On $p$-adic height pairings and locally free classgroups of Hopf orders

By A. AGBOOLA†

Department of Mathematics, University of California, Santa Barbara, CA 93106, USA
e-mail: agboola@math.ucsb.edu

(Received 7 May 1996)

Let $E$ be an elliptic curve with complex multiplication by the ring of integers $\mathcal{O}$ 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 Section 0, we give an account of the algebraic $p$-adic height pairing on $E$ in Section 1. The pairing that we describe was first introduced by Bernadette Perrin-Riou (see [PR1], [PR2]). In Section 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 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 beginnings 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 6.4).

† The author was partially supported by an NSF Postdoctoral Research Fellowship while the research described in this paper was carried out.
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 \( \Delta = \text{Gal}(F/K) \), and assume that all endomorphisms of \( E \) are defined over \( F \). If \( \alpha \in \mathcal{O} \) 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 \( \Omega_L = \text{Gal}(L^c/L) \).

Let \( p \) be an odd rational prime which splits in \( \mathcal{O} \) with \( p\mathcal{O} = pp^* \). Choose \( \pi \in p \) with \( \pi^h = \pi \mathcal{O} \) for some \( h \geq 1 \), and write \( \pi^* \) for the complex conjugate of \( \pi \). Set \( q = \pi \pi^* \).

Let \( \mathcal{E}_n \) (resp. \( \mathcal{E}_n^* \)) denote the subgroup of elements of \( E(\mathbb{Q}_p) \) which are killed by \( \pi^n \) (resp. \( \pi^{*n} \)). (We shall also often write \( G_n \) (resp. \( G_n^* \)) instead of \( \mathcal{E}_n \) (resp. \( \mathcal{E}_n^* \)).) Let
\[
\omega: \mathcal{E}_n \times \mathcal{E}_n^* \longrightarrow \mu_q \tag{0.1}
\]
denote the Weil pairing on \( E \). For each \( R \in \mathcal{E}_n \), we define a character \( \chi(n) \in \hat{G}_n \) by
\[
\chi(n) = \omega_n(g, R) \quad \forall g \in \mathcal{E}_n^* \tag{0.2}
\]
This identifies \( \hat{G}_n \) with \( \mathcal{E}_n^* \). If \( \omega \in \Omega_F \) and \( \chi \in \hat{G}_n \), then \( \omega \) acts on \( \chi \) via \( \chi(g) = \chi(g^{(g^{-1})})^{\omega} \). The identification (2) preserves this action since the Weil pairing is \( \Omega \)-equivariant.

For each \( R \in \mathcal{E}_n \) (resp. \( R^* \in \mathcal{E}_n^* \)), we let \( F[R] \) (resp. \( F[R^*] \)) denote the field obtained by adjoining the coordinates of \( R \) (resp. \( R^* \)) to \( F \). We write \( \mathcal{F}_n = \bigcup_{R \in \mathcal{E}_n} F[R] \) (resp. \( \mathcal{F}_n^* = \bigcup_{R \in \mathcal{E}_n^*} F[R] \)). Set \( F_\infty = \bigcup \mathcal{F}_n \) (resp. \( F_\infty^* = \bigcup \mathcal{F}_n^* \)), and write \( \Gamma_1 = \text{Gal}(F_\infty/F) \). Let \( N_\infty/F \) be the unique \( \mathbb{Z}_p \) extension contained in \( F_\infty/F \), and set \( \Gamma = \text{Gal}(N_\infty/F) \).

