Class invariants of Mordell-Weil groups.

Taylor, M.J.; Agboola, A.

in: Journal für die reine und angewandte Mathematik | Journal für die reine und angewandte Mathematik | Article

23 - 62

J. reine angew. Math. 447 (1994), 23—61

Journal für die reine und
angewandte Mathematik
© Walter de Gruyter
Berlin · New York 1994

Class invariants of Mordell-Weil groups

By *A. Agboola*[1]) at New York and Berkeley and *M. J. Taylor*[2]) at Manchester

§ 1. Introduction and statement of results

Let K be an imaginary quadratic number field of classnumber 1; let E/K be an elliptic curve with complex multiplication by the ring of integers $\mathfrak{O}_K$ of K, and let F/K be a finite abelian extension over which E/F acquires everywhere good reduction. Set $\Delta = \mathrm{Gal}(F/K)$. For any field L, we write L^c for a separable closure of L and Ω_L for $\mathrm{Gal}(L^c/L)$.

Choose a prime $p \in \mathbb{Z}$ such that

(a) p is non-anomalous and splits in $\mathfrak{O}_K$ with $p = \pi \cdot \pi^*$, $\mathfrak{p} = \pi\mathfrak{O}_K$, $\mathfrak{p}^* = \pi^*\mathfrak{O}_K$.

(b) $\mathfrak{p}$, $\mathfrak{p}^*$ are primes of good reduction of E/K.

(c) $p \nmid |\Delta|$.

(d) $p > 3$.

Let $E_{\mathfrak{p}^n}$ (resp. $E_{\mathfrak{p}^{*n}}$) denote the group of $\mathfrak{p}^n$ (resp. $\mathfrak{p}^{*n}$)-torsion points of $E(F^c)$. Set

$$G_n = E_{\mathfrak{p}^n}, \quad G_n^* = E_{\mathfrak{p}^{*n}}.$$

(We remark that from time to time we shall abuse notation and also write G_n (resp. G_n^*) for the $\mathfrak{O}_F$-group scheme associated to $E_{\mathfrak{p}^n}$ (resp. $E_{\mathfrak{p}^{*n}}$).)

In § 2 we shall introduce $\mathfrak{O}_F$-orders $\mathfrak{B}_n \subset \mathrm{Map}(G_n, F^c)^{\Omega_F}$ and $\mathfrak{A}_n \subset (\mathbb{Q}^c[G_n])^{\Omega_F}$ such that

$$\mathrm{Spec}(\mathfrak{B}_n) \cong G_n, \quad \mathrm{Spec}(\mathfrak{A}_n) \cong G_n^*$$

as $\mathfrak{O}_F$-group schemes.

[1]) Supported by an NSF Postdoctoral Research Fellowship. The first named author gratefully acknowledges the hospitality of the MSRI, Berkeley, where much of this paper was written.

[2]) Much of the work for this paper was done whilst the author held a Royal Society Leverhulme Senior Research Fellowship.

If $\mathfrak{P}$ is a prime of F, we write $k_{\mathfrak{P}}$ for the residue field of F at $\mathfrak{P}$, and we let $\tilde{E}(k_{\mathfrak{P}})$ denote the reduction of $E(F)$ at $\mathfrak{P}$. Define $E_{1,\mathfrak{p}^*}$ via exactness of the sequence

$$0 \to E_{1,\mathfrak{p}^*} \to E(F) \to \prod_{\mathfrak{P} \mid \mathfrak{p}^*} \tilde{E}(k_{\mathfrak{P}}).$$

Each principal homogeneous space (or p.h.s., for short) of $\mathfrak{B}_n$ is a locally free $\mathfrak{A}_n$-module. In § 3, we shall use this observation to construct a homomorphism

$$\psi_n : E_{1,\mathfrak{p}^*} \to \mathrm{Cl}(\mathfrak{A}_n)$$

where $\mathrm{Cl}(\mathfrak{A}_n)$ denotes the locally free classgroup of $\mathfrak{A}_n$.

Let $\mathfrak{M}_n$ denote the maximal order in $(\mathbb{Q}^c[G_n])^{\Omega_F}$ containing $\mathfrak{A}_n$. Composing ψ_n with the extension of scalars map $e_n : \mathrm{Cl}(\mathfrak{A}_n) \to \mathrm{Cl}(\mathfrak{M}_n)$, we obtain a homomorphism

$$\phi_n : E_{1,\mathfrak{p}^*} \to \mathrm{Cl}(\mathfrak{M}_n).$$

In § 5, we show that by piecing these maps together via inverse limits, we obtain a diagram

$$\begin{tikzcd} E_{1,\mathfrak{p}^*} \otimes_{\mathfrak{O}_K} \mathfrak{O}_{K,\mathfrak{P}} \arrow[r, "\psi"] \arrow[dr, "\phi"'] & \varprojlim \mathrm{Cl}(\mathfrak{A}_n) \arrow[d] \\ & \varprojlim \mathrm{Cl}(\mathfrak{M}_n) . \end{tikzcd}$$

The techniques for applying Iwaṣawa theory to the study of the maps ψ and ϕ originate from the first-named author's thesis (see [A 1]).

The $\mathfrak{A}_n$-module structure of p.h.s. arising from torsion points on $E(F)$ has been fully studied in [ST] (see also [CNT] and [CNS]). In the special case when $n = 1$, $\mathrm{Ker}\,\psi_1$ has been studied in [T 1]. Since principal homogeneous spaces are very closely related to the rings of integers of number fields obtained by dividing points of $E(F)$, knowledge concerning the homomorphisms ψ_n yields important information on the Galois module structure of these rings of integers. For further details on this matter see the introductory discussion to § 3. The main purpose of this paper is to investigate the behaviour of ψ_n on points of infinite order.

Set $\hat{\Delta} = \mathrm{Hom}(\Delta, \mathbb{Q}_p^{c*})$, and let $\mathfrak{O}'$ (resp. $\mathfrak{O}''$) be the ring of integers of some finite extension of $K_\mathfrak{p}$ (resp. $K_{\mathfrak{p}^*}$) which contains all of the character values of Δ. For each $\chi \in \hat{\Delta}$, define

$$r_\chi = \mathrm{rank}_{\mathfrak{O}'}(E(F) \otimes_{\mathfrak{O}_K} \mathfrak{O}')^\chi .$$

(Here, and in the sequel, the superscript χ denotes the χ-eigenspace of $E(F) \otimes_{\mathfrak{O}_K} \mathfrak{O}'$ for the action of Δ.) Let $\bar{\chi}$ be the contragredient of the character χ. Let $\text{Ш}(F)_p$ denote the p-primary component of the Tate-Shafarevitch group of E/F, and write $\{,\}_{F,\mathfrak{p}^*}$ for the algebraic local height pairing

$$\{,\}_{F,\mathfrak{p}^*} : E(F) \otimes_{\mathfrak{O}_K} \mathfrak{O}_{K,\mathfrak{p}} \times E(F) \otimes_{\mathfrak{O}_K} \mathfrak{O}_{K,\mathfrak{p}^*} \to \mathbb{Q}_p$$

described in [PR].

The first main result is the following, which is contained in [A1] (see also [A2]).

Theorem 1. *Suppose that* $|\text{Ш}(F)_p| < \infty$ *and that the pairing* $\{,\}_{F,\mathfrak{p}^*}$ *is non-degenerate modulo torsion. If* $r_\chi \geqq 1$, *then*

$$\operatorname{rank}_{\mathfrak{O}'}(\operatorname{Ker}\phi \otimes_{\mathfrak{O}_{K,\mathfrak{p}}} \mathfrak{O}')^\chi = 1\,.$$

It is interesting to remark that such distinguished one dimensional subspaces of the completed Mordell-Weil group have been constructed, in a completely different setting, by both Greenberg and Plater (see [G] and [P], see also [R]).

Although our main concern is the study of the kernels of ψ and ϕ, we shall also show that under the same hypotheses as Theorem 1:

Theorem 2. *Let* $H_n = F(E_{\pi^{*n}})$ *and write* T_{π^*} *for the* π^**-adic Tate module of E. Then* $\operatorname{Im}\psi$ *is isomorphic to a submodule of finite index in* $\operatorname{Hom}(T_{\pi^*}, \varprojlim \operatorname{Cl}(\mathfrak{O}_{H_n}))^{\Omega_F}$. *Here the inverse limit of ideal class groups is formed with respect to the norm maps from* H_n *to* H_{n-1}.

Our main result on the kernel of ψ is

Theorem 3. *Suppose that* $\mathfrak{p}^*$ *is completely split in F and that F and* $K(E_{p^\infty})$ *are linearly disjoint over K. Then* ψ *is injective on* $E_{1,\mathfrak{p}^*}$.

We remark that a similar result also holds in the case of CM abelian varieties defined over global function fields (see [A1]).

It is our belief that the results of this paper (when taken together with certain results in [MT], [P] and [W]) strongly suggest a new and as yet not understood relationship between class invariants and p-adic height pairings on abelian varieties.

The structure of this paper is as follows: In § 2, we give a detailed description of the orders $\mathfrak{A}_n$ and $\mathfrak{B}_n$. In § 3 and § 4, we briefly recall required results on the class invariants of p.h.s. and on locally free classgroups. § 5 deals with Selmer groups, and in § 6 we introduce the local height pairing of [PR]: we remark that this plays a fundamental role in the proof of Theorem 1.

The remainder of the article is devoted to a proof of Theorem 3. In § 7 we give Kummer descriptions of various subgroups of p.h.s. In § 8 and § 9 we describe a new norm operator, together with certain group ring related higher congruences which were first introduced in [T2]: these algebraic results are the key tools in the proof of Theorem 3. Finally in § 10 we prove Theorem 3.

The authors wish to express their gratitude to Philippe Cassou-Noguès for his detailed comments on an earlier version of this paper.

§ 2. The orders $\mathfrak{A}_n$ and $\mathfrak{B}_n$

In this section we shall give a description of the orders $\mathfrak{A}_n$ and $\mathfrak{B}_n$.

Consider the Hopf algebras

$$B_n = \operatorname{Map}(G_n, F^c)^{\Omega_F}, \quad A_n = (F^c[G_n])^{\Omega_F}$$

where in both cases Ω_F has its natural Galois action on both F^c and G_n.

There is a natural pairing (Cartier duality)

$$B_n \times A_n \to F^c$$

given by

$$\left(f, \sum_{g \in G_n} a_g g\right) \mapsto \sum_{g \in G_n} a_g f(g).$$

Since E/F has everywhere good reduction, $G_n/\operatorname{Spec}\mathfrak{O}_F$ and $G_n^*/\operatorname{Spec}\mathfrak{O}_F$ are both finite, flat group schemes. Thus there exist orders $\mathfrak{B}_n$ in B_n and $\mathfrak{A}_n$ in A_n such that, over $\operatorname{Spec}(\mathfrak{O}_F)$,

$$\operatorname{Spec}(\mathfrak{B}_n) \cong G_n, \quad \operatorname{Spec}(\mathfrak{A}_n) \cong G_n^*.$$

$\mathfrak{A}_n$ and $\mathfrak{B}_n$ are dual to each other with respect to the Cartier pairing. To identify $\mathfrak{A}_n$ as an $\mathfrak{O}_F$-order, we show

Proposition 2.1. *Let $\mathfrak{q}$ be a prime of $\mathfrak{O}_F$.*

(a) *If $\mathfrak{q} \nmid \mathfrak{p}^*$, then $\mathfrak{A}_{n,\mathfrak{q}}$ is the maximal $\mathfrak{O}_{F,\mathfrak{q}}$-order in $A_n \otimes_{\mathfrak{O}_F} \mathfrak{O}_{F,\mathfrak{q}}$.*

(b) *Let $L = F(E_{\mathfrak{p}^n})$. Then if $\mathfrak{q} | \mathfrak{p}^*$,*

$$(\mathfrak{A}_n \otimes_{\mathfrak{O}_F} \mathfrak{O}_L)_\mathfrak{q} \cong \mathfrak{O}_{L,\mathfrak{q}}[G_n].$$

(Here and elsewhere, the subscript $\mathfrak{q}$ denotes semi-localisation at $\mathfrak{q}$.)

Proof. (a) Since E/F has everywhere good reduction, $G_n^*/\operatorname{Spec}\mathfrak{O}_F$ is étale away from $\mathfrak{p}^*$, which implies the result.

(b) Write $\mathfrak{B}_{L,\mathfrak{q}} = \mathfrak{B}_n \otimes_{\mathfrak{O}_F} \mathfrak{O}_{L,\mathfrak{q}}$; then the Cartier dual of $\mathfrak{B}_{L,\mathfrak{q}}$ is $(\mathfrak{A}_n \otimes_{\mathfrak{O}_F} \mathfrak{O}_L)_\mathfrak{q}$. Since $\mathfrak{q}$ is non-ramified in L/F, we have $\operatorname{Spec}(\mathfrak{B}_{L,\mathfrak{q}}) = \operatorname{Spec}(\mathfrak{B}) \times_{\mathfrak{O}_L} \operatorname{Spec}(\mathfrak{O}_{L,\mathfrak{q}})$ (because locally the Néron model is stable under non-ramified extensions). As E/F has everywhere good reduction, $\operatorname{Spec}(\mathfrak{B}_{L,\mathfrak{q}})$ is étale. Hence $\mathfrak{B}_{L,\mathfrak{q}}$ is the $\mathfrak{O}_{L,\mathfrak{q}}$-maximal order in $B_n \otimes_{\mathfrak{O}_F} \mathfrak{O}_{L,\mathfrak{q}}$, and so the Cartier dual of $\mathfrak{B}_{L,\mathfrak{q}}$ is the group ring $\mathfrak{O}_{L,\mathfrak{q}}[G_n]$. □

We remark that $\mathfrak{A}_n$ acts on $\mathfrak{B}_n$ via

$$\left(f \cdot \sum_{g \in G_n} \alpha_g g\right)(R) = \sum_{g \in G_n} f(R-g)\alpha_g$$

for $f \in \mathfrak{B}_n$, $\sum_{g \in G_n} \alpha_g g \in \mathfrak{A}_n$, and $R \in G_n$. It is shown in Proposition 2 of [T3] that $\mathfrak{B}_n$ is a free $\mathfrak{A}_n$-module with respect to this action.

Let

$$W_n : G_n \times G_n^* \to \mu_{p^n}$$

denote the Weil pairing on E. (We shall sometimes regard W_n as being extended to a pairing $F^c[G_n] \times F^c[G_n^*] \to F^c$ via F^c-linearity.) W_n identifies $\hat{G}_n$ (resp. $\hat{G}_n^*$) with G_n^* (resp. G_n). Set $H_1 = F(E_{p^{*i}})$, $F_i = F(E_{p^i})$.

Proposition 2.2. (a) *Let G_n^*/Ω_F (resp. G_n/Ω_F) be a set of representatives of Ω_F-orbits of G_n^* (resp. G_n). Then*

$$A_n = \prod_{R \in G_n^*/\Omega_F} F(R), \quad B_n = \prod_{Q \in G_n/\Omega_F} F(Q).$$

(b) *In particular, if F is linearly disjoint from $K(E_{p^n})$ over K, then*

$$A_n = \prod_{i=0}^{n} H_i, \quad B_n = \prod_{i=0}^{n} F_i.$$

Proof. It is clear that (b) follows immediately from (a). We shall just prove (a) for the algebra A_n, as the proof for B_n is similar.

The F-algebra $A_n = (F^c[G_n])^{\Omega_F} = (F_n[G_n])^{\Omega_F}$ is generated by all elements of the form $\sum_{\omega} \ell^{\omega} g^{\omega}$, where $\ell \in F_n$, $g \in G_n$, and the sum is over a transversal of $\Omega_{F_n} \backslash \Omega_F$. Suppose that $R \in G_n^*$ and $\lambda \in \Omega_F$. Recall that we have identified $\hat{G}_n$ with G_n^* via the Weil pairing W_n. Then

$$\begin{aligned}\left(\sum_{\omega} \ell^{\omega} W_n(g^{\omega}, R)\right)^{\lambda} &= \sum_{\omega} \ell^{\omega\lambda} W_n(g^{\omega\lambda}, R^{\lambda}) \\ &= \sum_{\omega} \ell^{\omega} W_n(g^{\omega}, R^{\lambda}).\end{aligned}$$

Hence the map $\prod_{R} W(-, R)$ yields an embedding $(F_n[G_n])^{\Omega_F} \subseteqq \prod_{R \in G_n^*/\Omega_F} F(R)$. Since both sides of the inclusion have the same dimension over F as F-vector spaces, the result follows. □

Remark. In the sequel, we shall always suppose the isomorphisms in (b) to be induced by evaluation on $\bigoplus_{i=0}^{n} p^{n-i}Q$ for B_n, and by $\bigoplus_{i=0}^{n} W_n(-, p^{n-i}R)$ for A_n, where Q (resp. R) is a point of order π^n (resp. π^{*n}).

