $F_{\mathfrak{q}}$-algebras and $A_{n,\mathfrak{q}}$-modules

$$i_{\mathfrak{q}} : C_{\mathfrak{q}} \longrightarrow B_{n,\mathfrak{q}};$$

$i_{\mathfrak{q}}$ is only defined up to an element of $\mathrm{Aut}_{F_{\mathfrak{q}}}(B_{n,\mathfrak{q}}) = G_n(F_{\mathfrak{q}})$. There is also an isomorphism

$$j_{n,\mathfrak{q}} : B_{n,\mathfrak{q}} \longrightarrow A_{n,\mathfrak{q}}$$

of $A_{n,\mathfrak{q}}$-modules (but not of algebras) defined by

$$j_{\mathfrak{q}}(f) = \sum_{g \in G_n} f(g).g^{-1}.$$

Suppose that $C = c.A_n$, and set

$$\nu_{n,\mathfrak{q}}(c) = j_{\mathfrak{q}} \circ i_{\mathfrak{q}}(c).$$

Then $\nu_{n,\mathfrak{q}}(c)$ gives a well-defined element of $A_{n,\mathfrak{q}}^x / G_n(F_{\mathfrak{q}}).A_n^x$. We define the modified class invariant homomorphism

$$\psi_n' : \mathrm{PH}_{\mathfrak{p}}(\mathfrak{B}_n) \longrightarrow \mathrm{Cl}'(\mathfrak{A}_n)$$

by explaining how to construct an idele in $J(A_n)$ representing $\psi'_n(\mathfrak{C})$. Suppose that $\mathfrak{C}_{\mathfrak{q}} = c_{\mathfrak{q}}.\mathfrak{A}_{n,\mathfrak{q}}$ for each prime $\mathfrak{q}$ of F. Then $\psi'_n(\mathfrak{C})$ is represented by the idele whose components are given by

$$\begin{cases} r(c).r(c_{\mathfrak{q}})^{-1} & \mathfrak{q} \nmid \mathfrak{p} \\ \nu_{n,\mathfrak{q}}(c) & \mathfrak{q} | \mathfrak{p} \end{cases}$$

It may be easily checked that this gives a well-defined homomorphism independent of the choices of c and $c_{\mathfrak{q}}$. We shall abuse notation and write $\psi'_n(Q)$ for $\psi'_n(\mathfrak{C}_Q(n))$ if $Q \in \Sigma(F)^{(\pi^{*n})}$.

Proposition 3.1. *Suppose that $Q \in \Sigma(F)^{(\pi^{*n})}$. Then $e_n \circ \psi'_n(Q) = \psi_n(Q)$.*

Proof. Choose a generator $c \in C_Q(n)$ such that $C_Q(n) = c.A_n$ and $\mathfrak{C}_Q(n)_{\mathfrak{q}} = c.\mathfrak{A}_{n,\mathfrak{q}}$ for all places $\mathfrak{q}|\mathfrak{p}$. Then $\psi_n(Q)$ is represented by the idele

$$\begin{cases} r(c).r(c_{\mathfrak{q}})^{-1} & \mathfrak{q} \nmid \mathfrak{p} \\ 1 & \mathfrak{q} | \mathfrak{p} \end{cases}$$

Hence the class $(e_n \circ \psi'_n(Q)).\psi_n(Q)^{-1}$. is represented by the idele $(v_{\mathfrak{q}})$ that is equal to $\nu_{n,\mathfrak{q}}(c)$ for $\mathfrak{q}|\mathfrak{p}$ and equal to 1 elsewhere.

Now since $\mathfrak{C}_Q(n)_{\mathfrak{q}} = c.\mathfrak{A}_{n,\mathfrak{q}}$ for all places $\mathfrak{q}|\mathfrak{p}$, it follows that $\nu_{n,\mathfrak{q}}(c)$ is a generator of $\mathfrak{A}_{n,\mathfrak{q}}$ as a module over itself. Hence for each $\mathfrak{q}$ with $\mathfrak{q}|\mathfrak{p}$), we have $\nu_{n,\mathfrak{q}}(c) \in \mathfrak{A}^x_{n,\mathfrak{q}}$, and now the result follows, since the idele $(v_{\mathfrak{q}})$ lies in the denominator of the classgroup. □

Let m be a positive integer. We shall now give the definition of the mth Adams operation $[m]$ on $\mathrm{Cl}'(\mathfrak{A}_n)$. (There is also a similar operation on $\mathrm{Cl}(\mathfrak{A}_n)$ which is defined in an identical manner.)