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 section 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 \( q \) is a prime of \( F \), we write \( k_q \) for the residue field of \( F \) at \( q \), and we let \( \tilde{E}(k_q) \) denote the reduction of \( E \) at \( q \). Write \( E_{1,q}(F) \) for the kernel of reduction of \( E(F) \) at \( q \), and define \( E_{1,p}(F) = E_{1}(F) \) via exactness of the sequence
\[
0 \longrightarrow E_{1}(F) \longrightarrow E(F) \longrightarrow \prod_{q \mid p} \tilde{E}(k_q). \tag{1.1}
\]

Let \( L \) be any extension of \( K \) over which \( E \) is defined. The Selmer group \( S(L)_{\pi, \infty} \) is defined to be the kernel of the natural homomorphism
\[
H^1(\Omega_{L}, E_{\pi, \infty}) \longrightarrow \prod_{q} H^1(\Omega_{L_q}, E). \tag{1.2}
\]
(Here \( L_q \) denotes the local completion of \( L \) at the prime \( q \) of \( L \).) The Selmer group \( S(L)_{\pi, \infty} \) is defined similarly. We set \( S(L) = \lim_{q} S(L)_{\pi, q} \), 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
\[ 0 \rightarrow \Sigma(F)^{\pi^n} \rightarrow S(F)^{\pi^n} \rightarrow \prod_{q \mid p} H^1(\Omega_{F_q}, E_{\pi^n}) \]
eat. Set $\Sigma(F) = \lim_{\leftarrow} \Sigma(F)^{\pi^n}$. Then there is a natural injection
\[ E_1(F) \otimes \mathbb{C} \rightarrow \Sigma(F) \]
afforded by Kummer theory on $E$.

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

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
\[ \text{Hom}(E_{\pi^n}, W_n)^{\mathbb{Q}_p} \rightarrow \text{Hom}(E_{\pi^n}, \mathcal{C}_n(p))^{\mathbb{Q}_p} \rightarrow \Sigma(F)^{\pi^n} \rightarrow 0. \]
(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 $\eta_n$ in a moment. Before doing so, however, we 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
\[ \eta_n^{-1}: \Sigma(F)^{\pi^n} \rightarrow \text{Hom}(E_{\pi^n}, \mathcal{C}_n(p))^{\mathbb{Q}_p} / \text{Hom}(E_{\pi^n}, W_n)^{\mathbb{Q}_p}. \]

Define
\[ \Xi_n: \Sigma(F)^{\pi^n} \rightarrow \text{Hom}(E_{\pi^n}, \mathcal{C}_n(p))^{\mathbb{Q}_p} / \text{Hom}(E_{\pi^n}, W_n)^{\mathbb{Q}_p} \]
by $\Xi_n(s)(R) = \eta_n^{-1}(\pi^{\sim-n} R)$. For each $n$, let $\mathcal{A}_n/F_n$ be the maximal abelian pro-$p$ extension of $F_n$ which is unramified away from primes dividing $p$, and set $X_n = \text{Gal}(\mathcal{A}_n/F_n)$. $X_{\infty} = \text{lim}_{\leftarrow} X_n$. The global Artin map yields a surjection
\[ (-, \mathcal{A}_n/F_n): \mathcal{C}_n(p) \rightarrow X_n, \]
and this induces a homomorphism
\[ \Xi^\prime: \Sigma(F)^{\pi^n} \rightarrow \text{Hom}(E_{\pi^n}, X_n)^{\mathbb{Q}_p} \]
which is defined by $\Xi^\prime_n = (-, \mathcal{A}_n/F_n) \circ \Xi_n(s)$.

It is shown in Section 3-2 of [PR1] that we may take inverse limits of (1.3) to obtain a homorphism
\[ \Phi_F: \Sigma(F) \rightarrow \text{Hom}(T_{\pi}, X_{\infty})^{\mathbb{Q}_p}. \]
(Here $T_{\pi}$ denotes the $\pi$-adic Tate module of $E$.) $\Phi_F$ is an isomorphism if the weak $p$-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
\[ f: \text{Hom}(T_{\pi}, X_{\infty})^{\mathbb{Q}_p} \rightarrow Y(F_{\infty})^{\mathbb{Q}_p}, \]
and it may easily be shown via Pontryagin duality (see [PR1], pp. 378–379) that there is a natural homomorphism

$$\alpha_F: Y(F_{\infty})^f \longrightarrow \text{Hom}(E(F) \otimes \mathcal{C}_p, \mathcal{C}_p).$$