§ 3. Class invariants

We shall now recall the basic properties of class invariants. General references for the material discussed in this section are [BT] and [T3].

Let C denote an F-algebra on which A_n acts via its co-algebra structure. Thus C is an A_n module, and if $\Delta : A_n \to A_n \underset{F}{\otimes} A_n$ is the comultiplication of A_n, then for $a \in A_n$ and $c_1, c_2 \in C$, we have

$$(c_1 \cdot c_2) = a \sum_i (c_1 a_{i1}) \cdot (c_2 a_{2i})$$

where

$$\Delta(a) = \sum_i a_{i1} \otimes a_{i2} .$$

We call such a C a principal homogeneous space for B_n if there exists a field extension L/F and an isomorphism

$$\xi : C \underset{F}{\otimes} L \to B_n \underset{F}{\otimes} L$$

which respects A_n action in the first variables and L-action in the second. We call ξ a splitting isomorphism for C. Note that if we take $L \supset F_n$, then $A_n \otimes L = L[G]$ and so ξ will be an $L[G]$ module isomorphism.

A principal homogeneous space for $\mathfrak{B}_n$ is an $\mathfrak{O}_F$-algebra $\mathfrak{C}$ on which $\mathfrak{A}_n$ acts, such that $\mathfrak{C}$ is an order in some p.h.s. $C = \mathfrak{C} \cdot F$ for B and such that the splitting isomorphism ξ for C induces an isomorphism

$$\xi : \mathfrak{C} \otimes_{\mathfrak{O}_F} \mathfrak{O}_L \to \mathfrak{B}_n \otimes_{\mathfrak{O}_F} \mathfrak{O}_L .$$

We write $PH(B_n)$ (resp. $PH(\mathfrak{B}_n)$) for the set of isomorphism classes of p.h.s. for B_n (resp. $\mathfrak{B}_n$). Both $PH(B_n)$ and $PH(\mathfrak{B}_n)$ carry the structure of abelian groups.

$\mathfrak{C}$ is an $\mathfrak{A}_n$-module since ξ is G_n-equivariant and $\mathfrak{B}_n$ is an $\mathfrak{A}_n$-module. It can be shown that $\mathfrak{B}_n$ is $\mathfrak{A}_n$-free; it therefore follows that $\mathfrak{C}$ is projective over $\mathfrak{A}_n$. This implies that $\mathfrak{C}$ is a locally free $\mathfrak{A}_n$-module (see for instance [F2]). Let $(\mathfrak{C})$ denote the class of $\mathfrak{C}$ in the locally free classgroup $\mathrm{Cl}(\mathfrak{A}_n)$. Then we obtain a map

$$\text{(3.1)} \qquad \begin{aligned} \tilde{\psi}_n : PH(\mathfrak{B}_n) &\to \mathrm{Cl}(\mathfrak{A}_n), \\ \mathfrak{C} &\mapsto (\mathfrak{C}) . \end{aligned}$$

$\tilde{\psi}_n$ is a homomorphism (cf. e.g. Theorem 3.1 of [BT]).

For a more general version of this homomorphism, see [W].

We shall now recall the notion of the Kummer order associated to a point $Q \in E(F)$ (cf. §1 of [T3]). Suppose that $Q \in E(F)$, and write

$$G_Q(n) = \{Q' \in E(F^c) \mid \pi^n Q' = Q\} .$$

Define the Kummer algebra $F_Q(n)$ by

$$F_Q(n) = \mathrm{Map}\,(G_Q(n), F^c)^{\Omega_F}.$$

Then A_n acts on $F_Q(n)$ via

$$\left(f \cdot \sum_{g \in G_n} \alpha_g g\right)(Q') = \sum_{g \in G_n} \alpha_g f(Q' - g) \tag{3.2}$$

for $f \in F_Q(n)$, $\sum_{g \in G_n} \alpha_g g \in A_n$ and $Q' \in G_Q(n)$. $F_Q(n)$ is a p.h.s. of B_n (see § 3 of [T 3]).

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

$$\mathfrak{C}_Q(n) = \{x \in \mathfrak{O}_Q(n) \mid x \cdot \mathfrak{A}_n \subseteq \mathfrak{O}_Q(n)\}.$$

It is shown in [T 3] that, since E/F has everywhere good reduction, $\mathfrak{C}_Q(n)$ is a p.h.s. of $\mathfrak{B}_n$. Furthermore, $\mathfrak{C}_Q(n)$ is a trivial p.h.s. for $\mathfrak{B}_n$ if and only if $Q \in \mathfrak{p}^n E(F)$. Hence we obtain a map

$$\begin{aligned} E(F) &\to PH(\mathfrak{B}_n), \\ Q &\mapsto \mathfrak{C}_Q(n) \end{aligned} \tag{3.3}$$

which yields an injection

$$E(F)/\mathfrak{p}^n E(F) \to PH(\mathfrak{B}_n). \tag{3.4}$$

This injection may also be described in terms of a cohomological exact sequence arising from Kummer theory on the Néron model $\mathfrak{E}/\mathrm{Spec}\,\mathfrak{O}_F$ of E/F. The endomorphism π^n of E yields the exact Kummer sequence

$$0 \to \mathfrak{E}_{\pi^n} \to \mathfrak{E} \xrightarrow{\pi^n} \mathfrak{E} \to 0. \tag{3.5}$$

This in turn yields the following exact sequence of flat cohomology

$$0 \to \mathfrak{E}_{\pi^n} \to \mathfrak{E}(\mathfrak{O}_F) \xrightarrow{\pi^n} \mathfrak{E}(\mathfrak{O}_F) \to H^1(\mathrm{Spec}(\mathfrak{O}_F), \mathfrak{E}_{\pi^n}). \tag{3.6}$$

Since $H^1(\mathrm{Spec}(\mathfrak{O}_F), \mathfrak{E}_\pi) \cong PH(\mathfrak{B}_n)$ (see e.g. [M], Chapter III, §4), and $E(F) \cong \mathfrak{E}(\mathfrak{O}_F)$ (via the universal property of the Néron model), we obtain a composite homomorphism

$$\frac{E(F)}{\mathfrak{p}^n E(F)} \cong \frac{\mathfrak{E}(\mathfrak{O}_F)}{\mathfrak{p}^n \mathfrak{E}(\mathfrak{O}_F)} \to PH(\mathfrak{B}_n); \tag{3.7}$$

this is the same as the injection (3.4).

(3.1) and (3.4) yield a homomorphism

$$E(F) \to \mathrm{Cl}(\mathfrak{A}_n). \tag{3.8}$$

Via restriction, we obtain homomorphisms

$$\psi_n : E_{1,\mathfrak{p}^*} \to \mathrm{Cl}(\mathfrak{A}_n) \tag{3.9}$$

and

$$\phi_n : E_{1,\mathfrak{p}^*} \to \mathrm{Cl}(\mathfrak{M}_n), \tag{3.10}$$

where $\phi_n = e_n \circ \psi_n$. Since $\mathfrak{p}^n E_{1,\mathfrak{p}^*} \subseteq \mathrm{Ker}\,\psi_n$, it follows that both ψ_n and ϕ_n factor through $E_{1,\mathfrak{p}^*}/\mathfrak{p}^n E_{1,\mathfrak{p}^*}$. This gives homomorphisms (which we also denote by ψ_n and ϕ_n)

$$\psi_n : E_{1,\mathfrak{p}^*}/\mathfrak{p}^n E_{1,\mathfrak{p}^*} \to \mathrm{Cl}(\mathfrak{A}_n) \tag{3.11}$$

and

$$\phi_n : E_{1,\mathfrak{p}^*}/\mathfrak{p}^n E_{1,\mathfrak{p}^*} \to \mathrm{Cl}(\mathfrak{M}_n). \tag{3.12}$$

We shall write $\psi_n^{(F)}$ (resp. $\phi_n^{(F)}$) when it is necessary to indicate the dependence of ψ_n (resp. ϕ_n) upon the field F.

§ 4. Classgroups

In this section, we often view n as being fixed. When this is the case, we shall frequently write G, G^*, $\mathfrak{M}$, $\mathfrak{A}$, etc. in place of G_n, G_n^*, $\mathfrak{M}_n$, $\mathfrak{A}_n$ etc.

It follows immediately from Proposition 2.2 (a) that we have a decomposition

$$\mathfrak{M} \cong \prod_{R \in G^*/\Omega_F} \mathfrak{O}_{F(R)}$$

and so

$$\mathrm{Cl}(\mathfrak{M}) \cong \prod_{R \in G^*/\Omega_F} \mathrm{Cl}(\mathfrak{O}_{F(R)}). \tag{4.1}$$

We now briefly recall Fröhlich's Hom-description of locally free classgroups of orders. For details of this construction see [F1]. For any number field N, we write $J(N)$ for the group of finite ideles of N. Let J denote $\varinjlim_{F \subset N \subset F^c} J(N)$, the direct limit of the finite idele groups of number fields N containing F. Set

$$\tilde{\mathfrak{A}} = \prod_{\mathfrak{q}} \mathfrak{A}_{\mathfrak{q}},$$

where the product is taken over all maximal ideals of $\mathfrak{O}_F$.

Suppose that $u \in \tilde{\mathfrak{A}}^{\times}$. Then u determines a map $\mathrm{Det}(u) \in \mathrm{Map}(G^*, J)^{\Omega_F}$, which is defined by

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

(Here χ_R denotes the character of G which is identified with $R \in G^*$ via the Weil pairing W.) Then there is an isomorphism

$$\text{(4.2)} \qquad \mathrm{Cl}(\mathfrak{A}) \cong \frac{\mathrm{Map}(G^*, J)^{\Omega_F}}{\mathrm{Det}(\tilde{\mathfrak{A}}^{\times})\,\mathrm{Map}(G^*, F^{c\times})^{\Omega_F}}.$$

Let U denote the subgroup of unit ideles of J. Then

$$\mathrm{Det}(\tilde{\mathfrak{M}}^{\times}) = \mathrm{Map}(G^*, U)^{\Omega_F},$$

and we have an isomorphism

$$\text{(4.3)} \qquad \mathrm{Cl}(\mathfrak{M}) \cong \frac{\mathrm{Map}(G^*, J)^{\Omega_F}}{\mathrm{Map}(G^*, U)^{\Omega_F} \cdot \mathrm{Map}(G^*, F^{c\times})^{\Omega_F}}.$$

The isomorphism (4.1) is obtained from (4.3) by evaluating on a set of orbit representatives of G^*/Ω_F and taking idele content.

Recall that the kernel group $D(\mathfrak{A})$ is defined to be the kernel of the homomorphism e: $\mathrm{Cl}(\mathfrak{A}) \to \mathrm{Cl}(\mathfrak{M})$. Hence, via naturality of the Hom-description, we have an isomorphism

$$D(\mathfrak{A}) \cong \frac{\mathrm{Det}(\tilde{\mathfrak{M}}^{\times})}{\mathrm{Det}(\tilde{\mathfrak{A}}^{\times}) \cdot \mathrm{Map}(G^*, \mathfrak{O}_{F^c}^{\times})^{\Omega_F}}.$$

From (2.1) $\mathfrak{A}_{\mathfrak{q}} = \mathfrak{M}_{\mathfrak{q}}$ when $\mathfrak{q} \nmid \mathfrak{p}^*$; this implies that

$$\text{(4.4)} \qquad D(\mathfrak{A}) \cong \frac{\mathrm{Det}(\mathfrak{M}_{\mathfrak{p}^*}^{\times})}{\mathrm{Det}(\mathfrak{A}_{\mathfrak{p}^*}^{\times})\,\mathrm{Map}(G^*, \mathfrak{O}_{F^c}^{\times})^{\Omega_F}}.$$

Recall that F_n is the field generated over F by the coordinates of $E_{\mathfrak{p}^n}$. Let $C \in PH(B)$. Then in general C is not stable under the action of G; however, $C \underset{F}{\otimes} F_n$ is Galois over F_n with Galois group G – since $B \underset{F}{\otimes} F_n = \mathrm{Map}(G, F_n)$. Moreover, this latter algebra is seen to be a Galois algebra over F with Galois group $\mathrm{Gal}(F_n/F) \ltimes G$, where for $g \in G$ and $\gamma \in \mathrm{Gal}(F_n/F)$:

$$\gamma^{-1} g \gamma = \gamma(g) \quad \text{(i.e. Galois action of } \gamma \text{ on } g).$$

In the sequel we write this value unambiguously as g^{γ}.

Since $C \underset{F}{\otimes} F_n$ is a p.h.s. of $B \underset{F}{\otimes} F_n$ over F, we conclude that $C \underset{F}{\otimes} F_n$ is also a Galois algebra over F with Galois group $\Gamma' \ltimes G$, where $\Gamma' = \mathrm{Gal}(F_n/F)$. For $C \in PH(B)$ we define the resolvend map

$$r_C : C \to (C \otimes F_n)[G]$$

by

$$r_C(c) = \sum_{g \in G} c^g \cdot g^{-1}.$$

Note that by the above remarks $c^g \in C \otimes F_n$, but that in general c^g is not in C. From time to time it will be advantageous to enlarge the range of r_C to $C \otimes F_n$, by allowing $c \in C \otimes F_n$ in the defining formula. With this convention note that for $h \in G$

$$\begin{aligned} r_C(c^h) &= \sum c^{hg} g^{-1} = \sum c^g g^{-1} h \\ &= r_C(c) h \end{aligned}$$

and so we conclude that the map r_C is an A-module homomorphism. It is a standard result in Galois theory that $r_C(c)$ is invertible in $(C \otimes F_n)[G]$ iff $C = cA$. In the sequel we shall write r instead of r_C when C is clear from the context.

Now let $\mathfrak{C} \in PH(\mathfrak{B})$ with $C = \mathfrak{C}F$. We next show how the resolvend map r_C can be used to construct a representing map for $\psi(\mathfrak{C}) \in \mathrm{Cl}(\mathfrak{A})$ (under the isomorphism (4.2)).

Proposition 4.5. (a) *Both $\psi(\mathfrak{C})$ and $\phi(\mathfrak{C})$ are represented under* (4.2) *and* (4.3) *by the map*

$$\mathrm{Det}\left(r(c)\, r(\tilde{c})^{-1}\right),$$

where $C = c \cdot A$, $\tilde{c} = \prod_{\mathfrak{q} < \infty} c_{\mathfrak{q}}$, and $\mathfrak{C}_{\mathfrak{q}} = c_{\mathfrak{q}} \cdot \mathfrak{A}_{\mathfrak{q}}$.

(b) *Suppose that* $(\mathfrak{C}) \in \ker \phi$, *with $\mathfrak{C}\mathfrak{M} = c \cdot \mathfrak{M}$ and $\mathfrak{C}_{\mathfrak{p}*} = c_{\mathfrak{p}*} \mathfrak{A}_{\mathfrak{p}*}$. Then $\psi(\mathfrak{C})$ is represented under* (4.4) *by*

$$\mathrm{Det}\left(r(c)\, r(c_{\mathfrak{p}*})^{-1}\right).$$

Proof. (a) is proved in Proposition 6 of [T3] (see also Lemma 3.11 in [BT]), and (b) follows immediately from (a). □

For future reference, we record

Lemma 4.6. *Let $\mathfrak{O}_{C \otimes F_n}$ denote the integral closure of $\mathfrak{O}_F$ in $C \otimes F_n$. Then, with the above notation,*

(a) $r(c_{\mathfrak{p}*}) \in (\mathfrak{O}_{C \otimes F_n, \mathfrak{p}*}[G])^\times$,

(b) *$\pi^{-n} r(c_{\mathfrak{q}})$ is a unit in the maximal order containing $(\mathfrak{O}_{C \otimes F_n, \mathfrak{q}}[G])^\times$ for all primes $\mathfrak{q}$ of $\mathfrak{O}_F$.*

Proof. Clearly (b) implies (a). However, (b) follows immediately from Theorem 3 in [T3]. □

Proposition 4.7. *There is a commutative diagram*

(4.8)
$$\begin{tikzcd}
E_{1,\mathfrak{p}^*} \arrow[r, "\psi_{n+1}"] \arrow[dr, "\psi_n"'] & \mathrm{Cl}(\mathfrak{A}_{n+1}) \arrow[r, "e_{n+1}"] \arrow[d] & \mathrm{Cl}(\mathfrak{M}_{n+1}) \arrow[d] \\
& \mathrm{Cl}(\mathfrak{A}_n) \arrow[r, "e_n"'] & \mathrm{Cl}(\mathfrak{M}_n)
\end{tikzcd}$$

where the vertical arrows are induced by the quotient maps $[\pi]\colon \mathfrak{A}_{n+1} \to \mathfrak{A}_n$, $[\pi]\colon \mathfrak{M}_{n+1} \to \mathfrak{M}_n$ *which are in turn induced by the natural homomorphism* $[\pi]\colon G_{n+1} \to G_n$.