For any commutative F-algebra S, say, there is a natural map $[m] : S[G_n] \to$

$S[G_n]$ defined by

$$[m]\sum_{g\in G_n} s_g g = \sum_{g\in G_n} s_g g^m.$$

Now suppose that $\alpha \in \mathrm{Cl}'(\mathfrak{A}_n)$ is represented by the idele $(v_\mathfrak{q}) \in J(A_n)$. The mth Adams operation $[m] : \mathrm{Cl}'(\mathfrak{A}_n) \to \mathrm{Cl}'(\mathfrak{A}_n)$ is defined as follows: $[m]\alpha$ is the class represented by the idele $([m]v_\mathfrak{q}) \in J(A_n)$. It may easily be checked that this gives a well-defined operation on $\mathrm{Cl}'(\mathfrak{A}_n)$.

Proposition 3.2. *Suppose that $Q \in \Sigma(F)^{(\pi^{*n})}$. Then $([m]\psi'_n(Q))(\psi'_n(Q))^{-m} = 0$ for all positive integers m.*

Proof. It is shown in Lemma 4.15 and Proposition 7.5 of [AT] that $([m]r(c))(r(c))^{-m} \in A_n^x$ and that $([m]r(c_\mathfrak{q}))(r(c_\mathfrak{q}))^{-m} \in \mathfrak{A}_{n,\mathfrak{q}}^x$. This implies the result. □

§4. The class invariant and the p-adic height.

In this section, we shall describe the link between the homomorphisms ψ'_n of §3 and η_n of §1. We thus obtain a direct relationship between the class invariant of Q on the one hand, and the p-adic height of Q on the other.

We begin by observing that there is a natural homomorphism

$$\xi_n : \mathrm{Cl}'(\mathfrak{A}_n) \longrightarrow \frac{\mathrm{Map}(E_{\pi^n}, \mathcal{C}_n(p))^{\Omega_F}}{\prod_{\mathfrak{q}|\mathfrak{p}} \mathrm{Hom}(E_{\pi^n}, \mu_{q^n}(F_\mathfrak{q}))^{\Omega_F}}$$

defined as follows. Suppose that $\alpha \in \mathrm{Cl}'(\mathfrak{A}_n)$ is represented by the idele $(v_\mathfrak{q})$ of $J(A_n)$. Then $\xi_n(\alpha)$ is represented by the map $R \mapsto (\chi_R(v_\mathfrak{q}))$ of $\mathrm{Map}(E_{\pi^n}, J(F^c))^{\Omega_F}$.

The following result is an immediate consequence of Proposition 3.2.

Proposition 4.1. *Suppose that $Q \in \Sigma(F)^{(\pi^{*n})}$. Then*

$$\xi_n \circ \psi'_n(Q) \in \frac{\mathrm{Hom}(E_{\pi^n}, \mathcal{C}_n(p))^{\Omega_F}}{\prod_{\mathfrak{q}|\mathfrak{p}} \mathrm{Hom}(E_{\pi^n}, \mu_{q^n}(F_\mathfrak{q}))^{\Omega_F}}.$$

We are now able to describe the relationship between ψ'_n and η_n.