Hence we obtain a pairing

$$\{.,.: E_1(F) \otimes \mathcal{C}_p^r \times E_1(F) \otimes \mathcal{C}_p \longrightarrow \mathcal{C}_p$$
given by \(\{x, y\} = (\alpha_F \circ f \circ \Phi_F(x))(y)\); this extends to a pairing (which we shall also denote by \(\{.,.\}\))

$$\{.,.: E(F) \otimes \mathcal{C}_p^r \times E(F) \otimes \mathcal{C}_p \longrightarrow \mathcal{C}_p.$$  

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

We shall now give a description of the homomorphism \(\eta_n\).

Suppose that \(f \in \text{Hom}(E_{n}^{\pi}, \mathcal{C}_n(p))^{Op}.\) Let \(f \in \text{Map}(E_{n}^{\pi}, J(F_n))\) be a representative of \(f\). Write \(d_n: U_n^{(p)} F_n^{\pi} \longrightarrow F_n^{\pi}\) for the natural projection map.

Consider the sequence of homomorphisms

$$\text{Hom}(E_{n}^{\pi}, \mathcal{C}_n(p))^{Op} \longrightarrow \text{Ext}^1(E_{n}^{\pi}, U_n^{(p)} F_n^{\pi})^{Op} \longrightarrow \text{Ext}^1(E_{n}^{\pi}, F_n^{\pi})^{Op}.$$  

(1-4)

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

\[
(R, S) \longmapsto d_n \left( \frac{f(R + S)}{f(R) f(S)} \right), \quad R, S \in E_{n}^{\pi}.
\]

Next, consider the exact sequence

$$0 \longrightarrow F_n^{\pi} \longrightarrow F^{\pi} \longrightarrow F^{\pi}/F_n^{\pi} \longrightarrow 0;$$

this gives the \(\Omega_{F}\)-equivariant exact sequence

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

Now \(\text{Ext}^1(E_{n}^{\pi}, F^{\pi}) = 0\) since \(F^{\pi}\) is divisible. Hence there exists \(\beta \in \text{Hom}(E_{n}^{\pi}, F^{\pi}/F_n^{\pi})\) which maps onto \(f_1 \in \text{Ext}^1(E_{n}^{\pi}, F_n^{\pi})\). Any two different choices of \(\beta\) differ by an element of \(\text{Hom}(E_{n}^{\pi}, F^{\pi}) = \text{Hom}(E_{n}^{\pi}, \mu_{q^n}) \simeq E_{n}^{\pi}.\) Hence \(f_1\) is fixed by \(\Omega_{F}\), it follows that for each \(\sigma \in \Omega_{F}\), we have \(\beta^\sigma = h_\sigma \beta\), where \(h_\sigma \in \text{Hom}(E_{n}^{\pi}, \mu_{q^n}) \simeq E_{n}^{\pi}.\) The element \(\eta_n(f) \in H^1(\Omega_{F}, E_{n}^{\pi})\) 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 \(q\) with \(q \nmid p.\) Hence \(\eta_n(f) \in \Sigma(F)^{(q^n)}\), as claimed.

We conclude this section by remarking that it is the homomorphism \(\eta_n\) that lies at the heart of the construction of the \(p\)-adic height pairing. In Section 4, we shall relate \(\eta_n\) 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 $\mathcal{B}_n$ denote the $\mathcal{O}_F$-Hopf algebra which represents the $\mathcal{O}_F$-group scheme of $[\pi^n]$-torsion on $E$, and let $\mathcal{U}_n$ denote the Cartier dual of $\mathcal{B}_n$. Then $\mathcal{B}_n$ is an $\mathcal{O}_F$-order in the algebra $B_n = \text{Map}_{\mathcal{B}_F}(G_n, \mathcal{O}_F')$, and $\mathcal{U}_n$ is an order in the algebra $A_n = (F^eG_n)^{\Omega_F}$ (where $\Omega_F$ acts upon both $G_n$ and $F^e$). Let $E^{\pi^n}/\Omega_F$ denote a set of representatives of $\Omega_F$ orbits of $E_{\pi^n}$. Then the Wedderburn decomposition of $A_n$ is given by