Remark. In order that the corresponding diagram commutes, when the classgroups are given in their Fröhlich-descriptions (4.2), (4.3), we need to normalise the Weil pairing so that for $g \in G_{n+1}$, $R \in G_n^*$

$$W_n(\pi g, R) = W_{n+1}(g, R)$$

(see (3.7) in [PR]). This then guarantees that the diagram

$$\begin{tikzcd}
\mathrm{Map}(G_{n+1}^*, J)^{\Omega_F} \arrow[r] \arrow[d] & \mathrm{Cl}(\mathfrak{A}_{n+1}) \arrow[d, "{[\pi]}"] \\
\mathrm{Map}(G_n^*, J)^{\Omega_F} \arrow[r] & \mathrm{Cl}(\mathfrak{A}_n)
\end{tikzcd}$$

commutes, with the left-hand vertical arrow being induced by $G_n^* \subset G_{n+1}^*$.

Proof. The fact that the square commutes is a standard functoriality property; we now prove that the triangle commutes.

Let $\Sigma = \sum_{g \in G_1} g$. It is shown in Proposition 1 of [ST] that there is an isomorphism

$$\mathfrak{C}_{n+1} \cdot \frac{\Sigma}{\pi} \cong \mathfrak{C}_n$$

of $\mathfrak{A}_n$-modules. Hence (using the notation of Proposition 4.5), if $(\mathfrak{C}_{n+1}) \in \mathrm{Cl}(\mathfrak{A}_{n+1})$ is represented by $\mathrm{Det}(r_{C_{n+1}}(c)\, r_{C_{n+1}}(\tilde{c})^{-1})$, then $(\mathfrak{C}_n) \in \mathrm{Cl}(\mathfrak{A}_n)$ is represented by

$$\mathrm{Det}\left(r_{C_n}\left(c \cdot \frac{\Sigma}{\pi}\right) r_{C_n}\left(\tilde{c} \cdot \frac{\Sigma}{\pi}\right)^{-1}\right).$$

However,

$$\begin{aligned}
[\pi]\, r_{C_{n+1}}(c) &= \sum_{g \in G_{n+1}} c^g \cdot [\pi] g^{-1} \\
&= r_{C_n}(c \cdot \Sigma),
\end{aligned}$$

which implies the result. □

It follows that, using (3.11) and (3.12) and passing to the inverse limit of diagram (4.8), we obtain the commutative diagram

$$\begin{tikzcd}
E_{1,\mathfrak{p}^*}\otimes_{\mathfrak{O}_K}\mathfrak{O}_{K,\mathfrak{p}} \arrow[r, "\psi"] \arrow[dr, "\phi"'] & \varprojlim \mathrm{Cl}(\mathfrak{A}_n) \arrow[d, "e"] \\
 & \varprojlim \mathrm{Cl}(\mathfrak{M}_n)
\end{tikzcd}$$

of the Introduction.

We now return to the point of view of (4.1).

Proposition 4.9. (a) *For* $h \in G^*$ *let* $\chi : (C \otimes_F F_n)[G] \to F^c$ *denote any* F_n*-algebra homomorphism such that* $\chi | G = W(-, h)$, *then*

$$\chi(r_C(c))\mathfrak{O}_{F^c} = \mathfrak{b}(h)\mathfrak{O}_{F^c}$$

for some ideal $\mathfrak{b}(h)$ *in* $F(h)$. *If* h *is a chosen orbit representative in the decomposition* (4.1), *then the class* $(\mathfrak{C}\mathfrak{M}) \in \mathrm{Cl}(\mathfrak{M})$ *has* h*-component given by the* $\mathfrak{O}_{F(h)}$*-class of* $\mathfrak{b}(h)$.

(b) *For* $m \in \mathbb{Z}$, *we have*

$$(\mathfrak{b}(mh)) = (\mathfrak{b}(h)^m)$$

in $\mathrm{Cl}(\mathfrak{O}_{F(h)})$.

(c) *The equality*

$$(\mathfrak{b}(ph)) = N_{F(h)/F(ph)}(\mathfrak{b}(h))$$

holds in $\mathrm{Cl}(\mathfrak{O}_{F(ph)})$, *provided that the order of* h *is sufficiently large.*

Before proving this Proposition, we note that we have two Corollaries.

Corollary 4.10. *Each principal homogeneous space* $\mathfrak{C} \in PH(\mathfrak{B}_n)$ *determines an element in* $\mathrm{Hom}(E_{\mathfrak{p}^{*n}}, \mathrm{Cl}(\mathfrak{O}_{H_n}))^{\Omega_F}$ *which depends only upon* $(\mathfrak{C} \cdot \mathfrak{M}_n) \in \mathrm{Cl}(\mathfrak{M}_n)$.

Proof. This homomorphism is given by

$$\mathfrak{C} \mapsto \{h \mapsto (\mathfrak{b}(h) \cdot \mathfrak{O}_{H_n})\}. \quad \square$$

From Propositions 4.7 and 4.9 (c), we see that if $\mathfrak{C} \in PH(\mathfrak{B}_{n+1})$ and if f_{n+1} (resp. f_n) is the homomorphism corresponding to $(\mathfrak{C} \cdot \mathfrak{M}_{n+1}) \in \mathrm{Cl}(\mathfrak{M}_{n+1})$ (resp. $[\pi]$ $(\mathfrak{C} \cdot \mathfrak{M}_{n+1}) \in \mathrm{Cl}(\mathfrak{M}_n)$) under Corollary 4.10, then we have a commutative diagram

(4.11)
$$\begin{tikzcd} E_{\mathfrak{p}^{*n+1}} \arrow[r, "f_{n+1}"] \arrow[d, "{[p]}"] & \mathrm{Cl}(\mathfrak{O}_{H_{n+1}}) \arrow[d, "N_{H_{n+1}/H_n}"] \\ E_{\mathfrak{p}^{*n}} \arrow[r, "f_n"'] & \mathrm{Cl}(\mathfrak{O}_{H_n}) \, . \end{tikzcd}$$

(Here the left-hand vertical arrow is the natural map induced by $[p] \in \mathrm{End}(E)$.)

Now the element $[\pi^n] \in \mathrm{End}(E)$ induces an Ω_F-automorphism on G_n^*.

Let $\tau_n : G_n^* \to G_n^*$ denote the inverse of this automorphism. Then (4.11) implies that the following diagram commutes:

(4.12)
$$\begin{tikzcd} E_{\mathfrak{p}^{*n+1}} \arrow[r, "f_{n+1} \circ \tau_{n+1}"] \arrow[d, "{[\pi^*]}"] & \mathrm{Cl}(\mathfrak{O}_{H_{n+1}}) \arrow[d, "N_{H_{n+1}/H_n}"] \\ E_{\mathfrak{p}^{*n}} \arrow[r, "f_n \circ \tau_n"'] & \mathrm{Cl}(\mathfrak{O}_{H_n}) \, . \end{tikzcd}$$

Passing to the inverse limit of (4.12) yields a homomorphism

$$(4.13) \qquad \varprojlim f_n \circ \tau_n : T_{\pi^*} \to \varprojlim Cl(\mathfrak{O}_{H_n}) \, .$$

Piecing together Proposition 4.7, Corollary 4.10, and (4.13) gives

Corollary 4.14. *The homomorphism*

$$\phi : E_{1,\mathfrak{p}^*} \otimes_{\mathfrak{O}_K} \mathfrak{O}_{K,\mathfrak{p}} \to \varprojlim \mathrm{Cl}(\mathfrak{M}_n)$$

determines a homomorphism

$$\phi' : E_{1,\mathfrak{p}^*} \otimes_{\mathfrak{O}_K} \mathfrak{O}_{K,\mathfrak{p}} \to \mathrm{Hom}(T_{\pi^*}, \varprojlim \mathrm{Cl}(\mathfrak{O}_{H_n}))^{\Omega_F} \, . \quad \square$$

Now it follows at once from the construction of the homomorphism ϕ' that $\ker \phi = \ker \phi'$ and $\mathrm{im}\, \phi \cong \mathrm{im}\, \phi'$; we therefore deduce that in order to prove Theorem 1, we may work with ϕ' rather than ϕ.

We now return to the proof of Proposition 4.9.

Proof of 4.9 (a). $r = r(c)\, r(\tilde{c})^{-1}$ is an idele of the algebra A; thus, as per (2.2), the value $\chi(r)$ is an $F(h)$-idele, which is independent of the particular choice of extension χ. However, by 4.6 (b), $\chi(r(\tilde{c}))$ has content π^n. This then shows that the content of $\chi(r(c))$ is the content of some $\mathfrak{O}_{F(h)}$-ideal $\mathfrak{d}(h)$. The result now follows. □

Recall that $C \otimes_F F_n/F$ is a Galois algebra extension with Galois group $\Xi = \Gamma \ltimes G$, where $\Gamma = \mathrm{Gal}(F_n/F)$. Let Ξ act on $C \otimes F_n[G]$ via Galois action on the coefficients $C \otimes F_n$ and via the Galois action of Γ on G. Then

$$(C \otimes_F F_n[G])^{\Xi} = (F_n[G])^{\Gamma} = A \, .$$

In order to prove 4.9(b) and 4.9(c), we shall require the following result, which will be proved in §7. (See the proof of Proposition 7.5.)

Lemma 4.15. *Recall that, for $m \in \mathbb{Z}$,*

$$[m]\, r_C(c) = \sum_{g \in G_n} c^g g^{-m}$$

for all $c \in C$. Then given $\omega \in \Xi$ there is a $g_0 = g_0(\omega) \in G_n$ such that for all $m \in \mathbb{Z}$,

$$\sum_{g \in G_n} c^{g\omega} \cdot g^{-m\omega} = \left(\sum_{g \in G_n} c^g g^{-m} \right) g_0^m ,$$

i.e.

$$[m]\, r_C(c)^{\omega} = [m]\, r_C(c) \cdot g_0^m .$$

Proof of 4.9(b). This follows at once from 4.9(a), together with the observation that, by Lemma 4.15, $[m]\, r_C(c) \cdot r_C(c)^{-m}$ is Ξ fixed and so lies in A_n.

Proof of 4.9(c). Suppose that h has order p^{n+1}, and that this order is sufficiently large to guarantee that the extension $F(h)/F(ph)$ is of degree p. Then Lemma 4.15 implies that

$$r_C(c)^{-p} \prod_{i=0}^{p-1} ([1 + ip^n]\, r_C(c)) \in A_{n+1} .$$

The result now follows upon applying the character $W_n(-, h)$. □

§ 5. Selmer groups

We shall now recall the definitions of certain Selmer and Tate-Shafarevitch groups associated to E.

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

$$H^1(L, E_{\mathfrak{p}^{*n}}) \to \prod_{\mathfrak{q}} H^1(L_{\mathfrak{q}}, E) .$$

The Tate-Shafarevitch group Ш(L) of E/L is defined by

$$\text{Ш}(L) = \operatorname{Ker}(H^1(L, E) \to \prod_{\mathfrak{q}} H^1(L_{\mathfrak{q}}, E)) .$$

We shall also require the enlarged Selmer group $S'(L)^{(\pi^{*n})}$ which is defined by

$$S'(L)^{(\pi^{*n})} = \operatorname{Ker}\left(H^1(L, E_{\mathfrak{p}^{*n}}) \to \prod_{\mathfrak{q} \nmid \mathfrak{p}^*} H^1(L_{\mathfrak{q}}, E) \right)$$

and the enlarged Tate-Shafarevitch group

$$Ш'(L) = \operatorname{Ker}\left(H^1(L, E) \to \prod_{\mathfrak{q} \nmid \mathfrak{p}^*} H^1(L_{\mathfrak{q}}, E)\right).$$

Write $S(L, \pi^{*\infty}) = \varinjlim_n S(L)^{(\pi^{*n})}$, $S'(L, \pi^{*\infty}) = \varinjlim_n S'(L)^{(\pi^{*n})}$ and denote the Pontryagin dual of $S(L, \pi^{*\infty})$ by $Y(L, \pi^{*\infty})$.

Set $\Gamma = \operatorname{Gal}(H_\infty/F)$ and $D_{\mathfrak{p}^*} = K_{\mathfrak{p}^*}/\mathfrak{O}_{\mathfrak{p}^*}$. Then $\Gamma = \Delta_1 \times \Gamma_1$ where $\Gamma_1 \cong \mathbb{Z}_p$ and Δ_1 is of order prime to p. We observe that, as F/K is abelian, $Y(H_\infty, \pi^{*\infty})$ is a torsion module for the Iwasawa algebra associated to Γ. (See e.g. [C], Theorem 12 and Proposition 15.)

Theorem 4 (Coates). *Let $\mathfrak{X}_\infty$ denote the Galois group over H_∞ of the maximal pro-p abelian extension of H_∞ which is unramified away from all primes dividing $\mathfrak{p}^*$.*

(a) *There are natural Γ-isomorphisms*

$$S(H_\infty, \pi^{*\infty}) \cong \operatorname{Hom}(\mathfrak{X}_\infty, E_{\mathfrak{p}^{*\infty}})$$

and

$$S'(F, \pi^{*\infty}) \cong \operatorname{Hom}(\mathfrak{X}_\infty, E_{\mathfrak{p}^{*\infty}})^\Gamma .$$

(b) *There is a further isomorphism*

$$Y(H_\infty, \pi^{*\infty}) \cong \operatorname{Hom}(T_{\pi^*}, \mathfrak{X}_\infty),$$

and the following diagram commutes for some isomorphism a:

$$\begin{tikzcd}
S(H_\infty, \pi^{*\infty}) \times Y(H_\infty, \pi^{*\infty}) \arrow[r] \arrow[d] & D_{\mathfrak{p}^*} \arrow[d, "a"] \\
\operatorname{Hom}(\mathfrak{X}_\infty, E_{\mathfrak{p}^{*\infty}}) \times \operatorname{Hom}(T_{\pi^*}, \mathfrak{X}_\infty) \arrow[r] & E_{\mathfrak{p}^{*\infty}}
\end{tikzcd}$$

where the bottom row is the pairing given by

$$(5.1) \qquad (f_1, f_2) \mapsto f_1(f_2(t))$$

for a chosen generator t of T_{π^*}.

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

(b) Choosing a generator t of T_{π^*} over $\mathfrak{O}_{\mathfrak{p}^*}$ is equivalent to fixing an isomorphism $\mathfrak{O}_{\mathfrak{p}^*} \xrightarrow{\sim} T_{\pi^*}$ such that $1 \mapsto t$. This in turn induces an isomorphism a: $D_{\mathfrak{p}^*} \to E_{\mathfrak{p}^{*\infty}}$. It is easy to check that the pairing induced by (5.1) and a^{-1} is non-degenerate and independent of the choice of t. This gives the result. □

Now let $\mathcal{X}_\infty$ denote the Galois group over H_∞ of the maximal pro-p abelian extension of H_∞ which is everywhere unramified. Define $\mathcal{U} = \mathrm{Hom}(\mathcal{X}_\infty, E_{\mathfrak{p}^{*\infty}})$. Then there is a natural injection $\mathcal{U} \to S(H_\infty, \pi^{*\infty})$. We shall refer to $\mathcal{U}$ as the unramified Selmer group.