Theorem 4.2. *Suppose that $Q \in \Sigma(F)^{(\pi^{*n})}$. Then $\eta_n \circ \xi_n \circ \psi'_n(Q) = Q$.*

Proof. This follows from carefully unwinding the definitions of the homomorphisms involved. We begin by observing that $\xi_n \circ \psi'_n(Q)$ is represented by $\bar{f} \in \mathrm{Map}(E_{\pi^n}, J(F^c))^{\Omega_F}$ defined by

$$\begin{aligned} \bar{f}(R) &= \chi_R(u_{\mathfrak{q}}) \qquad \mathfrak{q} \nmid \mathfrak{p} \\ &= \chi_R(\nu_{n,\mathfrak{q}}(c)) \qquad \mathfrak{q} | \mathfrak{p} \end{aligned}$$

Let $f_1 \in \mathrm{Ext}^1(E_{\pi^n}, F_n^x)^{\Omega_F}$ denote the image of $\xi_n \circ \psi'_n(Q)$ under the sequence of homomorphisms (1.4). Then f_1 is represented by the map

$$(R, S) \longmapsto d_n(\frac{\bar{f}(R+S)}{\bar{f}(R)\bar{f}(S)})$$

i.e.

$$(R, S) \longmapsto \prod_{\mathfrak{q}|\mathfrak{p}} \frac{\chi_{R+S}(\nu_{n,\mathfrak{q}}(c))}{\chi_R(\nu_{n,\mathfrak{q}}(c))\chi_S(\nu_{n,\mathfrak{q}}(c))}.$$

Next we note that since $C_n(Q)$ is a principal homogeneous space of B_n, there is an isomorphism (of algebras and $A_n \otimes F^c$-modules)

$$i' : C_n(Q) \otimes F^c \longrightarrow B_n \otimes F^c.$$

There is also an isomorphism

$$j' : B_n \otimes F^c \longrightarrow A_n \otimes F^c$$

of $A_n \otimes F^c$-modules (but not of algebras) defined by $j'(f) = \sum_{g \in G_n} f(g)g^{-1}$. Set $\nu'_n = j' \circ i'$.

Recall from §1 that there is a natural surjection

$$\mathrm{Hom}(E_{\pi^n}, (F^c)^x/F_n^x) \longrightarrow \mathrm{Ext}^1(E_{\pi^n}, F_n^x).$$

Define $\beta \in \mathrm{Hom}(E_{\pi^n}, (F^c)^x/F_n^x)$ by $\beta(R) = \chi_R(\nu_n'(c)) \pmod{F_n^x}$. Then $\beta \mapsto f_1$ under the above surjection.

The fact that $\eta_n \circ \xi_n \circ \psi_n'(Q) = Q$ now follows from the definition of η_n together with the remarks on Galois action on principal homogeneous spaces in §1. $\square$

§5. Further remarks on classgroups.

The remainder of this paper is devoted to an analysis of a certain piece of $\mathrm{Cl}(\mathfrak{A}_n)$ via the techniques of Ullom and Kervaire-Murty (see [KM], [U1], [U2]). In order to carry out this analysis, we shall require certain results proved in [AT]. We therefore make the following assumptions from now on:

(i) We assume that F/K is abelian, and that F and $K(E_{p^\infty})$ are linearly disjoint over K.

(ii) We assume that the prime $\mathfrak{p}$ is completely split in F/K.

The assumption (i) implies that the Wedderburn decompositions of A_n and B_n are given by

$$A_n \simeq \oplus_{i=0}^n F_i, \quad B_n \simeq \oplus_{i=0}^n F_i^*. \tag{5.1}$$

Let $\{\chi_i\}_{i=0}^n$ denote a sequence of characters of G_n^* such that χ_i has order q^i and $\chi_{i+1}^q = \chi_i$. We assume that the above decomposition of A_n is induced by $\oplus_{i=0}^n \chi_i$.

We shall now describe two different homomorphisms from $\mathrm{Cl}(\mathfrak{A}_n)$ to $\mathrm{Cl}(\mathfrak{A}_{n-1})$. It is most important that the reader keep in mind the distinction between these maps.