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

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

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

and

$$\mathcal{U}_n = \left\{ (\pi^n)^{-n} \sum_{g \in G_n} f(g)g^{-1} | f \in \mathcal{B}_n \right\}.$$

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

$$0 \longrightarrow \mathcal{E}/\pi^n \longrightarrow \mathcal{E} \cdot \pi^n \longrightarrow \mathcal{E} \longrightarrow 0.$$ 

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

$$0 \longrightarrow \mathcal{E}/\pi^n \longrightarrow \mathcal{E}(\mathcal{O}_F) \cdot \pi^n \longrightarrow \mathcal{E}(\mathcal{O}_F) \longrightarrow H^1(\mathcal{O}_F, \mathcal{E}/\pi^n).$$

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

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

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

$$\psi_n : E(F) \longrightarrow \text{Cl}(\mathcal{U}_n)$$

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

Let us now make a remark on Galois action. Write $C_Q(n) = \mathcal{C}_Q(n) \otimes_{\mathcal{O}_F} F$; then $C_Q(n)$ is a principal homogeneous space of $B_n$, and so determines an element $s_Q(n) \in H^1(F, E_{\pi^n})$. 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 $\text{Gal}(F_n/F) \ltimes G_n$, where for $g \in G_n$ and $\gamma \in \text{Gal}(F_n/F)$, we have

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

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

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

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

\[
\text{Cl}(\mathfrak{B}_n) \cong \frac{J(A_n)}{\prod_q \mathfrak{B}_{n,q} \cap A_n^2} \cong \frac{\text{Map}(E_{\mathbb{Q}^n}, J(\mathbb{Q}^n))^{\Omega_p}}{\prod_q (\text{Det}(\mathfrak{B}_{n,q})) \text{Map}(E_{\mathbb{Q}^n}, (F_{c,q})^{\Omega_p})}.
\]  

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

\[
\text{Det}(u)(R) = \chi_R(u_{A_n}).
\]

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

We shall now describe the construction of an idele in \( J(A_n) \) representing the class \( (\mathfrak{C}_Q(n)) \in \text{Cl}(\mathfrak{B}_n) \). Define the resolvent 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 \( q \) of \( F \), choose a local generator \( c_q \in \mathfrak{C}_Q(n)_{\mathfrak{p}} \) such that \( \mathfrak{C}_Q(n)_{\mathfrak{p}} = c_q \mathfrak{B}_{n,\mathfrak{p}} \), and let \( c \in C_Q(n) \) satisfy \( C_Q(n) = c A_n \). Then we have that \( r(c) = r(c_q) u_q \), with \( u_q \in A_{n,\mathfrak{p}}^c \). The idele \( (u_q) \in J(A_n) \) represents the class \( (\mathfrak{C}_Q(n)) \in \text{Cl}(\mathfrak{B}_n) \).

3. 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 \( J_p(\mathfrak{B}_n) \) denote the subgroup of \( \prod_q \text{Det}(\mathfrak{B}_{n,q}) \) consisting of those elements that are equal to 1 at all places dividing \( p \). If \( q \) is a prime of \( F \), we write \( G_n(F_q) \) for the subgroup of elements of \( G_n \) that are rational over \( F_q \). The modified class group \( \text{Cl}'(\mathfrak{B}_n) \) of \( \mathfrak{B}_n \) is defined as follows:

\[
\text{Cl}'(\mathfrak{B}_n) = \frac{J(A_n)}{J_p(\mathfrak{B}_n)(\prod_{q \mid p} G_n(F_q)) A_n^2}.
\]