Let V be the subgroup of $Y(H_\infty, \pi^{*\infty})$ defined by

$$V = \mathrm{Ker}\left(\mathrm{Hom}(T_{\pi^*}, \mathfrak{X}_\infty) \to \mathrm{Hom}(T_{\pi^*}, \mathcal{X}_\infty)\right),$$

and set

$$\mathfrak{W} = \mathrm{Ker}(\mathfrak{X}_\infty \to \mathcal{X}_\infty).$$

Proposition 5.2. *$V^{\perp} = \mathcal{U}$ and $\mathcal{U}^{\perp} = V$, with respect to the pairing* (5.1).

Proof. We first show that $\mathcal{U}^{\perp} = V$. Plainly $f \in V$ implies that $f \in \mathcal{U}^{\perp}$, and so $V \subseteq \mathcal{U}^{\perp}$. Suppose that $f \in \mathcal{U}^{\perp}$. Then $f_1(f(t)) = 0$ for all $f_1 \in \mathcal{U}$. Thus $f(t) \in \bigcap_{f_1 \in \mathcal{U}} \mathrm{Ker} f_1 = \mathfrak{W}$ and $\mathcal{U}^{\perp} = V$.

Next, observe that clearly $\mathcal{U} \subseteq V^{\perp}$. So suppose that $h \in V^{\perp}$. Then $h(f_2(t)) = 0$ for all $f_2 \in V$. However $\{f_2(t) \mid f_2 \in V\} = \mathfrak{W}$, and so h vanishes on $\mathfrak{B}$ i.e. $h \in \mathcal{U}$. Hence $V^{\perp} = \mathcal{U}$. □

Corollary 5.3. *There is a perfect duality*

$$\frac{S(H_\infty, \pi^{*\infty})}{\mathcal{U}} \times V \to D_{\mathfrak{p}^*}$$

and hence also a perfect duality

$$\left(\frac{S(H_\infty, \pi^{*\infty})}{\mathcal{U}}\right)_\Gamma \times V^\Gamma \to D_{\mathfrak{p}^*}. \quad \square$$

§ 6. Height pairings

Throughout this section we shall assume that $\text{Ш}(F)_p$ is finite. In [PR] B. Perrin-Riou defines an algebraic local height pairing

$$\{,\}_{F,\mathfrak{p}^*}: E(F) \otimes_{\mathfrak{O}_K} \mathfrak{O}_{K,\mathfrak{p}} \times E(F) \otimes_{\mathfrak{O}_K} \mathfrak{O}_{K,\mathfrak{p}^*} \to \mathbb{Q}_p.$$

It may be shown that this pairing is Δ-equivariant. In this section we shall always suppose that this pairing is non-degenerate modulo torsion. The main result of [PR] asserts that, with the above assumptions, a certain p-adic L-function $\mathcal{L}_{\mathfrak{p}^*}(E, s)$ attached to E/F, has a zero at $s = 1$ of order equal to $\mathrm{rank}_{\mathfrak{O}_K}(E(F))$ and satisfies a certain p-adic conjecture of Birch-Swinnerton-Dyer type.

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

$$0 \to \Sigma(F)^{(\pi^n)} \to S(F)^{(\pi^n)} \to \prod_{\mathfrak{q} \mid \mathfrak{p}^*} H^1(F_{\mathfrak{q}}, E_{\pi^n}).$$

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

$$E_{1,\mathfrak{p}^*} \otimes_{\mathfrak{O}_K} \mathfrak{O}_{K_\mathfrak{p}} \to \Sigma(F).$$

Lemma 6.1. *If* $|Ш(F)_\mathfrak{p}| < \infty$, *then* $E_{1,\mathfrak{p}^*} \otimes_{\mathfrak{O}_K} \mathfrak{O}_{K_\mathfrak{p}} = \Sigma(F)$.

Proof. See Corollaire 3.3 of [PR]. □

Let J_n denote the group of ideles of H_n, and write $U_n^{(\mathfrak{p}^*)}$ for the subgroup of unit ideles whose components at all places above $\mathfrak{p}^*$ are equal to 1. Define

$$\mathscr{C}_n = \frac{J_n}{H_n U_n^{(\mathfrak{p}^*)}}$$

and

$$W_n = \prod_{\mathfrak{q} | \mathfrak{p}^*} \mu_{p^n}(H_{n,\mathfrak{q}}).$$

It is shown in Proposition 3.13 of [PR] that there is an isomorphism

$$\eta_n^{-1} : \Sigma(F)^{(\pi^n)} \to \frac{\operatorname{Hom}(E_{\mathfrak{p}^{*n}}, \mathscr{C}_n)^{\Omega_F}}{\operatorname{Hom}(E_{\mathfrak{p}^{*n}}, W_n)^{\Omega_F}}. \tag{6.2}$$

Suppose that $Q \in E_{1,\mathfrak{p}^*}$, and write $\bar{Q}_n$ for the image of Q under the projection $E_{1,\mathfrak{p}^*} \to \Sigma(F)^{(\pi^n)}$. Then, by Corollary 4.10, we may associate a homomorphism $\mathfrak{d}_{n,Q} \in \operatorname{Hom}(E_{\mathfrak{p}^{*n}}, \operatorname{Cl}(\mathfrak{O}_{H_n}))^{\Omega_F}$ to the p.h.s. for $\mathfrak{B}_n$ afforded by $\bar{Q}_n$. It follows from the construction of η_n given on p. 385 of [PR] that

$$(c(\eta_n^{-1}(Q)(h))) = \mathfrak{d}_{n,Q}(h), \tag{6.3}$$

for all $h \in E_{\mathfrak{p}^{*n}}$, were c denotes idele content.

Let M_n be the maximal abelian pro-p extension of H_n which is unramified away from $\mathfrak{p}^*$, and set $\mathfrak{X}_n = \operatorname{Gal}(M_n/H_n)$. The global Artin reciprocity map yields a homomorphism

$$(-, M_n/H_n) : \mathscr{C}_n \to \mathfrak{X}_n.$$

Define

$$\gamma_n : \operatorname{Hom}(E_{\mathfrak{p}^{*n}}, \mathscr{C}_n)^\Gamma \to \operatorname{Hom}(E_{\mathfrak{p}^{*n}}, \mathfrak{X}_n)^\Gamma$$

by $\gamma_n(f) = (-, M_n/H_n) \circ f$, and

$$\bar{\tau}_n : \operatorname{Hom}(E_{\mathfrak{p}^{*n}}, \mathscr{C}_n)^\Gamma \to \operatorname{Hom}(E_{\mathfrak{p}^{*n}}, \mathscr{C}_n)^\Gamma$$

by $\bar{\tau}_n(f) = f \circ \tau_n$. (Recall that τ_n is the inverse of the automorphism of $E_{\mathfrak{p}^{*n}}$ given by π^n.) Then we have a homomorphism

$$\gamma_n \circ \bar{\tau}_n \circ \eta_n^{-1} : \Sigma(F)^{(\pi^n)} \to \operatorname{Hom}(E_{\mathfrak{p}^{*n}}, \mathfrak{X}_n)^\Gamma. \tag{6.4}$$

It is shown in § 3.2 of [PR] that we may take inverse limits of (6.4) and that this yields an isomorphism $\Sigma(F) \cong \operatorname{Hom}(T_{\pi^*}, \mathfrak{X}_\infty)^\Gamma$.

Let Φ' denote the composite homomorphism

$$(6.5) \qquad \Sigma(F) \xrightarrow{\sim} \operatorname{Hom}(T_{\pi^*}, \mathfrak{X}_\infty)^\Gamma \to \operatorname{Hom}(T_{\pi^*}, \mathscr{X}_\infty)^\Gamma$$

(where the right-hand arrow is the natural projection). Recall from § 5 that V denotes the orthogonal complement of the unramified Selmer group $\mathscr{U}$ with respect to the pairing afforded by Pontryagin duality.

Proposition 6.6. (a) $\operatorname{Ker}\Phi' \cong V^\Gamma$.

(b) *The following diagram commutes*:

$$\begin{tikzcd}
E_{1,\mathfrak{p}^*} \otimes_{\mathfrak{O}_K} \mathfrak{O}_{K,\mathfrak{p}} \arrow[r, equal] \arrow[d, "\phi'"] & \Sigma(F) \arrow[d, "\Phi'"] \\
\operatorname{Hom}(T_{\pi^*}, \varprojlim \operatorname{Cl}(\mathfrak{O}_{H_n}))^{\Omega_F} \arrow[r, "\sim"] & \operatorname{Hom}(T_{\pi^*}, \mathscr{X}_\infty)^{\Omega_F} .
\end{tikzcd}$$

Here ϕ' is the homomorphism defined in Corollary 4.14 *while the bottom arrow is induced by the Artin map.*

Proof. (a) Follows at once from the definition of ϕ' given in (6.5), and from the definition of V.

(b) This is immediate from (6.3) together with the definition of ϕ' given in Corollary 4.14. □

It follows from Proposition 6.6 that

$$\operatorname{Ker}\phi' = \operatorname{Ker}\Phi' = V^\Gamma .$$

Hence, in order to prove Theorem 1, we can now focus our attention on V^Γ.

Before stating the next result, we introduce some notation. We shall say that two $\mathbb{Z}_p$-modules, A, B are pseudo-isomorphic, 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 $\operatorname{rank}_{\mathbb{Z}_p}(A) = \operatorname{rank}_{\mathbb{Z}_p}(B)$, and so $A \sim B$ if and only if $B \sim A$. In the sequel $\hat{A}$ always denotes the Pontryagin dual of A.

We would like to thank Karl Rubin for showing us the following result.

Proposition 6.7 (Rubin).

$$(\hat{\mathscr{U}})^\Gamma \oplus \left(\frac{S(H_\infty, \pi^{*\infty})}{\mathscr{U}}\right)^{\wedge,\Gamma} \sim Y(H_\infty, \pi^{*\infty})^\Gamma .$$

Proof. The exact sequence

$$(6.8) \qquad 0 \to \mathscr{U} \to S(H_\infty, \pi^{*\infty}) \to \frac{S(H_\infty, \pi^{*\infty})}{\mathscr{U}} \to 0$$

yields

$$(6.9) \qquad 0 \to \left(\frac{S(H_\infty, \pi^{*\infty})}{\mathscr{U}}\right)^{\hat{}, \Gamma} \to Y(H_\infty, \pi^{*\infty})^\Gamma \to (\hat{\mathscr{U}})^\Gamma .$$

We claim that the right-hand arrow of (6.9) is surjective up to finite index. For suppose not. Then,

$$\operatorname{rank}_{Z_p}\left(\frac{S(H_\infty, \pi^{*\infty})}{\mathscr{U}}\right)^{\hat{}, \Gamma} + \operatorname{rank}_{Z_p}(\hat{\mathscr{U}})^\Gamma > \operatorname{rank}_{Z_p} Y(H_\infty, \pi^{*\infty})^\Gamma .$$

Theorem 3.2 of [PR] implies that

$$\begin{aligned} \operatorname{rank}_{Z_p} Y(H_\infty, \pi^{*\infty})^\Gamma &= \operatorname{rank}_{\mathfrak{O}_{K_{\mathfrak{p}^*}}}(E_{1,\mathfrak{p}^*}(F) \otimes_{\mathfrak{O}_K} \mathfrak{O}_{K_{\mathfrak{p}^*}}) \\ &= \operatorname{rank}_{\mathfrak{O}_K}(E(F)) \\ &= n , \end{aligned}$$

say.

Since Δ_1 is of order prime to p, taking Δ_1 invariants of (6.8) gives an exact sequence

$$(6.10) \qquad 0 \to \mathscr{U}^{\Delta_1} \to S(H_\infty, \pi^{*\infty})^{\Delta_1} \to \left(\frac{S(H_\infty, \pi^{*\infty})}{\mathscr{U}}\right)^{\Delta_1} \to 0 .$$

This implies

$$\begin{aligned} &\operatorname{rank}_{Z_p}(S(H_\infty, \pi^{*\infty})^{\Delta_1, \hat{}}) = \operatorname{rank}_{Z_p}(Y(H_\infty^{\Delta_1}, \pi^{*\infty})) \\ &= \operatorname{rank}_{Z_p}\left(\left(\frac{S(H_\infty, \pi^{*\infty})}{\mathscr{U}}\right)^{\Delta_1, \hat{}}\right) + \operatorname{rank}_{Z_p}(\mathscr{U}^{\Delta_1, \hat{}}) \\ &\geqq \operatorname{rank}_{Z_p}\left[\left(\frac{S(H_\infty, \pi^{*\infty})}{\mathscr{U}}\right)^{\Gamma_1 \times \Delta_1, \hat{}}\right] + \operatorname{rank}_{Z_p}(\mathscr{U}^{\Delta_1 \times \Gamma_1, \hat{}}) \\ &= \operatorname{rank}_{Z_p}\left[\left(\left(\frac{S(H_\infty, \pi^{*\infty})}{\mathscr{U}}\right)^{\hat{}}\right)_\Gamma\right] + \operatorname{rank}_{Z_p}(\hat{\mathscr{U}}_\Gamma) . \end{aligned}$$

Let M denote any $\mathbb{Z}_p[\![\Gamma]\!]$-module which is a finitely generated torsion module for the associated Iwasawa algebra. Then by standard theory

$$(6.11) \qquad \operatorname{rank}_{Z_p}(M^\Gamma) = \operatorname{rank}_{Z_p}(M_\Gamma) .$$

Since H_∞/K is abelian and since Leopoldt's conjecture is known to hold for abelian extensions of K, it follows that $S(H_\infty, \pi^{*\infty})$ is a finitely generated Λ-torsion module. (See § 2 of [C] for details.) Hence

$$\operatorname{rank}_{Z_p}(Y(H_\infty^{\Delta_1}, \pi^{*\infty})) \geqq \operatorname{rank}_{Z_p}\left[\left(\frac{S(H_\infty, \pi^{*\infty})}{\mathcal{U}}\right)^{\wedge, \Gamma}\right] + \operatorname{rank}_{Z_p}(\hat{\mathcal{U}}^\Gamma)$$

i.e.

$$> n, \quad \text{by the above}.$$

However $\operatorname{rank}_{Z_p}(Y(H_\infty^{\Delta_1}, \pi^{*\infty}))$ is equal to the order of vanishing of the p-adic L-function $\mathfrak{L}_{\mathfrak{p}^*}(E/F, s)$ at $s = 1$. It is shown in [PR] that this order of vanishing is equal to n when $|\text{Ш}(F)_{\mathfrak{p}^*}| < \infty$ and $\{,\}_{F, \mathfrak{p}^*}$ is non-degenerate modulo torsion. Thus we have obtained a contradiction, and so the result follows. □

Corollary 6.12. *Suppose that* $\chi \in \hat{\Delta}$. *Then,*

$$\left[\left(\frac{S(H_\infty, \pi^{*\infty})}{\mathcal{U}}\right)^{\wedge, \Gamma} \otimes_{\mathfrak{O}_{K_{\mathfrak{p}^*}}} \mathfrak{O}''\right]^\chi \oplus [(\hat{\mathcal{U}})^\Gamma \otimes_{\mathfrak{O}_{K_{\mathfrak{p}^*}}} \mathfrak{O}'']^\chi \sim [Y(H_\infty, \pi^{*\infty})^\Gamma \otimes_{\mathfrak{O}_{K_{\mathfrak{p}^*}}} \mathfrak{O}'']^\chi. \quad \square$$

We shall now introduce a certain subgroup $U(E, \mathfrak{p}^*)$ of $E(F) \otimes_{\mathfrak{O}_K} \mathfrak{O}_{K_{\mathfrak{p}^*}}$ which we shall call the group of unramified points of $E(F) \otimes_{\mathfrak{O}_K} \mathfrak{O}_{K_{\mathfrak{p}^*}}$.

Let $\chi_\infty : \Gamma \to \mathfrak{O}_{K_{\mathfrak{p}^*}}^\times$ be the character of Γ which gives the action of Γ on $E_{\mathfrak{p}^{*\infty}}$. Suppose that $T \in E(F) \otimes_{\mathfrak{O}_K} \mathfrak{O}_{K_{\mathfrak{p}^*}}$, and for each $n \in \mathbb{N}$, choose $T_n \in E(F)$ such that

$$T_n \equiv T(\operatorname{mod} \pi^{*n}(E(F) \otimes_{\mathfrak{O}_K} \mathfrak{O}_{K_{\mathfrak{p}^*}})).$$

Choose any $T_n' \in E(F^c)$ such that $\pi^{*n} T_n' = T_n$. We may define a homomorphism

$$h_n : \mathfrak{X}_\infty \to E_{\mathfrak{p}^{*\infty}}$$

by

$$h_n(\omega) = T_n'^{\omega} - T_n'.$$

We say that $T \in E(F) \otimes \mathfrak{O}_{K, \mathfrak{p}^*}$ is an unramified point if h_n vanishes on $\mathfrak{W}$ for all $n \in \mathbb{N}$. (Recall $\mathfrak{W} = \operatorname{Ker}(\mathfrak{X}_\infty \to \mathscr{X}_\infty)$.) We write $U(E, \mathfrak{p}^*)$ for the group of all such unramified points.