Let $\alpha \in \mathrm{Cl}(\mathfrak{A}_n)$, and let $m_n \in J(A_n)$ be a representative of α in (2.1). Then $q_n(\alpha) \in \mathrm{Cl}(\mathfrak{A}_{n-1})$ is defined to be the class represented by the element

$$R \longmapsto \chi_R(m_n), \quad R \in E_{\pi^{n-1}}$$

of $\mathrm{Map}(E_{\pi^{n-1}}, J(\mathbb{Q}^c))^{\Omega_F}$. This gives us a homomorphism ('passage to quotient'; see chapter 1, §4 of [T2])

$$q_n : \mathrm{Cl}(\mathfrak{A}_n) \longrightarrow \mathrm{Cl}(\mathfrak{A}_{n-1}).$$

The other map that we wish to consider is the restriction map on classgroups. Suppose that $\alpha \in \mathrm{Cl}(\mathfrak{A}_n)$ and $m_n \in J(A_n)$ are as above. Then $\mathrm{res}_{n/n-1}(\alpha) \in \mathrm{Cl}(\mathfrak{A}_{n-1})$ is defined to be the class represented by the element

$$R \longmapsto (\mathrm{Ind}_{G_{n-1}}^{G_n} \chi_R)(m_n), \quad R \in E_{\pi^{n-1}}$$

of $\mathrm{Map}(E_{\pi^{n-1}}, J(\mathbb{Q}^c))^{\Omega_F}$. (Here $\mathrm{Ind}_{G_{n-1}}^{G_n} \chi_R$ denotes the character of G_n induced from G_{n-1} by χ_R.) Now a straightforward computation shows that we have

$$\begin{aligned}(\mathrm{Ind}_{G_{n-1}}^{G_n} \chi_R)(m_n) &= \prod_{\{R' \in G_n | [q]R' = R\}} \chi_{R'}(m_n) \\ &= N_{F_n/F_{n-1}}(\chi_{R'})(m_n)\end{aligned}$$

for any choice of $R' \in G_n$ with $[q]R' = R$. Hence a representing map for $\mathrm{res}_{n/n-1}(\alpha) \in \mathrm{Cl}(\mathfrak{A}_{n-1})$ is given by

$$R \longmapsto N_{F_n/F_{n-1}}(\chi_R)(m_n) = \prod_{\{R' \in G_n | [q]R' = R\}} \chi_{R'}(m_n).$$

We shall now focus our attention on certain natural automorphisms of $\mathrm{Cl}(\mathfrak{A}_n)$. Write $\kappa : \Omega_F \to \mathbb{Z}_p^x$ for the character giving the action of Ω_F on the π-adic Tate module T_π of E. Let $\mathrm{Aut}(G_n)$ denote the group of automorphisms of G_n. Then there is a canonical isomorphism $\mathrm{Aut}(G_n) \to \mathrm{Gal}(F_n/F)$ given by $\tau \mapsto \sigma_\tau$. This isomorphism induces an action of $\mathrm{Aut}(G_n)$ on A_n via Galois action on each factor occuring in the Wedderburn decomposition (4.1) of A_n. We now examine this action. Suppose that $m = \sum_g a_g g$ is an element of A_n, and that $R \in E_{\pi^n}$. For each $\tau \in \mathrm{Aut}(G_n)$, we have

$$\begin{aligned}
[\chi_R(m)]^{\sigma_\tau} &= \sum_{g \in G_n} a_g^{\sigma_\tau} w_n(R, g)^{\sigma_\tau} \\
&= \sum_{g \in G_n} a_g^{\sigma_\tau} w_n(R^{\sigma_\tau}, g^{\sigma_\tau}) \\
&= \sum_{g \in G_n} a_g w_n(R^{\sigma_\tau}, g) \\
&= \sum_{g \in G_n} a_g w_n(\kappa(\sigma_\tau)R, g) \\
&= \sum_{g \in G_n} a_g w_n(R, \kappa(\sigma_\tau)g) \\
&= \chi_R([\kappa(\sigma_\tau)]m).
\end{aligned}$$

Now $[\kappa(\sigma_\tau)] : A_n \to A_n$ is a homomorphism of algebras. Hence $\mathrm{Aut}(G_n)$ preserves the denominator of (2.1), whence it follows that $\mathrm{Aut}(G_n)$ acts on $\mathrm{Cl}(\mathfrak{A}_n)$ via its action on A_n. Thus, $\mathrm{Cl}(\mathfrak{A}_n)$ is an $\mathrm{Aut}(G_n)$-module.