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

\[
e_n: \text{Cl}'(\mathfrak{B}_n) \longrightarrow \text{Cl}(\mathfrak{B}_n).
\]

Now suppose that \( C \in \text{PH}_p(\mathfrak{B}_n) \), with \( C := \mathfrak{C} \otimes F \). For each \( q \mid p \), there is a natural
On p-adic height pairings

isomorphism of $F_q$-algebras and $A_{n,q}$-modules

$$i_q: C_q \longrightarrow B_{n,q};$$

$i_q$ is only defined up to an element of $\text{Aut}_{F_q}(B_{n,q}) = G_n(F_q)$. There is also an isomorphism

$$j_{n,q}: B_{n,q} \longrightarrow A_{n,q}$$
of $A_{n,q}$-modules (but not of algebras) defined by

$$j_q(f) = \sum_{g \in G_n} f(g) g^{-1}.$$Suppose that $C = c A_n$, and set

$$\nu_{n,q}(c) = j_q \circ i_q(c).$$Then $\nu_{n,q}(c)$ gives a well-defined element of $A_{n,q}^e / G_n(F_q) A_{n,q}^e$. We define the modified class invariant homomorphism

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

$$\nu_{n,q}(c) = j_q \circ i_q(c).$$It may be easily checked that this gives a well-defined homomorphism independent of the choices of $c$ and $c_q$. We shall abuse notation and write $\psi'_n(Q)$ for $\psi'_n(\mathfrak{C}_Q(n))$ if $Q \in \Sigma(F)^{\pi^m}$. Proposition 3.1. Suppose that $Q \in \Sigma(F)^{\pi^m}$. 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 $\mathfrak{C}_Q(n)_q = c \mathfrak{A}_{n,q}$ for all places $q \mid p$. Then $\psi_n(Q)$ is represented by the idele

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

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

Let $m$ be a positive integer. We shall now give the definition of the $m$th Adams operation $[m]$ on $\text{Cl}(\mathfrak{A}_n)$. (There is also a similar operation on $\text{Cl}(\mathfrak{A}_n)$ which is defined in an identical manner.) For any commutative $F$-algebra $S$, say, there is a natural map $[m]: S[G_n] \rightarrow S[G_n]$ defined by

$$[m] \sum_{g \in G_n} s_g g = \sum_{g \in G_n} s_g g^m.$$
Now suppose that $\alpha \in \text{Cl}^i(\mathfrak{A}_n)$ is represented by the idele $(v_q) \in J(A_n)$. The $m$th Adams operation $[m] : \text{Cl}^i(\mathfrak{A}_n) \to \text{Cl}^i(\mathfrak{A}_n)$ is defined as follows: $[m]\alpha$ is the class represented by the idele $([m]v_q) \in J(A_n)$. It may easily be checked that this gives a well-defined operation on $\text{Cl}^i(\mathfrak{A}_n)$.

**Proposition 3.2.** Suppose that $Q \in \Sigma(F)^{(\pi^m)}$. 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 $(|m|r(c))(r(c))^{-m} \in A_n^\pi$ and that $(|m|r(c))(r(c))^{-m} \in \mathfrak{A}_{n,a}$. This implies the result.

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

In this section, we shall describe the link between the homomorphisms $\psi'_n$ of Section 3 and $\eta_n$ of Section 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

$$\xi_n : \text{Cl}^i(\mathfrak{A}_n) \to \prod_{q \in p} \text{Hom}(E_{\pi^n,n}(p),\mu_{q^p}(F_q))^\Omega.$$ 

defined as follows. Suppose that $\alpha \in \text{Cl}^i(\mathfrak{A}_n)$ is represented by the idele $(v_q)$ of $J(A_n)$. Then $\xi_n(\alpha)$ is represented by the map $R \mapsto (\chi_R(v_q))$ of $\text{Map}(E_{\pi^n,n}, J(F^n))^\Omega$.