We shall now give another description of the group $U(E, \mathfrak{p}^*)$ up to pseudo-isomorphism. For each prime $\mathfrak{P}$ of F lying above $\mathfrak{p}^*$, write $E_1(F_{\mathfrak{P}})$ for the kernel of reduction of $E(F_{\mathfrak{P}})$. Set $\mathbb{E}_{1, \mathfrak{p}^*} = \prod_{\mathfrak{P} | \mathfrak{p}^*} E_1(F_{\mathfrak{P}})$. Then $E_1(F_{\mathfrak{P}})$ is an $\mathfrak{O}_{K_{\mathfrak{p}^*}}$-module, and so there is a natural homomorphism

$$f_{\mathfrak{P}} : E_{1, \mathfrak{p}^*}(F) \otimes_{\mathfrak{O}_K} \mathfrak{O}_{K_{\mathfrak{p}^*}} \to E_1(F_{\mathfrak{P}})$$

which induces a Δ-homomorphism

$$f = \prod_{\mathfrak{P} | \mathfrak{p}^*} f_{\mathfrak{P}} : E_{1, \mathfrak{p}^*}(F) \otimes_{\mathfrak{O}_K} \mathfrak{O}_{K_{\mathfrak{p}^*}} \to \mathbb{E}_{1, \mathfrak{p}^*}.$$

Proposition 6.13. (a) $\mathbb{E}_{1, \mathfrak{p}^*} \sim \mathfrak{O}_F \otimes_{\mathfrak{O}_K} \mathfrak{O}_{K_{\mathfrak{p}^*}}$.

(b) $\operatorname{Ker} f \sim U(E, \mathfrak{p}^*)$.

Proof. (a) This follows immediately from [Si], Chapter VII, Proposition 6.3.

(b) We shall show that $U(E, \mathfrak{p}^*) \cap (E_{1,\mathfrak{p}^*}(F) \otimes_{\mathfrak{O}_K} \mathfrak{O}_{K_{\mathfrak{p}^*}}) \sim \operatorname{Ker} f$. (This will suffice, since $[E(F) : E_{1,\mathfrak{p}^*}(F)] < \infty$.)

It is clear from the definitions that

$$\operatorname{Ker} f \subseteqq U(E, \mathfrak{p}^*) \cap E_{1,\mathfrak{p}^*}(F) \otimes_{\mathfrak{O}_K} \mathfrak{O}_{K_{\mathfrak{p}^*}}.$$

Suppose that $T \in E_{1,\mathfrak{p}^*}(F) \otimes_{\mathfrak{O}_K} \mathfrak{O}_{K_{\mathfrak{p}^*}}$. For each $n \in \mathbb{N}$ and $\mathfrak{P} \mid \mathfrak{p}^*$, let $H_{\infty,\mathfrak{P}}\left(\frac{1}{\pi^{*n}} f_{\mathfrak{P}}(T)\right)$ be the field obtained by adjoining π^{*n}th roots of $f_{\mathfrak{P}}(T)$ (taken with respect to the formal group law on E) to $H_{\infty,\mathfrak{P}}$. Then $T \in U(E, \mathfrak{p}^*)$ if and only if the extension $H_{\infty,\mathfrak{P}}\left(\frac{1}{\pi^{*n}} f_{\mathfrak{P}}(T)\right)\Big/ H_{\infty,\mathfrak{P}}$ is unramified for all $\mathfrak{P} \mid \mathfrak{p}^*$ and for all $n \in \mathbb{N}$. As we are only concerned with modules up to pseudo-isomorphism, we may assume that either $f_{\mathfrak{P}}(T) = 0$ or that $f_{\mathfrak{P}}(T)$ is of infinite order, for some $\mathfrak{P} \mid \mathfrak{p}^*$. However if $f_{\mathfrak{P}}(T)$ is of infinite order, then $H_{\infty,\mathfrak{P}}\left(\frac{1}{\pi^{*n}} f_{\mathfrak{P}}(T)\right)\Big/ H_{\infty,\mathfrak{P}}$ is non-trivial and ramified for all sufficiently large n (see [CW], Theorem 11), and so $T \notin U(E, \mathfrak{p}^*)$. The result follows. □

Proposition 6.14. *Suppose that $\chi \in \hat{\Delta}$, and write $\bar{\chi}$ for the contragredient character of χ. Then*

(a) $\operatorname{rank}_{\mathfrak{O}''} [Y(H_\infty, \pi^{*\infty})_\Gamma \otimes_{\mathfrak{O}_{K\mathfrak{p}^*}} \mathfrak{O}'']^\chi = \operatorname{rank}_{\mathfrak{O}''} (E(F) \otimes_{\mathfrak{O}_K} \mathfrak{O}'')^{\bar{\chi}}$.

(b) $\operatorname{rank}_{\mathfrak{O}''} [(\hat{\mathscr{U}})_\Gamma \otimes_{\mathfrak{O}_{K\mathfrak{p}^*}} \mathfrak{O}'']^\chi = \operatorname{rank}_{\mathfrak{O}''} (U(E, \mathfrak{p}^*) \otimes_{K_{\mathfrak{p}^*}} \mathfrak{O}'')^{\bar{\chi}}$.

Proof. Combining the standard exact sequence (see (24) in [C])

$$0 \to E(F) \otimes_{\mathfrak{O}_K} D_{\mathfrak{p}^*} \to S'(F, \pi^{*\infty}) \to Ш'(F)_{\mathfrak{p}^*} \to 0$$

with Theorem 5 (a) yields an exact sequence

$$0 \to E(F) \otimes_{\mathfrak{O}_K} D_{\mathfrak{p}^*} \to S(H_\infty, \pi^{*\infty})^\Gamma \to Ш'(F)_{\mathfrak{p}^*} \to 0. \tag{6.15}$$

From the very definition of $U(E, \mathfrak{p}^*)$, it is clear that

$$U(E, \mathfrak{p}^*) \otimes_{\mathfrak{O}_{K\mathfrak{p}^*}} D_{\mathfrak{p}^*} \subseteqq \mathscr{U}^\Gamma. \tag{6.16}$$

Next note that $|Ш'(F)_{\mathfrak{p}^*}| < \infty$ since we have assumed that $|Ш(F)_p| < \infty$. (See for instance Proposition 2 of [C].)

For an $\mathfrak{O}_{K,\mathfrak{p}^*}$-module M write $T(M) = \operatorname{Hom}(D_{\mathfrak{p}^*}, M)$ for the associated Tate module. Then from (6.15)

$$T(\mathscr{U}^\Gamma) \subseteqq T(S(H_\infty, \pi^{*\infty})^\Gamma) = T(E(F) \otimes D_{\mathfrak{p}^*}).$$

It therefore follows from the definition of $\mathcal{U}$ and $U(E, \mathfrak{p}^*)$ that

$$T(\mathcal{U}^\Gamma) \subset T(U(E, \mathfrak{p}^*) \otimes D_{\mathfrak{p}^*})$$

and so by (6.16) these two Tate modules coincide. Now $U(E, \mathfrak{p}^*) \otimes D_{\mathfrak{p}^*}$ and $\mathcal{U}^\Gamma$ are both isomorphic to $\mathfrak{O}_{K, \mathfrak{p}^*}$ modules of the form $D^r_{\mathfrak{p}^*} \oplus M_1$ with M_1 finite. We therefore deduce that

$$[\mathcal{U}^\Gamma : U(E, \mathfrak{p}^*) \otimes_{\mathfrak{O}_{K, \mathfrak{p}^*}} D_{\mathfrak{p}^*}] < \infty$$

and this immediately implies that

$$[U(E, \mathfrak{p}^*) \otimes_{\mathfrak{O}_{K, \mathfrak{p}^*}} D_{\mathfrak{p}^*}]^\wedge \sim \mathcal{U}^{\Gamma, \wedge}.$$

There are isomorphisms

$$(E(F) \otimes_{\mathfrak{O}_K} D_{\mathfrak{p}^*})^\wedge \cong \mathrm{Hom}(E(F) \otimes_{\mathfrak{O}_K} \mathfrak{O}_{K_{\mathfrak{p}^*}}, \mathfrak{O}_{K_{\mathfrak{p}^*}})$$

and

$$(U(E, \mathfrak{p}^*) \otimes D_{\mathfrak{p}^*})^\wedge \cong \mathrm{Hom}(U(E, \mathfrak{p}^*), \mathfrak{O}_{K_{\mathfrak{p}^*}}).$$

Also,

$$S(H_\infty, \pi^{*\infty})^{\Gamma, \wedge} = Y(H_\infty, \pi^{*\infty})_\Gamma$$

and

$$\mathcal{U}^{\Gamma, \wedge} = (\hat{\mathcal{U}})_\Gamma.$$

Piecing together the above yields

$$\mathrm{rank}_{\mathfrak{O}''} [Y(H_\infty, \pi^{*\infty})_\Gamma \otimes_{\mathfrak{O}_{K, \mathfrak{p}^*}} \mathfrak{O}'']^\chi = \mathrm{rank}_{\mathfrak{O}''} (E(F) \otimes_{\mathfrak{O}_K} \mathfrak{O}'')^{\bar{\chi}}$$

and

$$\mathrm{rank}_{\mathfrak{O}''} [(\hat{\mathcal{U}})_\Gamma \otimes_{\mathfrak{O}_{K, \mathfrak{p}^*}} \mathfrak{O}'']^\chi = \mathrm{rank}_{\mathfrak{O}''} (U(E, \mathfrak{p}^*) \otimes_{\mathfrak{O}_{K, \mathfrak{p}^*}} \mathfrak{O}'')^{\bar{\chi}},$$

as asserted. □

Theorem 5. *For each $\chi \in \hat{\Delta}$, set*

$$r_\chi = \mathrm{rank}_{\mathfrak{O}'} (E(F) \otimes_{\mathfrak{O}_K} \mathfrak{O}')^\chi$$

and

$$r^*_\chi = \mathrm{rank}_{\mathfrak{O}''} (E(F) \otimes_{\mathfrak{O}_K} \mathfrak{O}'')^\chi.$$

Suppose that $r_\chi \geqq 1$. Then

$$\mathrm{rank}_{\mathfrak{O}''} [Y(H_\infty, \pi^{*\infty})^\Gamma \otimes_{\mathfrak{O}_{K\mathfrak{p}^*}} \mathfrak{O}'']^\chi = 1 + \mathrm{rank}_{\mathfrak{O}''} [(\hat{\mathcal{U}})^\Gamma \otimes_{\mathfrak{O}_{K\mathfrak{p}^*}} \mathfrak{O}'']^\chi.$$

We note that Theorem 1 is an immediate consequence of Theorem 5 and 6.6 together with Corollaries 5.3 and 6.12.

The next part of this section will be devoted to giving a proof of Theorem 5. First we show

Proposition 6.17. *Suppose that $\chi \in \hat{\Delta}$ with $r_\chi^* \geqq 1$. Then*

$$\operatorname{rank}_{\mathfrak{O}''}(U(E, \mathfrak{p}^*) \otimes_{\mathfrak{O}_{K_{\mathfrak{p}^*}}} \mathfrak{O}'')^\chi = \operatorname{rank}_{\mathfrak{O}''}(\operatorname{Ker} f \otimes_{\mathfrak{O}_{K_{\mathfrak{p}^*}}} \mathfrak{O}'')^\chi = r_\chi^* - 1 .$$

Proof. The first equality follows at once from Proposition 6.13 (b), and so we shall just prove the second.

Let $\{\chi_1 = \chi, \ldots, \chi_m\}$ be the set of all characters in $\hat{\Delta}$ lying in the Ω_K-orbit of χ. Then $r_{\chi_j}^* = r_\chi^* \geqq 1$ for all $1 \leqq j \leqq m$, and so we deduce that $E(F) \cap \left(\bigoplus_{j=1}^{m} (E_1(F) \otimes_{\mathfrak{O}_K} \mathfrak{O}'')^{\chi_j} \right)$ contains a point Q of infinite order. Since f is a Δ-homomorphism and $f(Q)$ is of infinite order, we deduce that $\prod_{j=1}^{m} (\operatorname{Im} f \otimes_{\mathfrak{O}_{K_{\mathfrak{p}^*}}} \mathfrak{O}'')^{\chi_j}$ has $\mathfrak{O}''$-rank at least 1. But this implies that

$$s_{\chi_j} = \operatorname{rank}_{\mathfrak{O}''}(\operatorname{Im} f \otimes_{\mathfrak{O}_{K_{\mathfrak{p}^*}}} \mathfrak{O}'')^{\chi_j} \geqq 1 ,$$

since $s_{\chi_j} = s_\chi$, for all $1 \leqq j \leqq m$. However, it follows immediately from Proposition 6.13 (a) that $s_\chi = 1$, and this implies the result. □

From the existence of the height pairing $\{,\}_{F, \mathfrak{p}^*}$ together with the fact that

$$[E(F) : E_1(F)] < \infty ,$$

it follows that

$$r_\chi^* = r_{\bar{\chi}} . \tag{6.18}$$

Using (6.11), together with 6.13, 6.14, 6.17 and (6.18), then gives Theorem 5. This also completes the proof of Theorem 1.

Remark. One can use the localisation map f to give an alternative characterisation of $\ker \phi$. Using the definition of the height pairing

$$\{,\} : E(F) \otimes_{\mathfrak{O}_K} \mathfrak{O}_{K,\mathfrak{p}} \times E(F) \otimes_{\mathfrak{O}_K} \mathfrak{O}_{K,\mathfrak{p}^*} \to \mathbb{Q}_p$$

together with the above work, one easily shows that $\ker \phi \sim \ker f^\perp$. (For further details see [A2].)

We conclude this section by proving Theorem 2. By the remark after 4.14 we know that $\operatorname{Im} \phi \cong \operatorname{Im} \phi'$, and by 6.6 $\operatorname{Im} \phi' \cong \operatorname{Im} \Phi'$.

Thus, by (6.5), it will suffice to show that the map

$$\operatorname{Hom}(T_{\pi^*}, \mathscr{X}_\infty)^\Gamma \xrightarrow{b} \operatorname{Hom}(T_{\pi^*}, \mathscr{X}_\infty)^\Gamma$$

has finite cokernel. By the very definition of V (given prior to 5.2),

$$0 \to V \to \operatorname{Hom}(T_{\pi^*}, \mathscr{X}_\infty) \to \operatorname{Hom}(T_{\pi^*}, \mathscr{X}_\infty) \to 0 .$$

Taking Γ-fixed points and Pontryagin duals, and then using both 5.3 and Theorem 4, we obtain an exact sequence:

$$[\mathrm{Hom}\,(T_{\pi^*}, \mathscr{X}_\infty)\hat{}\,]_\Gamma \xrightarrow{\hat{b}} S(H_\infty, \pi^{*\infty})_\Gamma \to \left(\frac{S(H_\infty, \pi^{*\infty})}{\mathscr{U}}\right)_\Gamma \to 0\,.$$

Reasoning as per Theorem 4(b), $\mathscr{U}\,(=\mathrm{Hom}\,(\mathscr{X}_\infty, E_{\mathfrak{p}^*_\infty}))$ identifies as the Pontryagin dual of $\mathrm{Hom}\,(T_{\pi^*}, \mathscr{X}_\infty)$. Therefore 6.7, together with (6.11), then shows that $\mathrm{Ker}\,\hat{b} \sim 0$, as required.

§ 7. Kummer theory of principal homogeneous spaces

The remainder of this article will be devoted to the proof of Theorem 3; so from now on we assume $\mathfrak{p}^*$ to be completely split in F/K, and that F is linearly disjoint with $K(E_{p^\infty})$ over K. The splitting condition on $\mathfrak{p}^*$ will only be needed for the proof of Proposition 7.9 and Lemma 7.10.

Throughout this section, we suppose that n is fixed and we set $N = H_n \cdot F_n$.