We next observe that $\mathrm{Aut}(G_n) \simeq \Delta \times \Gamma_n$, where $|\Delta| = p - 1$, and Γ_n is cyclic of order q^n. Set $\Gamma = \varprojlim \Gamma_n$ (where here the inverse limit is taken with respect to the natural quotient map $\Gamma_n \to \Gamma_{n-1}$). Then $\varprojlim \mathrm{Cl}(\mathfrak{A}_n)$ (inverse limit taken with respect to the restriction maps $\mathrm{res}_{n/n-1}$) carries the structure of a Γ-module in the obvious manner.

Let $\mathrm{Cl}(\mathfrak{A}_n)^{(p)}$ denote the p-primary part of $\mathrm{Cl}(\mathfrak{A}_n)$, and set $\mathcal{Q}(F) = \varprojlim \mathrm{Cl}(\mathfrak{A}_n)^{(p)}$ (where here again the inverse limit is taken with respect to the restriction maps $\mathrm{res}_{n/n-1}$). Then $\mathcal{Q}(F)$ is a $\Lambda := \mathbb{Z}_p[[\Gamma]]$-module.

§6. The kernel group.

Write $\mathcal{M}_n$ for the $\mathfrak{O}_F$-maximal order of A_n. The kernel group $D(\mathfrak{A}_n)$ of $\mathfrak{A}_n$ is defined to be the kernel of the natural homomorphism $\mathrm{Cl}(\mathfrak{A}_n) \to \mathrm{Cl}(\mathcal{M}_n)$. Since

$\mathfrak{A}_{n,\mathfrak{p}} = \mathcal{M}_{n,\mathfrak{q}}$ for $\mathfrak{q} \nmid \mathfrak{p}$ (see Proposition 2.1 of [AT]), it follows from standard theory that

$$D(\mathfrak{A}_n) \simeq \frac{\mathcal{M}_{n,\mathfrak{p}}^x}{\mathfrak{A}_{n,\mathfrak{p}}^x . A_n^x}. \tag{6.1}$$

The following result is proved in §9 (see especially (9.7)) of [AT].

Proposition 6.1. *There is a natural homomorphism*

$$\delta_n : D(\mathfrak{A}_n) \longrightarrow \frac{\mathfrak{O}_{F_{n-1},\mathfrak{p}}^x \bmod \mathfrak{p}}{\mathrm{Im}(\mathfrak{O}_{F_{n-1}}^x)} \tag{6.2}$$

where $\mathrm{Im}(\mathfrak{O}_{F_{n-1}}^x)$ *denotes the image of* $\mathfrak{O}_{F_{n-1}}^x \bmod \mathfrak{p}$. *This homomorphism is defined as follows. Set* $L_n = F_n.F_n^*$*; then via the existence of the Weil pairing, we see that* $\mu_{q^n} \subset L_n$. *Let* $f \in \mathrm{Gal}(L_n/F(\mu_{q^n}))$ *denote the Frobenius automorphism for the primes of* $F(\mu_{q^n})$ *above* $\mathfrak{p}$. *Suppose that* $\alpha \in D(\mathfrak{A}_n)$ *is represented in (6.1) by an element* $m \in \mathcal{M}_{n,\mathfrak{p}}^x$. *Then*

$$\delta_n(\alpha) = N_{F_n/F_{n-1}}(\chi_n(m)).\chi_{n-1}(m)^{-f}\,\mathrm{Im}(\mathfrak{O}_{F_{n-1}}^x) \bmod \mathfrak{p}. \quad \square$$

Now set $V_n = \ker(q_n | D(\mathfrak{A}_n))$. We remark that classes in V_n may be represented by elements $m \in \mathcal{M}_{n,\mathfrak{p}}^x$ satisfying $\chi_i(m) = 1$ for $i < n$. It is easily seen that $\mathrm{res}_{n/n-1}(D(\mathfrak{A}_n)) \subset D(\mathfrak{A}_{n-1})$ and that $\mathrm{res}_{n/n-1}(V_n) \subset V_{n-1}$. In the remainder of this section, we shall determine the structure of $\varprojlim V_n$ (where the inverse limit is taken with respect to the restriction map on classgroups) as a Λ-module. We begin by examining $\varprojlim \mathrm{Ker}(\delta_n | V_n)$.