The following result is an immediate consequence of Proposition 3.2.

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

$$\xi_n \circ \psi'_n(Q) \in \prod_{q \in p} \text{Hom}(E_{\pi^n,n}(p),\mu_{q^p}(F_q))^\Omega.$$

We are now able to describe the relationship between $\psi'_n$ and $\eta_n$.

**Theorem 4.2.** Suppose that $Q \in \Sigma(F)^{(\pi^m)}$. 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 $f \in \text{Map}(E_{\pi^n,n}, J(F^n))^\Omega$ defined by

$$f(R) = \chi_R(v_q) \quad q \nmid p$$

$$= \chi_R(\nu_i(a)(c)) \quad q | p.$$

Let $f_1 \in \text{Ext}^1(E_{\pi^n,n}, F_n^\pi)^\Omega$ 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

$$(R,S) \mapsto d_n\left(\frac{f(R+S)}{f(R)f(S)}\right)$$

i.e.

$$(R,S) \mapsto \prod_{q | p} \frac{\chi_{R+S}(\nu_i(a)(c))}{\chi_R(\nu_i(a)(c))\chi_S(\nu_i(a)(c))}.$$ 

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

$$i' : C_n(Q) \otimes F^e \to B_n \otimes F^e.$$
There is also an isomorphism

$$j': B_0 \otimes F^c \to A_0 \otimes F^c$$

of \( A_0 \otimes F^c \)-modules (but not of algebras) defined by \( j'(f) = \sum_{g \in G_0} f(g) g^{-1} \). Set \( \nu' = j' \circ i' \).

Recall from Section 1 that there is a natural surjection

$$\text{Hom}(E_{\pi^\infty}, (F^c)^\pi / F^c) \to \text{Ext}^1(E_{\pi^\infty}, F^c).$$

Define \( \beta \in \text{Hom}(E_{\pi^\infty}, (F^c)^\pi / F^c) \) by \( \beta(R) = \chi_R(\nu'_n(c)) \mod F^c_n \). 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 \( \eta_n \) together with the remarks on Galois action on principal homogeneous spaces in Section 1.

5. Further remarks on classgroups

The remainder of this paper is devoted to an analysis of a certain piece of \( \text{Cl}(\mathfrak{K}_n) \) 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 assume from now on:

(i) that \( F / K \) is abelian, and that \( F \) and \( K(E_{\pi^\infty}) \) are linearly disjoint over \( K \);

(ii) that the prime \( p \) is completely split in \( F/K \).

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

$$A_n \cong \bigoplus_{i=0}^n F_i, \quad B_n \cong \bigoplus_{i=0}^n F_i^*.$$  \hspace{1cm} (5.1)

Let \( \{ \chi_i \}_{i=0}^n \) denote a sequence of characters of \( G_n \) such that \( \chi_i \) has order \( q_i^j \) and \( \chi_{i+1} = \chi_i \). We assume that the above decomposition of \( A_n \) is induced by \( \bigoplus_{i=0}^n \chi_i \).

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

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

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

of \( \text{Map}(E_{\pi^{n-1}}, J(Q^c)^{2p}). \) This gives us a homomorphism (‘passage to quotient’; see chapter 1, section 4 of [T2])

$$q_n : \text{Cl}(\mathfrak{K}_n) \to \text{Cl}(\mathfrak{K}_{n-1}).$$

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

$$R \mapsto (\text{Ind}_{G_{n-1}^0}^{G_n^0} \chi_R)(m_n), \quad R \in E_{\pi^{n-1}}$$

of \( \text{Map}(E_{\pi^{n-1}}, J(Q^c)^{2p}). \) (Here \( \text{Ind}_{G_{n-1}^0}^{G_n^0} \chi_R \) denotes the character of \( G_n \) induced from \( G_{n-1} \) by \( \chi_R \).) Now a straightforward computation shows that we have