Write $\mathfrak{B}_n = \mathfrak{B} \otimes_{\mathfrak{O}_F} \mathfrak{O}_N$; then $\mathfrak{B}_N$ is an $\mathfrak{O}_N$-order in $B_N = B \underset{F}{\otimes} N = \mathrm{Map}\,(G, N)$. Recall from § 3 that $PH(\mathfrak{B})$ (resp. $PH(B)$) denotes the group of isomorphism classes of principal homogeneous spaces of $\mathfrak{B}/\mathfrak{O}_F$ (resp. B/F). We use similar notation for $\mathfrak{B}_N$ and B_N.

If follows from standard theory (see e.g. [BT]) that there are isomorphisms

$$PH(B) \cong H^1(F, G)$$

and

$$PH(B_N) \cong H^1(N, G) = \mathrm{Hom}\,(\Omega_N, G)\,.$$

It may also be shown via a simple cohomological argument that the natural map

$$PH(\mathfrak{B}) \to PH(B)\,,$$
$$\mathfrak{C} \mapsto \mathfrak{C} \otimes_{\mathfrak{O}_F} F$$

is injective. A similar result holds if $\mathfrak{B}$ (resp. B) is replaced by $\mathfrak{B}_N$ (resp. B_N).

We set $\Lambda = \mathrm{Gal}\,(N/F_n)$, and $\Gamma' = \mathrm{Gal}\,(N/H_n)$.

Lemma 7.1. (a) $H^i(\Gamma' \times \Lambda, G) = \{1\}$ *for* $i = 1, 2$.

(b) *The natural restriction map*

$$\mathrm{Res}\colon H^1(F, G) \to H^1(N, G)^{\Gamma' \times \Lambda}$$

on cohomology groups is an injection.

(c) *The natural map*

$$PH(\mathfrak{B}) \to PH(\mathfrak{B}_N),$$
$$\mathfrak{C} \mapsto \mathfrak{C} \underset{\mathfrak{O}_F}{\otimes} \mathfrak{O}_N$$

is an injection.

Proof. (a) We first consider the case $i = 1$. From the restriction-inflation exact sequence of cohomology groups, we obtain

$$1 \to H^1(\Lambda, G^{\Gamma'}) \to H^1(\Gamma' \times \Lambda, G) \to H^1(\Gamma', G).$$

As $G^{\Gamma'} = \{1\}$, it follows that $H^1(\Lambda, G^{\Gamma'}) = \{1\}$. Since Γ' is cyclic we know that

$$|H^1(\Gamma', G)| = |\hat{H}^0(\Gamma', G)| = \left|\frac{G^{\Gamma'}}{N_{\Gamma'} G}\right| = 1,$$

where here $N_{\Gamma'} = \sum_{\gamma \in \Gamma'} \gamma$. This shows that $H^1(\Gamma' \times \Lambda, G) = \{1\}$.

For the corresponding result for $H^2(\Gamma' \times \Lambda, G)$, we argue as above, applying Proposition 5 of [CF], p. 101.

(b) This follows from the above and Proposition 3 of Chapter VII of [S].

(c) This follows from the diagram

$$\begin{tikzcd}
1 \arrow[r] & H^1(\Gamma' \times \Lambda, G) \arrow[r] & H^1(F, G) \arrow[r, "\mathrm{Res}"] & H^1(N, G) \\
 & & PH(\mathfrak{B}) \arrow[r] \arrow[u, hook] & PH(\mathfrak{B}_N) \arrow[u, hook]
\end{tikzcd}$$

. □

Lemma 7.2. *For brevity write H in place of H_n; then*

$$(N^\times / N^{\times q})^{\Gamma'} \cong H^\times / H^{\times q}.$$

Proof. Consider the exact Kummer sequence

$$1 \to \mu_q \to N^\times \to N^{\times q} \to 1,$$
$$x \mapsto x^q.$$

Taking Γ'-fixed points yields the long exact sequence

$$1 \to 1 \to H^\times \to N^{\times q} \cap H^\times \to H^1(\Gamma', \mu_q) \to H^1(\Gamma', N^\times)$$
$$\to H^1(\Gamma', N^{\times q}) \to H^2(\Gamma', \mu_q).$$

Via an argument similar to that of Proposition 8.1 (a) we have that

$$H^1(\Gamma', \mu_q) = H^2(\Gamma', \mu_q) = \{1\},$$

and by Hilbert's Theorem 90,

$$H^1(\Gamma', N^\times) = \{1\}.$$

This shows that

(a) $N^{\times q} \cap H^\times = H^{\times q}$, and

(b) $H^1(\Gamma', N^{\times q}) = \{1\}$.

Next consider the Γ'-fixed points of the sequence

$$1 \to N^{\times q} \to N^\times \to N^\times / N^{\times q} \to 1;$$

this yields

$$1 \to (N^{\times q})^{\Gamma'} \to H^\times \to (N^\times / N^{\times q})^{\Gamma'} \to H^1(\Gamma', N^{\times q}).$$

It follows at once from (a) that

$$(N^{\times q})^{\Gamma'} = N^{\times q} \cap H^\times = H^{\times q},$$

and now using (b), we deduce that

$$H^\times / H^{\times q} \cong (N^\times / N^{\times q})^{\Gamma'},$$

as asserted. □

Proposition 7.3. *There are isomorphisms*

$$H^1(N, G)^{\Gamma' \times \Delta} \cong [H^1(N, \mu_q)^{\Gamma'}]^\varepsilon \cong [(N^\times / N^{\times q})^{\Gamma'}]^\varepsilon \cong (H^\times / H^{\times q})^\varepsilon,$$

where ε is the character of Δ giving the action of Δ on $E_{\mathfrak{p}^{*n}}$.

Proof. Let P be a generator of $E_{\mathfrak{p}^{*n}}$, and let $\chi : G \to \mu_q$ be the corresponding faithful character of G afforded by the Weil pairing. Then χ induces an isomorphism $H^1(N, G) \cong H^1(N, \mu_q)$.

Now suppose that $f \in H^1(N, G)^{\Gamma' \times \Delta} = \operatorname{Hom}(\Omega_N, G)^{\Gamma' \times \Delta}$; then for $\gamma \in \Gamma' \times \Delta$ and $\omega \in \Omega_N$ we have

$$\begin{aligned}\chi(f(\omega^{\gamma^{-1}}))^\gamma = W_n(f(\omega)^{\gamma^{-1}}, P)^\gamma = W_n(f(\omega), P^\gamma)\\ = \chi(f(\omega))^{\varepsilon(\gamma)}.\end{aligned}$$

Hence χ induces an injection

$$H^1(N, G)^{\Gamma' \times \Delta} \to [H^1(N, \mu_q)^{\Gamma'}]^\varepsilon;$$

that this injection is also surjective follows from the fact that the Weil pairing W_n is Ω_F-equivariant.

The isomorphism $[H^1(N, \mu_q)^{\Gamma'}]^\varepsilon \cong [(N^\times/N^{\times q})^{\Gamma'}]^\varepsilon$ comes from the Ω_F-equivariant Kummer pairing

$$\Omega_N \times N^\times/N^{\times q} \to \mu_q .$$

The final isomorphism $[(N^\times/N^{\times q})^{\Gamma'}]^\varepsilon \cong (H^\times/H^{\times q})^\varepsilon$ follows immediately from Lemma 7.2. □

Before proving the next result, we recall some elementary facts concerning the Galois theory of principal homogeneous spaces (see [T4]). Fix a faithful character χ of G. Recall that we have an isomorphism

$$(7.4) \qquad N^\times/N^{\times q} \cong PH(B_N) .$$

Explicitly, this is induced by the map

$$n \mapsto C = \frac{N[X]}{(X^q - n)}, \quad n \in N^\times ,$$

where G acts on the algebra $N[X]/(X^q - n)$ via the rule $X^g = \chi(g)X$. By standard Galois theory, the inverse of this map is the homomorphism

$$\theta_N : PH(B_N) \to N^\times/N^{\times q},$$
$$C \mapsto \chi(r_C(c)^q),$$

where $r_C(c)$ is the resolvend of a normal basis element c of C. Let G act on $C[G]$ via Galois action on the coefficients C; then, of course $C[G]^G = N[G]$. In order to show that $r_C(c)^q \in N[G]^\times$ (and hence $\chi(r_C(c)^q) \in N^\times$), it suffices to show that $r_C(c)^q$ is G-fixed. However, this follows at once from the standard G-action formula for $h \in G$:

$$\begin{aligned} r_C(c)^h &= \sum_{g \in G} c^{gh} g^{-1} = \sum_{g \in G} c^{gh} g^{-1} h^{-1} h \\ &= r_C(c)\, h . \end{aligned}$$

We now give a similar result for $PH(B)$.

Proposition 7.5. *The following diagram commutes*:

$$\begin{tikzcd} PH(B_N) \arrow[r, "\theta_N"'] & N^\times/N^{\times q} \\ PH(B) \arrow[u, hook] \arrow[r, "\theta_F"'] & H_n^\times/H_n^{\times q} \arrow[u, hook] \end{tikzcd} .$$

Here θ_F is defined as follows: if C is a p.h.s. *for B and if $C = c \cdot A$, then $\theta_F(C)$ is represented by $\chi(r_C(c)^q)$.*

Proof. We adopt the notation given prior to Proposition 4.5. To prove that the diagram commutes, it suffices to show that $r_C(c)^q \in A$. Now $r_C(c) \in C \underset{F}{\otimes} F_n[G]$ and we know that $C \underset{F}{\otimes} F_n$ is a Galois algebra over F with Galois group $\Xi = \Gamma' \ltimes G$, where $\Gamma' = \mathrm{Gal}(F_n/F)$. We let Ξ act on $C \underset{F}{\otimes} F_n[G]$ by Galois action on the coefficients and by the rule that for $(\gamma, h) \in \Gamma' \ltimes G$, $g^{(\gamma, h)} = g^\gamma$ $(= \gamma(g)$ as explained in § 4). Then the fixed point algebra

$$(C \underset{F}{\otimes} F_n[G])^{\Gamma' \ltimes G} = (F_n[G])^{\Gamma'} = A$$

and so it will suffice to show that for $\omega \in \Xi$

$$r_C(c)^\omega = r_C(c)h \quad \text{for some } h \in G\,.$$

Note that, on applying the endomorphism $[m]$ of $C \otimes F_n[G]$ induced by $g \mapsto g^m$, we shall have also proved Lemma 4.15.

Write $\omega = (\gamma, h)$. Then

$$\begin{aligned} r_C(c)^\omega = \sum_{g \in G} c^{g\omega} g^{-\omega} &= \sum c^{\omega g^\omega} g^{-\omega} \\ &= \sum c^{hg^\omega} g^{-\omega} \\ &= \sum c^{hg^\omega} g^{-\omega} h^{-1} h \\ &= r_C(c)h\,. \quad \square \end{aligned}$$

There is also a local version of Proposition 7.5. For each prime $\mathscr{P}$ of F, we have an isomorphism

$$N_{\mathscr{P}}^\times / N_{\mathscr{P}}^{\times q} \cong PH(B_{N,\mathscr{P}})$$

together with a map

$$\theta_{N_{\mathscr{P}}} : PH(B_{N,\mathscr{P}}) \xrightarrow{\sim} N_{\mathscr{P}}^\times / N_{\mathscr{P}}^{\times q}\,;$$

these are defined as in the global case. Then we have

Proposition 7.5′. *The following diagram commutes:*

$$\begin{tikzcd} PH(B_{N,\mathscr{P}}) \arrow[r, "\theta_N"] & N_{\mathscr{P}}^\times / N_{\mathscr{P}}^{\times q} \\ PH(B_{\mathscr{P}}) \arrow[u, hook] \arrow[r, "\theta_{F_{\mathscr{P}}}"'] & H_{n,\mathscr{P}}^\times / H_{n,\mathscr{P}}^{\times q} \arrow[u, hook] \end{tikzcd}\ .$$

Proof. As per Proposition 7.5. □

We now define $PH_{\mathfrak{p}^*}(\mathfrak{B})$ to be the subgroup of $PH(\mathfrak{B})$ consisting of all principal homogeneous spaces of $\mathfrak{B}$ which are trivial at all primes of F lying over $\mathfrak{p}^*$. Thus $\mathfrak{C} \in PH(\mathfrak{B})$ lies in $PH_{\mathfrak{p}^*}(\mathfrak{B})$ if and only if

$$\mathfrak{C} \otimes_{\mathfrak{O}_F} \mathfrak{O}_{F,\mathfrak{p}^*} \cong \mathfrak{B} \otimes_{\mathfrak{O}_F} \mathfrak{O}_{F,\mathfrak{p}^*} .$$

We define a subgroup $PH_{\mathfrak{p}^*}(B)$ of $PH(B)$ etc. in a similar manner. Note that, as the endomorphism π of E acts as an automorphism when restricted to the local points $E_{1,\mathfrak{p}^*}(F_{\mathscr{P}})$, the natural homomorphism

$$E(F) \to PH(\mathfrak{B})$$

of § 3 induces a homomorphism

$$E_{1,\mathfrak{p}^*} \to PH_{\mathfrak{p}^*}(\mathfrak{B}) .$$

Suppose now that $\mathfrak{C} \in PH(\mathfrak{B}_N)$, with $\mathfrak{C}\mathfrak{M}_N = c \cdot \mathfrak{M}_N$, where $\mathfrak{M}_N$ denotes the maximal order of A_N. Then it follows from Lemma 4.6(b) that $\pi^{-n} r(c)$ is a unit in the maximal order of $C[G]$. Hence, this shows that

$$\text{(7.7)(a)} \qquad \theta_N(\operatorname{Ker} \phi_n^{(N)}) \subset \frac{\mathfrak{O}_N^\times N^{\times q}}{N^{\times q}} \cong \frac{\mathfrak{O}_N^\times}{\mathfrak{O}_N^{\times q}} .$$

Identical reasoning shows that

$$\text{(7.7)(b)} \qquad \theta_F(\operatorname{Ker} \phi_n) \subset \frac{\mathfrak{O}_{H_n}^\times H_n^{\times q}}{H_n^{\times q}} \cong \frac{\mathfrak{O}_{H_n}^\times}{\mathfrak{O}_{H_n}^{\times q}} .$$

We next claim that a p.h.s. C lies in $PH_{\mathfrak{p}^*}(B_N)$ (resp. $PH_{\mathfrak{p}^*}(B)$) if and only if a representative of $\theta_N(C)$ (resp. of $\theta_F(C)$) is a local q^{th} power at primes above $\mathfrak{p}^*$. It is clear that the assertion holds for B_N, since for each prime $\mathscr{P}$ of N over $\mathfrak{p}^*$, we have the Kummer isomorphism

$$PH(B_{N,\mathscr{P}}) \cong N_{\mathscr{P}}^\times / N_{\mathscr{P}}^{\times q} .$$

For B the result follows from the diagram

$$\text{(7.8)} \qquad \begin{tikzcd} PH(B) \arrow[r, hook, "\theta_F"] \arrow[d] & H_n^\times / H_n^{\times q} \arrow[d] \\ \prod\limits_{\mathfrak{P} | \mathfrak{p}^*} PH(B_{\mathfrak{P}}) \arrow[r, hook, "\prod\limits_{\theta_{F_{\mathfrak{P}}}}"'] & \prod\limits_{\mathfrak{P} | \mathfrak{p}^*} H_{n,\mathfrak{P}}^\times / H_{n,\mathfrak{P}}^{\times q} \end{tikzcd}$$

From this, together with (7.7) and Proposition 7.3, we shall now show

Proposition 7.9. *Let $\mathfrak{M}$ denote the maximal order in A and for an abelian group Y, let Y_{p^n} denote the subgroup of elements annihilated by p^n. There is a natural injection*

$$\tilde{\theta}_n : \operatorname{Ker} \phi_n \to (\mathfrak{O}_{H_n,\mathfrak{p}^*}^\times / \mathfrak{O}_{H_n}^\times)_{p^n}^{\varepsilon} .$$

Proof. The injection is defined as follows: consider the isomorphism

$$\frac{\mathfrak{O}^{\times}_{H_{n,\mathfrak{p}^*}}}{\mathfrak{O}^{\times}_{H_n}} \cong \frac{\left(\prod\limits_{\mathfrak{P}|\mathfrak{p}^*} \mathfrak{O}^{\times}_{H_{n,\mathfrak{P}}}\right)}{\mathfrak{O}^{\times}_{H_n}}$$

and suppose that $\mathfrak{C} \in \operatorname{Ker} \phi_n$ with $\mathfrak{C}\mathfrak{M} = c \cdot \mathfrak{M}$. Then $\mathfrak{C}$ is mapped to the class whose representative in $\mathfrak{O}^{\times}_{H_{n,\mathfrak{p}}}$ is given by the unique qth root in $H^{\times}_{n,\mathfrak{P}}$ of $\chi(r(c)^q)$. The uniqueness of the root follows from the first part of:

Lemma 7.10. (a) $\mu_q(H_{n,\mathfrak{P}}) = 1$.