Lemma 6.3. $\varprojlim \mathrm{Ker}(\delta_n | V_n) = 0$.

Proof. Suppose that $(s_n) \in \varprojlim \mathrm{Ker}(\delta_n | V_n)$. Then each class $s_n \in V_n$ may be represented (via the isomorphism (6.1) by an element $m_n \in \mathcal{M}_{n,\mathfrak{p}}^x$ satisfying $\chi_i(m_n) = 1$ for $i < n$.

Fix n, and choose $M > n$. Suppose that $s_M \in V_M$ is represented by m_M with $\chi_i(m_M) = 1$ for $i < M$. Since $s_n = \mathrm{res}_{M/n}(s_M)$, it follows that there is a representative $m_n(M) \in \mathcal{M}^x_{n,\mathfrak{p}}$ of s_n, say, which is such that $\chi_n(m_n(M)) = N_{F_M/F_n}(\chi_M(m_M))$, and $\chi_i(m_n(M)) = 1$ for $i < n$.

Now $s_M \in \ker(\delta_M)$, and so there is a global unit $u_{M-1} \in \mathfrak{O}^x_{F_{M-1}}$ such that $N_{F_M/F_{M-1}}(\chi_M(m_M)) \equiv u_{M-1} (\mathrm{mod}\, \mathfrak{p})$. This implies that $\chi_n(m_n(M)) = u_n.\gamma_n$, where $u_n \in \mathfrak{O}^x_{F_n}$ is a global unit, and $\gamma_n \in \mathfrak{O}^x_{F_n,\mathfrak{p}}$. The local unit γ_n may be made as $\mathfrak{p}$-adically close to 1 as we please by choosing M to be sufficiently large (as may be seen by an argument very similar to that given in Lemma 3.2 of [U2]). Hence $m_n(M)$ lies in the denominator of the RHS of (6.1) for all sufficiently large M, and so it follows that $s_n = 0$. This establishes the result. $\square$

Hence we deduce that the natural map

$$\delta = \varprojlim \delta_n : \varprojlim V_n \longrightarrow \varprojlim \frac{\mathfrak{O}^x_{F_{n-1},\mathfrak{p}} \bmod \mathfrak{p}}{\mathrm{Im}(\mathfrak{O}^x_{F_{n-1}})}$$

(where the right-hand inverse limit is taken with respect to the norm map) is an injection. We remark that δ is clearly a Γ-homomorphism.

We shall now show that $\delta_n | V_n$ is surjective, whence it follows that δ_n is an isomorphism. This is an immediate consequence of the following lemma.

Lemma 6.4.. *Let $\mathfrak{q}$ be any prime of F lying above $\mathfrak{p}$. Then*

$$(1 + p\mathfrak{O}_{F,\mathfrak{q}})N_{F_{n+1}/F_n}(\mathfrak{O}^x_{F_{n+1},\mathfrak{q}}) = \mathfrak{O}^x_{F_n,\mathfrak{q}}.$$

Proof. The proof is via classfield theory. We begin by observing that $[\mathfrak{O}^x_{F_n,\mathfrak{q}} : N_{F_{n+1}/F_n}(\mathfrak{O}^x_{F_{n+1},\mathfrak{q}})] = p$, since $F_{n+1,\mathfrak{q}}/F_{n,\mathfrak{q}}$ is totally ramified. Now $1 + p\mathfrak{O}_{F,\mathfrak{q}}$ is topologically generated by $1+p$, and so to prove our result it suffices to show that the Artin symbol $(1+p, F_{n+1,\mathfrak{q}}/F_{n,\mathfrak{q}})$ is non-trivial.