$$\text{Ind}_{G_{n-1}^0}^{G_n^0} \chi_R(m_n) = \prod_{\{R' \in G_n \mid [R'] = R\}} \chi_{R'}(m_n),$$

$$= N_{F_n/F_{n-1}}(\chi_R)(m_n).$$
for any choice of \( R' \in G_n \) with \([q]R' = R\). Hence a representing map for \( \text{res}_{n/n-1}(\alpha) \) in \( \text{Cl}(\mathfrak{H}_n) \) is given by
\[
R \mapsto N_{F_n/F_{n-1}}(\chi_R)(m_n) = \prod_{\{R' \in G_n | [q]R' = R\}} \chi_{R'}(m_n).
\]

We shall now focus our attention on certain natural automorphisms of \( \text{Cl}(\mathfrak{H}_n) \).
Write \( \kappa: \Omega_F \to \mathbb{Z}_p^* \) for the character giving the action of \( \Omega_F \) on the \( p \)-adic Tate module \( T_n \) of \( E \). Let \( \text{Aut}(G_n) \) denote the group of automorphisms of \( G_n \). Then there is a canonical isomorphism \( \text{Aut}(G_n) \to \text{Gal}(F_n/F) \) given by \( \tau \mapsto \sigma_\tau \).
This isomorphism induces an action of \( \text{Aut}(G_n) \) on \( A_n \) via Galois action on each factor occurring 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 \( \tau \in \text{Aut}(G_n) \), we have
\[
[x_R(m)]^{\sigma_\tau} = \sum_{g \in G_n} a_g^\tau w_n(R, g)^{\sigma_\tau}
= \sum_{g \in G_n} a_g^\tau w_n(R^{\tau_\sigma}, g^{\sigma_\tau})
= \sum_{g \in G_n} a_g w_n(R^{\tau_\sigma}, g)
= \sum_{g \in G_n} a_g w_n(\kappa(\sigma_\tau)R, g)
= \sum_{g \in G_n} a_g w_n(R, \kappa(\sigma_\tau)g)
= \chi_R(\kappa(\sigma_\tau)\gamma(m)).
\]
Now \( [\kappa(\sigma_\tau)]: A_n \to A_n \) is a homomorphism of algebras. Hence \( \text{Aut}(G_n) \) preserves the denominator of (2.1), whence it follows that \( \text{Aut}(G_n) \) acts on \( \text{Cl}(\mathfrak{H}_n) \) via its action on \( A_n \).
Thus, \( \text{Cl}(\mathfrak{H}_n) \) is an \( \text{Aut}(G_n) \)-module.

We next observe that \( \text{Aut}(G_n) \simeq \Delta \times \Gamma_n \), where \( |\Delta| = p - 1 \), and \( \Gamma_n \) 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 \( \text{Cl}(\mathfrak{H}_n) \) (inverse limit taken with respect to the restriction maps \( \text{res}_{n/n-1} \)) carries the structure of a \( \Gamma \)-module in the obvious manner.

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

6. The kernel group

Write \( \mathcal{M}_n \) for the \( \mathfrak{S}_F \)-maximal order of \( A_n \). The kernel group \( D(\mathfrak{H}_n) \) of \( \mathfrak{H}_n \) is defined to be the kernel of the natural homomorphism \( \text{Cl}(\mathfrak{H}_n) \to \text{Cl}(\mathcal{M}_n) \). Since \( \mathfrak{H}_{n,p} = \mathcal{M}_{n,p} \) for \( q \nmid p \) (see proposition 2-1 of [AT]), it follows from standard theory that
\[
D(\mathfrak{H}_n) \simeq \frac{\mathcal{M}^e_{n,p}}{\mathfrak{H}_{n,p}}.
\]