(b) *Let f denote the Frobenius automorphism of $\mathfrak{p}^*$ in $N/F(\mu_q)$. Then $\varepsilon(f) \not\equiv 1 \bmod (p)$.*

Proof. (a) Since $\mathfrak{p}^*$ is totally ramified in H_n/F and totally split in F/K, it follows that $H_{n,\mathfrak{P}}$ has residue classfield $\mathbb{F}_p$. As p is not anomalous, $E_p(\mathbb{F}_p) = 1$, and so $E_\pi(H_{n,\mathfrak{P}}) = 1$. Therefore, by the Weil pairing, it follows that $H_{n,\mathfrak{P}}$ has no non-trivial pth roots of unity.

(b) Suppose for contradiction that $\varepsilon(f) \equiv 1 \bmod (p)$. Then f fixes both μ_p and E_{π^*}; hence, by the Weil pairing, f fixes E_π. This would then imply $|E_p(\mathbb{F}_p)| > 1$ which would contradict p being non-anomalous. □

§ 8. Galois action

In this section we establish a number of results describing the action of Galois groups on various resolvents. As in the previous section n is fixed and we therefore write G, A, $\mathfrak{A}$ etc. We again put $N = H_n \cdot F_n$, and we set $L_i = F_n \cdot H_i = F_n(\zeta_{p^i})$.

Since F and $K(E_{p^\infty})$ are linearly disjoint over K, by 2.2(b) we have decompositions

$$(8.1)\text{(a)} \qquad A = \bigoplus_{i=0}^{n} H_i, \quad B = \bigoplus_{i=0}^{n} F_i\,.$$

Tensoring the first decomposition by F_n gives

$$(8.1)\text{(b)} \qquad F_n[G] = \bigoplus_{i=0}^{n} L_i\,.$$

Let $\{\chi_i\}_{i=0}^{n}$ denote a sequence of abelian characters of G such that χ_i has order p^i and $\chi_{i+1}^p = \chi_i$. Then, by the convention stated after 2.2, we may assume the decompositions of A and $F_n[G]$ to be induced by $\bigoplus\limits_{i=0}^{n} \chi_i$.

For each i with $0 \leqq i < n$, we let $N_{n/i}: H_n^\times \to H_i^\times$ be the norm map. Using the decomposition (8.1)(a), we define the norm operator

$$(8.2) \qquad \sigma: H_n^\times \to A \quad \text{by} \quad \sigma(x) = \bigoplus_{i=0}^{n} N_{n/i}(x)\,.$$

More generally, for any finite dimensional commutative F-algebra R, we write

$$\sigma_R : (H_n \underset{F}{\otimes} R)^\times \rightarrow (A \underset{F}{\otimes} R)^\times$$

for the norm operator induced by the norm maps $H_n \underset{F}{\otimes} R \rightarrow H_i \underset{F}{\otimes} R$. Fix a p.h.s. C for B. Choose $c \in C$ with $C = c \cdot A$, and write $r(c)$ for $r_C(c)$. Recall that $C \underset{F}{\otimes} N/F$ is a Galois algebra with Galois group $\Xi = \Omega \ltimes G$ where $\Omega = \mathrm{Gal}(N/F)$. The first of our Galois action formulae concerns the Lagrange resolvent $\chi(r(c))$:

Lemma 8.3. *Let $\chi \in \hat{G}$ and $\xi = \omega \cdot g \in \Xi$ with $\omega \in \Omega$, $g \in G$. Then*

$$\chi(r(c))^\xi = \chi^{\kappa_1(\omega)}(r(c))\, \chi^{\kappa_1(\omega)}(g)$$

where κ_1 denotes the character giving the action of Ω on G^*.

Proof. Suppose $P \in G^*$ is such that $\chi(g) = W_n(g, P)$ for all $g \in G$. Then

$$\begin{aligned}\chi(r(c))^\xi &= \Big(\sum_{h \in G} c^h W_n(-h, P)\Big)^\xi \\ &= \sum_h c^{h\omega g} W_n(-h^\omega, P^\omega) \\ &= \sum c^{\omega h^\omega g} W_n(-h^\omega, \kappa_1(\omega) P) \\ &= \chi^{\kappa_1(\omega)}(r(c) \cdot g) \quad \text{as } c = c^\omega. \quad \square\end{aligned}$$

We can now use this result to study Galois action on the components of $\sigma(\chi_n(r(c)))$ under the decomposition (8.1)(a); we shall then be able to conclude that

Proposition 8.4.

$$\sigma(\chi_n(r(c)))\, r(c)^{-1} \in A^\times .$$

Proof. From (8.1)(a) we see that it suffices to show that

$$\chi_i(\sigma(\chi_n(r(c)))\, r(c)^{-1}) \in H_i^\times .$$

Thus by the very definition of σ this amounts to showing

$$N_{n/i}(\chi_n(r(c)))\, \chi_i(r(c))^{-1} \in H_i^\times . \tag{8.5}$$

With this in view we let Ξ_i denote the subgroup of Ξ which fixes $H_i = F \underset{F}{\otimes} H_i \subset C \otimes N$. For $\xi = \omega g \in \Xi_i$, we know that ω fixes G_i^*; hence $\kappa_1(\omega) \equiv 1 \bmod (p^i)$, and so by 8.3

$$\chi_i(r(c))^\xi = \chi_i(r(c))\, \chi_i(g) . \tag{8.6}$$

Therefore, in order to establish (8.5), it will be enough to show

$$N_{n/i}(\chi_n(r(c)))^\xi = N_{n/i}(\chi_n(r(c)))\,\chi_i(g)\,. \tag{8.7}$$

Since $(C \underset{F}{\otimes} L_n)/(C \underset{F}{\otimes} L_i)$ is generated by μ_q, we have

$$N_{n/i}(\chi_n(r(c))) = \prod_{\substack{m \bmod p^n Z \\ m \equiv 1 \bmod (p^i)}} \chi_n^m(r(c))\,. \tag{8.8}$$

Thus, by 8.3, for $\xi = \omega g \in \Xi_i$

$$\begin{aligned} N_{n/i}(\chi_n(r(c)))^\xi &= \prod_m{}' \chi_n^m(r(c))^\xi \\ &= \prod_m{}' \chi_n^{m\kappa_1(\omega)}(r(c)) \prod_m{}' \chi_n^m(g)\,. \end{aligned}$$

But, because $\kappa_1(\omega) \equiv 1 \bmod (p^i)$, $m \mapsto m\kappa_1(\omega)$ is just a permutation of the exponents m of χ_n, and so finally we have shown

$$\begin{aligned} N_{n/i}(\chi_n(r(c)))^\xi &= N_{n/i}(\chi_n(r(c))) \prod_m{}' \chi_n^m(g) \\ &= N_{n/i}(\chi_n(r(c)))\,\chi_n^{p^{n-i}}(g)\,. \end{aligned}$$

This then proves (8.7) since $\chi_n^{p^{n-i}} = \chi_i$. □

§ 9. Local group rings

We keep the notation of the previous section. Let $f \in \mathrm{Gal}(N/F(\mu_q))$ denote the Frobenius automorphism for the primes of $F(\mu_q)$ above $\mathfrak{p}^*$. Because $\mathfrak{p}^*$ is completely split in F/K and is non-ramified in F_n/F, we note that for all $x \in \mathfrak{O}_{F_n}$

$$x^f \equiv x^p \bmod \mathfrak{p}^*\,. \tag{9.1}$$

We abuse notation slightly and also write f for the F automorphism of $B_n = \mathrm{Map}(G, N)$ given by the valuewise action of f, i.e. for $b \in B_n$ and $g \in G$

$$(b^f)(g) = (b(g))^f\,. \tag{9.2}$$

Lemma 9.3. *f commutes with the action of Ξ. (Here we regard Ξ as a Galois group of the Galois algebra B_N/F.)*

Proof. Let $\xi = \omega \cdot g \in \Xi$. Then for $b \in B$, $h \in G$:

$$\begin{aligned} b^{\xi f}(h) &= (b^{\omega g}(h))^f = (b^{\omega}(h-g))^f \\ &= b\big((h-g)^{\omega^{-1}}\big)^{\omega f}, \\ b^{f\xi}(h) &= b^{f\omega}(h-g) = (b^f((h-g)^{\omega^{-1}}))^{\omega} \\ &= b\big((h-g)^{\omega^{-1}}\big)^{f\omega}. \end{aligned}$$

The result follows as $\omega f = f\omega$, since N/F is abelian. □

We shall now extend this valuewise Frobenius to the semi-local algebra $C_{\mathfrak{p}^*}$ for any $C \subset PH_{\mathfrak{p}^*}(\mathfrak{B}_n)$. Indeed, by the very definition of $PH_{\mathfrak{p}^*}(\mathfrak{B}_n)$ in §7, we have the triviality condition at $\mathfrak{p}^*$:

$$C \underset{K}{\otimes} K_{\mathfrak{p}^*} \cong B \underset{K}{\otimes} K_{\mathfrak{p}^*}.$$

So, tensoring by N and writing $C_N = C \underset{F}{\otimes} N$, we have an isomorphism of $(G, N_{\mathfrak{p}^*})$ algebras:

$$C_N \underset{K}{\otimes} K_{\mathfrak{p}^*} \cong B_N \underset{K}{\otimes} K_{\mathfrak{p}^*}$$

and therefore we obtain an automorphism of $C_N \otimes K_{\mathfrak{p}^*}$ which we again denote by f. A priori f depends on the above choice of isomorphism; however, for each prime $\mathfrak{P}$ of N above $\mathfrak{p}^*$ the isomorphism $C_{N,\mathfrak{P}} \cong B_{N,\mathfrak{P}}$ is unique up to an element of $\mathrm{Aut}_{N_{\mathfrak{P}}}(B_{N,\mathfrak{P}}) = G$, and from 9.3 we know that f commutes with the action of G. We therefore conclude that the valuewise Frobenius automorphism of $C_{N,\mathfrak{p}^*}$ is uniquely defined.

The remainder of this section is devoted to various character value congruences for local group rings. The basic such congruences from which we derive all others is

Proposition 9.4. (a) *Let $\chi \in \hat{G}$ and let $x \in \mathfrak{O}_{F_{n},\mathfrak{p}^*}[G]$. Then*

$$\chi(x)^p \equiv \chi^p(x)^f \bmod \mathfrak{p}^*.$$

(b) *For $1 < m \leqq n$:*

$$N_{m/m-1}(\chi_m(x)) \equiv \chi_m(x)^p \bmod \mathfrak{p}^*.$$

Proof. (a) Write $x = \sum x_g g$ with $x_g \in \mathfrak{O}_{F_n,\mathfrak{p}^*}$. Then by the Binomial theorem we have congruences $\bmod\, \mathfrak{p}^*$:

$$\begin{aligned} \chi(x)^p &\equiv \sum x_g^p \chi^p(g) \\ \text{by (9.1)} \qquad &\equiv \sum x_g^f \chi^p(g) \\ &\equiv (\chi^p(x))^f, \end{aligned}$$

with the last congruence holding because by definition f fixes μ_q and so $\chi^{pf} = \chi^p$.

(b) As per (8.8) we know

$$N_{m/m-1}(\chi_m(x)) = \prod_{r \equiv 1 \bmod (p^{m-1})} \chi_m^r(x).$$

Let g denote a generator of the cyclic group G, write $x = \sum_{i=0}^{p-1} x_i g^i$ with $x_i \in \mathfrak{O}_{F_n,\mathfrak{p}^*}[G^p]$ and put $\chi_m(g) = \zeta_{p^m}$. Then

$$\chi_m^r(x) = \sum \chi_m(x_i)\zeta_{p^m}^{ir}.$$

It will therefore now suffice to prove:

Lemma 9.5. *Let ζ denote a primitive pth root of unity and let $X_0, \dots, X_{p-1}$ be p algebraic independent commuting indeterminates. Then*

$$\prod_{j=0}^{p-1} \left(\sum X_i \zeta^{ij}\right) = \sum_{0}^{p-1} X_i^p + pk(X_0, \dots, X_{p-1})$$

for some $k(X_0, \dots, X_{p-1}) \in \mathbb{Z}[X_0, \dots, X_{p-1}]$.

Proof. By the Binomial theorem the left-hand expression is congruent to

$$\sum X_i^p \bmod (1-\zeta)\mathbb{Z}[\zeta, X_0, \dots, X_{p-1}].$$

However, by Galois theory we know that the left-hand term belongs to $\mathbb{Z}[X_0, \dots, X_{p-1}]$. We therefore conclude that the congruence indeed holds $\bmod (p)$. □

Proposition 9.6. *Let $\mathfrak{C} \in PH_{\mathfrak{p}^*}(\mathfrak{B})$. Then for $c \in (\mathfrak{C} \otimes_{\mathfrak{O}_F} \mathfrak{O}_{F_n}[G])_{\mathfrak{p}^*}$ and for any $m: n \geqq m > 1$*

$$N_{m/m-1}(\chi_m(c)) \equiv \chi_{m-1}(c)^f \bmod \mathfrak{p}^*.$$

Proof. Since this result is semilocal at $\mathfrak{p}^*$, by 9.4 we may, without loss of generality, take $\mathfrak{C} = \mathfrak{B}$. Using the decomposition

$$(\mathfrak{B} \otimes_{\mathfrak{O}_F} \mathfrak{O}_{F_n})_{\mathfrak{p}^*} = \mathrm{Map}(G, \mathfrak{O}_{F_n,\mathfrak{p}^*}) \cong \bigoplus \mathfrak{O}_{F_n,\mathfrak{p}^*}$$

we are reduced to showing that for $x \in \mathfrak{O}_{F_n,\mathfrak{p}^*}[G]$

$$N_{m/m-1}(\chi_m(x)) \equiv \chi_{m-1}(x)^f \bmod \mathfrak{p}^*$$

and this congruence follows at once from parts (a) and (b) of 9.4. □

We now conclude this section by using the above congruences to construct a homomorphism

$$(9.7) \qquad v_n : D(\mathfrak{A}) \to \frac{\mathfrak{O}^\times_{H_{n-1},\mathfrak{p}^*} \bmod \mathfrak{p}^*}{\mathrm{Im}(\mathfrak{O}^\times_{H_{n-1}})}$$

where $D(\mathfrak{A}) = \mathrm{Ker}(\mathrm{Cl}(\mathfrak{A}) \to \mathrm{Cl}(\mathfrak{M}))$ is the kernel group described in (4.4) and $\mathrm{Im}(\mathfrak{O}^\times_{H_{n-1}})$ denotes the image of $\mathfrak{O}^\times_{H_{n-1}} \bmod \mathfrak{p}^*$. For a class $\mathfrak{C} \in D(\mathfrak{A})$ which is represented by $\mathrm{Det}(m) \in \mathrm{Det}(\mathfrak{M}^\times_{\mathfrak{p}^*})$ under (4.4), we define

$$v_n(\mathfrak{C}) = N_{n/n-1}(\chi_n(m))\chi_{n-1}(m)^{-f}\mathrm{Im}(\mathfrak{O}^\times_{H_{n-1}}) \bmod \mathfrak{p}^*.$$

There are two important points here: firstly for $m \in \mathfrak{M}_{\mathfrak{p}^*}^{\times}$

$$N_{n/n-1}(\chi_n(m))\,\chi_{n-1}(m)^{-f} \in \mathfrak{O}_{H_{n-1,\mathfrak{p}^*}}^{\times};$$

secondly thanks to 2.1 (b) $\mathfrak{A}_{\mathfrak{p}^*} \subset \mathfrak{O}_{F_{n,\mathfrak{p}^*}}[G]$, and so by 9.6 it follows that for $a \in \mathfrak{A}_{\mathfrak{p}^*}^{\times}$

$$N_{n/n-1}(\chi_n(a))\,\chi_{n-1}^{-f}(a) \equiv 1 \bmod \mathfrak{p}^*,$$

which in turn implies that v_n is a well-defined homomorphism via (4.4).