We have the following sequence of maps:

$$\mathfrak{O}^{x}_{F,\mathfrak{q}} \xrightarrow{\text{Artin}} \mathrm{Gal}(F_{n+1,\mathfrak{q}}/F_{\mathfrak{q}}) \xrightarrow{\text{transfer}} \mathrm{Gal}(F_{n+1,\mathfrak{q}}/F_{n,\mathfrak{q}}).$$

Under this sequence of maps, $1+p\mathfrak{O}_{F,\mathfrak{q}}$ maps surjectively onto the p-Sylow subgroup of $\mathrm{Gal}(F_{n+1,\mathfrak{q}}/F_{n,\mathfrak{q}})$ since $[\mathfrak{O}^{x}_{F,\mathfrak{q}} : 1+p\mathfrak{O}_{F,\mathfrak{q}}]$ is of order prime to p. The result now follows from the fact that $\mathrm{Gal}(F_{n+1,\mathfrak{q}}/F_{n,\mathfrak{q}})$ is a p-group. □

Thus, we have now shown that

$$\varprojlim V_n \simeq \varprojlim \frac{\mathfrak{O}^{x}_{F_{n-1},\mathfrak{p}} \bmod \mathfrak{p}}{\mathrm{Im}(\mathfrak{O}^{x}_{F_{n-1}})},$$

where the left-hand inverse limit is taken with respect to the restriction map on classgroups and the right-hand inverse limit is taken with respect to the norm map.

Now let $\mathcal{H}_\infty$ (resp. $\mathcal{X}_\infty$) be the maximal abelian pro-p extension of F_∞ which is everywhere unramified (resp. unramified away from $\mathfrak{p}$), and set $Y_\infty = \mathrm{Gal}(\mathcal{X}_\infty/\mathcal{H}_\infty)$. It follows from classfield theory (cf. the argument given in §3 of [U2]) that

$$\varprojlim \frac{\mathfrak{O}^{x}_{F_{n-1},\mathfrak{p}} \bmod \mathfrak{p}}{\mathrm{Im}(\mathfrak{O}^{x}_{F_{n-1}})} \simeq Y_\infty$$

as Γ-modules. The following result, which may be regarded as an elliptic analogue of Theorem 3.6(a) of [U2], is now immediate.

Theorem 6.5. *There is a canonical isomorphism of Λ-modules*

$$\varprojlim V_n \simeq Y_\infty. \quad \square$$

References

[**A1**] A. Agboola, *Iwasawa theory of elliptic curves and Galois module structure*, Duke Math. J. **71** (1993), 441-462.

[**A2**] A. Agboola, *A geometric description of the class invariant homomorphism*, Journal des Théorie des Nombres de Bordeaux **6** (1994), 273-280.

[**A3**] A. Agboola, *p-adic representations and Galois module structure*, in preparation.

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

[**BT**] N. P. Byott, M. J. Taylor, *Hopf orders and Galois module structure*, In: Group rings and classgroups, K. W. Roggenkamp, M. J. Taylor (eds.), Birkhauser, 1992.

[**C**] J. Coates, *Infinite descent on elliptic curves with complex multiplication*, In: Arithmetic Geometry, Progr. Math, vol. 35, 1983, pp. 107-137.

[**KM**] M. A. Kervaire, M. P. Murthy, *On the projective class group of cyclic groups of prime power order*, Comment. Math. Helvetici **52** (1977), 415-452.

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

[**PR2**] B. Perrin-Riou, *Arithmétique des courbes elliptiques et théorie d'Iwasawa*, Mém. Soc. Math. France (N.S.) **112** (1984), no. 17.

[**PR3**] B. Perrin-Riou, *Théorie d'Iwasawa et hauteurs p-adiques*, Invent. Math **109** (1992), 137-185.

[**R**] J. J. Rotman, *An introduction to homological algebra*, Academic Press, 1979.

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

[**T2**] M. J. Taylor, *Classgroups of group rings*, CUP, 1984.

[**U1**] S. V. Ullom, *Fine structure of class groups of cyclic p-groups*, J. Algebra **49** (1977), 112-124.

[**U2**] S. V. Ullom, *Class groups of cyclotomic fields and group rings*, J. London Math. Soc. **17** (1978), 231-239.

School of Mathematics, Institute for Advanced Study, Princeton, NJ 08540, USA. (Address from September 1, 1996: Department of Mathematics, University of California, Santa Barbara, CA 93106, USA. Email: agboola@math.ucsb.edu)

E-mail address: agboola@math.ias.edu