The following result is proved in section 9 (see especially (9-7)) of [AT].
Proposition 6.1. There is a natural homomorphism
\[ \delta_n : D(\mathbb{Q}_n) \rightarrow \frac{\mathcal{O}_{F_{n-1}}^\times \mod p}{\text{Im}(\mathcal{O}_{F_{n-1}}^{\times})}, \tag{6.2} \]
where \( \text{Im}(\mathcal{O}_{F_{n-1}}^{\times}) \) denotes the image of \( \mathcal{O}_{F_{n-1}}^{\times} \) mod \( p \). This homomorphism is defined as follows. Set \( L_n = F_n F_n^\ast \); then via the existence of the Weil pairing, we see that \( \mu_{q^n} \subset L_n \). Let \( f \in \text{Gal}(L_n/F(\mu_{q^n})) \) denote the Frobenius automorphism for the primes of \( F(\mu_{q^n}) \) above \( p \). Suppose that \( \alpha \in D(\mathbb{Q}_n) \) is represented in (6.1) by an element \( m \in \mathcal{M}_{\chi,n}^\times \). Then
\[ \delta_n(\alpha) = N_{F_n/F_{n-1}}(\chi_n(m)) \chi_{n-1}(m) \mod \text{Im}(\mathcal{O}_{F_{n-1}}^{\times}) \mod p. \]

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

Lemma 6.2. \( \lim \ker \delta_n(V_n) = 0. \)

Proof. Suppose that \( (s_n) \in \lim \ker \delta_n(V_n) \). Then each class \( s_n \in V_n \) may be represented (via the isomorphism (6.1)) by an element \( m_n \in \mathcal{M}_{\chi,n}^\times \) 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 \( s_n = \text{res}_{M/n}(s_M) \), it follows that there is a representative \( m_n(M) \in \mathcal{M}_{\chi,n}^\times \) 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 \( u_{M-1} \in \mathcal{O}_{F_{M-1}}^\times \) such that \( N_{F_M/F_{M-1}}(\chi_M(m_M)) = u_{M-1} \mod p \). This implies that \( \chi_n(m_n(M)) = u_n \gamma_n \), where \( u_n \in \mathcal{O}_{F_n}^\times \) is a global unit, and \( \gamma_n \in \mathcal{O}_{F_n,n}^\times \). The local unit \( \gamma_n \) may be made as \( p \)-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
\[ \delta = \lim \delta_n : \lim \text{ker} V_n \rightarrow \lim \frac{\mathcal{O}_{F_{n-1}}^\times \mod p}{\text{Im}(\mathcal{O}_{F_{n-1}}^{\times})} \]
(where the right-hand inverse limit is taken with respect to the norm map) is an injection. We remark that \( \delta \) is clearly a \( \Gamma \)-homomorphism.

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

Lemma 6.3. Let \( q \) be any prime of \( F \) lying above \( p \). Then
\[ (1 + p\mathcal{O}_{F,q})N_{F_{n+1}/F_n}(\mathcal{O}_{F_{n+1},q})^\times = \mathcal{O}_{F_n,q}^\times. \]

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

We have the following sequence of maps:

$$
\mathfrak{S}^\prime_{F,a} @ > \text{Artin} >> \text{Gal} (F_{n+1,a}/F_n) @ > \text{transfer} >> \text{Gal} (F_{n+1,a}/F_n).
$$

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

Thus, we have now shown that

$$
\lim V_n \simeq \lim \frac{\mathfrak{S}^\prime_{F_{n+1},p} \mod p}{\text{Im} (\mathfrak{S}^\prime_{F_n})},
$$

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

$$
\lim \frac{\mathfrak{S}^\prime_{F_{n+1},p} \mod p}{\text{Im} (\mathfrak{S}^\prime_{F_n})} \simeq Y_\infty
$$

as $\Gamma$-modules. The following result, which may be regarded as an elliptic analogue of theorem 3-6(a) of [U2], is now immediate.

**Theorem 6-4.** There is a canonical isomorphism of $\Lambda$-modules

$$
\lim V_n \simeq Y_\infty.
$$

**REFERENCES**


On $p$-adic height pairings