§ 10. Proof of Theorem 3

The notation is again as in the previous section, and we now let M denote an integer greater than n. We recall the injection

$$\theta_{F,M}: PH(\mathfrak{B}_M) \to (H_M^{\times}/H_M^{\times p^M})^{\varepsilon}$$

and we consider the behaviour of θ with respect to the homomorphism

$$[\pi^{M-n}]: PH(\mathfrak{B}_M) \to PH(\mathfrak{B}_n).$$

Proposition 10.1. *Let $\mathfrak{C}_M \in PH(\mathfrak{B}_M)$ and put $\mathfrak{C}_n = [\pi^{M-n}]\mathfrak{C}_M$. Then $\theta_n(\mathfrak{C}_n)$ is represented by $N_{M/n}(\chi_M(r(c_M)))^{p^n}$, where $\mathfrak{C}_M \cdot F = c_M A$.*

Remark. It is precisely the ability to choose large M in the above which gives us the required leverage for our proof of Theorem 3.

Proof. Recall that $\Xi_n = \mathrm{Gal}(N/H_n) \ltimes G$ is the Galois group of $C \underset{F}{\otimes} N/H_n$. Now from (8.6) and (8.7) we know that

$$\chi_n(r(c_M)) \quad \text{and} \quad N_{M/n}(\chi_M(r(c_M)))$$

have the same Ξ_n action formulae, and so

$$\chi_n(r(c_M))^{-1} N_{M/n}(\chi_M(r(c_M))) \in H_n^{\times}.$$

It therefore remains to show that $\chi_n(r(c_M))^{p^n}$ represents $\theta_{F\,n}(\mathfrak{C}_n)$. To this end we view $C_n = \mathfrak{C}_n \cdot F$ as a subalgebra of C_M. Then,

$$\begin{aligned}
\chi_n(r_{C_M}(c_M)) &= \chi_n\Big(\sum_{g \in G_M} c_M^g g^{-1}\Big) \\
&= \chi_n\Big(\sum_{\bar{g} \in G_n} t_{M/n}(c_M)^{\bar{g}} \cdot \bar{g}^{-1}\Big) \\
&= \chi_n(r_{C_n}(t_{M/n}(c_M)))
\end{aligned}$$

where $t_{M/n}: C_M \to C_n$ is the trace map. The result then follows at once since $t_{M/n}(c_M)$ is an A_n normal basis of C_n. □

Suppose now that $\mathfrak{C}_M$ lies in $\mathrm{Ker}(\phi_M : PH_{\mathfrak{p}^*}(\mathfrak{B}_M) \to \mathrm{Cl}(\mathfrak{M}_M))$. Then by 4.5(b) we know that the class $(\mathfrak{C}_M) \in D(\mathfrak{A}_M)$ has representative $\mathrm{Det}(m') \in \mathrm{Det}(\mathfrak{M}_{\mathfrak{p}^*}^{\times})$ for

$$m' = r(c_M)\, r(c_M^*)^{-1}$$

where

$$\mathfrak{C}_M \cdot \mathfrak{M}_M = c_M \cdot \mathfrak{M}_M \quad \text{and} \quad \mathfrak{C}_{M,\mathfrak{p}^*} = c_M^* \cdot \mathfrak{A}_{M,\mathfrak{p}^*}\,.$$

Now put $y_M = \chi_M(r(\pi^{-M} c_M))$; then by 4.6(b) it follows that y_M is a unit.

Lemma 10.2. *Let $s(y_m)$ denote the unique solution in $H_{M,\mathfrak{p}^*}$ to the equation $X^{p^M} = y_M^{p^M}$. Then $\tilde{\theta}_{F,M}(\mathfrak{C}_M)$ is represented (in 7.9) by $s(y_M)$. Moreover $y_M^{1-f} \in \mathfrak{O}_{H_{M,\mathfrak{p}^*}}^{\times}$ and $y_M^{1-f} = s(y_M)^{1-f}$.*

Proof. The first part comes from 7.9. For the final equality it will suffice to show $y_M^{1-f} \in H_{M,\mathfrak{p}^*}$, for then both sides are the unique solution in $H_{M,\mathfrak{p}^*}$ to $X^{p^M} = y_M^{(1-f)p^M}$.

We now compare Galois action formulae for y_M and y_M^f: for $g \in G$

$$\chi_M(r(c_M))^g = \chi_M(r(c_M))\, \chi_M(g)$$

and applying f, using 9.3 together with the fact that f fixes p-power roots of unity, gives

$$\chi_M(r(c_M))^{fg} = \chi_n(r(c_M))^f \cdot \chi_M(g)\,.$$

This then shows y_M^{1-f} is fixed by G, and is therefore an element of $H_{M,\mathfrak{p}^*}$. □

We also observe that by 8.4

$$\mathrm{Det}(r(c_M)\, \sigma(y_M)^{-1}) \in \mathrm{Det}(A^{\times}) = \mathrm{Map}(G_M^*, F^{c\times})^{\Omega_F}\,.$$

Therefore, because this element lies in the denominator of the description (4.4), we conclude that the class $(\mathfrak{C}_M) \in D(\mathfrak{A}_M)$ is represented by $\mathrm{Det}(m_M)$

$$(10.3) \qquad m_M = \sigma(y_M)\, r_2^{-1}$$

where we now write r_2 for $r(c_M^*)$.

Prior to embarking on the proof of Theorem 3, we need a further result which relates global and local units:

Proposition 10.4. *Given positive integers n and k, there exists a constant $\varepsilon > 0$ with the following property: if $z \in \mathfrak{O}_{H_{n,\mathfrak{p}^*}}^{\times}$ with $z^{p^n} \in \mathfrak{O}_{H_n}^{\times}$ and with $|z-1|_v < \varepsilon$ for all $v \mid \mathfrak{p}^*$, then $z^{p^n} \in \mathfrak{O}_{H^n}^{\times p^k}$. (Here $|\;|_v$ denotes the normalised absolute value associated to v.)*

Proof. Let $u_1, \ldots, u_r$ denote a system of fundamental units of H_n. Then by Leopoldt's conjecture, which is true for H_n (by the theorem of Ax-Baker-Brumer),

$$\{u_0 = 1 + p, u_1, \ldots, u_r\}$$

is a $\mathbb{Z}_p$ basis for a submodule of finite index in $\mathfrak{O}^\times_{H_n,\mathfrak{p}^*}$. We may then write

$$z^{p^n} = \prod_{i=0}^{r} u_i^{m_i}, \quad m_i \in \mathbb{Z}_p;$$

indeed, because $z^{p^n} \in \mathfrak{O}^\times_{H_n}$, it follows that $m_0 = 0$ and $m_i \in \mathbb{Z}$ for $i > 0$. As z^{p^n} is $\mathfrak{p}^*$-adically close to 1 and as the u_i are $\mathbb{Z}_p$ linearly independent, it follows that all the m_i are p-adically small. This then shows that, by choosing ε sufficiently small, we may ensure that $z^{p^n} \in \mathfrak{O}^{\times p^k}_{H_n}$. □

To prove the theorem we consider

$$Q \in \operatorname{Ker}(\psi : E_{1,\mathfrak{p}^*} \otimes_{\mathfrak{O}_K} \mathfrak{O}_{K,\mathfrak{p}} \to \varprojlim \mathrm{Cl}(\mathfrak{A}_n)).$$

For each n we choose a representative in $E_{1,\mathfrak{p}^*}$ of $Q \bmod \mathfrak{p}^n$, and thereby obtain a sequence of $\mathfrak{C}_n \in PH_{\mathfrak{p}^*}(\mathfrak{B}_n)$ with

$$(\ldots, \mathfrak{C}_n, \mathfrak{C}_{n+1}, \ldots) \in \varprojlim PH_{\mathfrak{p}^*}(\mathfrak{B}_n)$$

and with each $\mathfrak{C}_n \in \operatorname{Ker} \psi_n$. We shall show that

$$(10.5) \qquad \mathfrak{C}_n = 1 \quad \text{for all } n.$$

Again we now view n as being fixed, and M denotes some integer greater than n. Since $\psi_M(\mathfrak{C}_M) = 1$, clearly $v_M(\mathfrak{C}_M) = 1$ (see (9.7)). We therefore conclude that

$$(10.6) \qquad N_{M/M-1}(\chi_M(m_M)) \equiv u_{M-1}\chi_{M-1}(m_M)^f \bmod \mathfrak{p}^*$$

for some $u_{M-1} \in \mathfrak{O}^\times_{H_{M-1}}$. However, by (10.3)

$$\chi_M(m_M) = \chi_M(\sigma(y_M))\,\chi_M(r_2)^{-1}$$

by (8.2) $$= y_M \cdot \chi_M(r_2)^{-1},$$

$$\chi_{M-1}(m_M) = \chi_{M-1}(\sigma(y_M))\,\chi_{M-1}(r_2)^{-1}$$

by (8.2) $$= N_{M/M-1}(y_M)\,\chi_{M-1}(r_2)^{-1}.$$

Next observe that by Lemma 4.6 $r_2 \in \mathfrak{C}_M \otimes_{\mathfrak{O}_F} \mathfrak{O}_{F_M}[G]^\times_{\mathfrak{p}^*}$, and so by Proposition 9.6

$$N_{M/M-1}(\chi_M(r_2)) \equiv \chi_{M-1}(r_2)^f \bmod \mathfrak{p}^*.$$

Substituting into (10.6) now gives

$$(10.7) \qquad N_{M/M-1}(y_M)^{1-f} \equiv u_{M-1} \bmod \mathfrak{p}^*.$$

Note that by 10.2 and 9.3

$$(10.8) \qquad N_{M/M-1}(y_M^{1-f}) = N_{M/M-1}(y_M)^{1-f} \in \mathfrak{O}^\times_{H_{M-1},\mathfrak{p}^*}.$$

Thanks to 10.1 we know that $\theta_{n,F}(\mathfrak{C}_n)$ is represented in $(H_n^\times/H_n^{\times q})^{(\varepsilon)}$ by the unit

$$N_{M-1/n}(y_{M-1})^{p^n} \quad \text{where } y_{M-1} = N_{M/M-1}(y_M)\,.$$

By 7.10 (b) we know that $1-f$ acts as an automorphism of $(H_n^\times/H_n^{\times p^n})^{(\varepsilon)}$, and so, in order to show that $\mathfrak{C}_n$ is the trivial p.h.s. (as per 10.4), it will suffice to show

$$N_{M-1/n}(y_{M-1})^{p^n(1-f)} \in \mathfrak{O}_{H_n}^{\times p^n}$$

i.e. by 9.3

$$N_{M-1/n}(y_{M-1}^{(1-f)})^{p^n} \in \mathfrak{O}_{H_n}^{\times p^n}\,.$$

Multiplying by $N_{M-1/n}(u_{M-1})^{-p^n}$, we need only to show

$$(10.9) \qquad N_{M-1/n}(y_{M-1}^{1-f}\,u_{M-1}^{-1})^{p^n} \in \mathfrak{O}_{H_n}^{\times p^n}\,.$$

Now by (10.7) we know that

$$(10.10) \qquad y_{M-1}^{1-f}\,u_{M-1}^{-1} \equiv 1 \bmod \mathfrak{p}^*\,.$$

Lemma 10.11. *For $i \geqq 1$*

$$N_{M-1/i}(y_{M-1}^{1-f}\,u_{M-1}^{-1}) \equiv 1 \bmod \mathfrak{p}^{*^{M-i}}\,.$$

Proof. We argue by induction on $M-1-i$. The case $i = M-1$ is then given by (10.10).

Writing $\mathrm{Tr}_{j/j-1}$ for the trace map from $\mathrm{C} \underset{F}{\otimes} L_j \to C \underset{F}{\otimes} L_{j-1}$, by standard cyclotomic theory,

$$\mathrm{Tr}_{j/j-1}(\mathfrak{O}_{C\otimes L_j,\mathfrak{p}^*}) = \mathfrak{p}^*\,\mathfrak{O}_{C\otimes L_{j-1},\mathfrak{p}^*}\,,$$

and therefore for $h \geqq 1$

$$N_{j/j-1}(1+\mathfrak{p}^{*^h}\mathfrak{O}_{C\otimes L_j,\mathfrak{p}^*}) \subseteqq 1+\mathfrak{p}^{*^{h+1}}\mathfrak{O}_{C\otimes L_{j-1},\mathfrak{p}^*}\,.$$

This then establishes the inductive step. □

Choosing M to be large and applying the above lemma, it follows that we can make the element of the left-hand side of (10.9) as $\mathfrak{p}^*$-adically close to 1 as we choose. We then apply 10.4 with $k = n$ to

$$z = N_{M-1/n}(y_{M-1}^{1-f}\,u_{M-1}^{-1})$$

observing that $z \in \mathfrak{O}_{H_n,\mathfrak{p}^*}^*$ by (10.8); this then shows $z^{p^n} \in \mathfrak{O}_{H_n}^{\times p^n}$, and so proves (10.9), as required. □

References

[A1] *A. Agboola*, Abelian varieties and Galois module structure in global fields, Ph. D. Thesis, Columbia University, 1991.

[A2] *A. Agboola*, Iwasawa theory of elliptic curves and Galois module structure, in preparation.

[BT] *N. Byott* and *M.J. Taylor*, Hopf structure and Galois modules, in: Group rings and class groups, K. Roggenkamp and M.J. Taylor, DMV Seminar **18**, Basel–Stuttgart–Boston 1992.

[CF] *J.W.S. Cassels* and *A. Fröhlich* (eds.), Algebraic number theory, Orlando 1967.

[CNS] *Ph. Cassou-Noguès* and *A. Srivastav*, On Taylor's conjecture for Kummer orders, Sém. Th. nomb. Bordeaux **2** (1990), 349–363.

[CNT] *Ph. Cassou-Noguès* and *M.J. Taylor*, Elliptic functions and rings of integers, Progr. Math. **66**, Boston 1987.

[C] *J. Coates*, Infinite descent on elliptic curves with complex multiplication, in: Arithmetic Geometry, Progr. Math. **35** (1983), 107–137.

[CS] *G. Cornell* and *J. Silverman*, Arithmetic Geometry, Berlin–Heidelberg–New York 1986.

[dS] *E. de Shalit*, Iwasawa theory of elliptic curves with complex multiplication, Orlando 1987.

[F1] *A. Fröhlich*, Galois module structure of algebraic integers, Erg. Math. Grenzgeb. 3. Folge **1**, New York–Berlin–Heidelberg 1983.

[F2] *A. Fröhlich*, Invariants for modules over commutative separable orders, Quart. J. Math. Oxford (2) **16** (1965), 193–232.

[G] *R. Greenberg*, Iwasawa theory for p-adic representations, Adv. stud. pure math. **17** (1989), 97–137.

[MT] *B. Mazur, J. Tate*, Canonical height pairings via biextensions, in: Arithmetic Geometry, Progr. Math. **35** (1983), 195–237.

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

[P] *A.J. Plater*, Height Pairings on Elliptic Curves, Ph. D. thesis, Cambridge University, 1991.

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

[S] *J.-P. Serre*, Local Fields, New York–Berlin–Heidelberg 1979.

[Si] *J. Silverman*, The arithmetic of elliptic curves, New York–Berlin–Heidelberg 1986.

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

[T1] *M.J. Taylor*, Galois module structure of arithmetic principal homogeneous spaces, J. Alg. **153**, N° 1 (1992), 203–214.

[T2] *M.J. Taylor*, Galois module structure of rings of integers, Ann. Inst. Fourier **30** (3) (1980), 11–48.

[T3] *M.J. Taylor*, Mordell-Weil groups and the Galois module structure of rings of integers, Ill. J. Math. **32** (1988), 428–452.

[T4] *M.J. Taylor*, Résolvandes et espaces homogènes principaux de schémas en groupe, Sém. Th. nomb. Bordeaux **2** (1990), 255–271.

[W] *W. Waterhouse*, Principal homogeneous spaces and group scheme extensions, AMS Transactions **153**, 181–9.

Department of Mathematics, Columbia University, New York, NY 10027, U.S.A.

M.S.R.I., 1000 Centennial Drive, Berkeley, CA 94720, U.S.A.

Department of Mathematics, UMIST, Manchester, U.K.

Eingegangen 26. Oktober 1992