ON CERTAIN SPECIAL VALUES OF THE KATZ TWO-VARIABLE p-ADIC L-FUNCTION

A. AGBOOLA

Abstract. We develop a framework that enables us to study a broad class of special values of the Katz two-variable p-adic L-functions, including certain special values lying outside the range of p-adic interpolation.

Contents

Date: November 7, 2014.
2000 *Mathematics Subject Classification.* 11G05, 11R23, 11G16.
Partially supported by NSA grants.

1. Introduction

In this article we shall study a wide class of special values of the Katz two-variable p-adic L-function by extending the techniques and results of [1, 2, 23, 24]

Let K be an imaginary quadratic field, and let E/K be an elliptic curve with complex multiplication by the ring of integers O_K of K; then K is necessarily of class number one. Let $p > 3$ be a prime of good, ordinary reduction for E. We may write $p = \mathfrak{p}\mathfrak{p}^*$, with $\mathfrak{p} = \pi O_K$ and $\mathfrak{p}^* = \pi^* O_K$.

Let

$$\psi : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(E_{\pi^\infty}) \xrightarrow{\sim} O_{K,\mathfrak{p}}^\times \xrightarrow{\sim} \mathbf{Z}_p^\times,$$
$$\psi^* : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(E_{\pi^{*\infty}}) \xrightarrow{\sim} O_{K,\mathfrak{p}^*}^\times \xrightarrow{\sim} \mathbf{Z}_p^\times$$

denote the natural $\mathbf{Z}_p^\times$-valued characters of $\mathrm{Gal}(\overline{K}/K)$ arising via Galois action on E_{π^∞} and $E_{\pi^{*\infty}}$ respectively. We may identify ψ with the Grossecharacter associated to E (and ψ^* with the complex conjugate $\overline{\psi}$ of this Grossencharacter), as described, for example, in [23, p. 325].

Set $\mathfrak{K}_\infty := K(E_{p^\infty})$, and let $\mathcal{O}$ denote the completion of the ring of integers of the maximal unramified extension of $K_{\mathfrak{p}}$. For any extension L/K we set

$$\Lambda(L) := \Lambda(\mathrm{Gal}(L/K)) := \mathbf{Z}_p[[\mathrm{Gal}(L/K)]],$$

and $\Lambda(L)_{\mathcal{O}} := \mathcal{O}[[\mathrm{Gal}(L/K)]]$.

The Katz two-variable p-adic L-function $\mathcal{L}_{\mathfrak{p}} \in \Lambda(\mathfrak{K}_\infty)_{\mathcal{O}}$ satisfies a p-adic interpolation formula that may be described as follows (see [23, Theorem 7.1] for the version given here, and also [10, Theorem II.4.14]. Note also that, as the notation indicates, $\mathcal{L}_{\mathfrak{p}}$ depends upon a choice of prime $\mathfrak{p}$ lying above p). For all pairs of integers $j, k \in \mathbf{Z}$ with $0 \leq -j < k$, and for all characters $\chi : \mathrm{Gal}(K(E_p)/K) \to \overline{K}^{\times}$, we have

$$\mathcal{L}_{\mathfrak{p}}(\psi^k \psi^{*j} \chi) = A \cdot L(\psi^{-k} \overline{\psi}^{-j} \chi^{-1}, 0). \tag{1.1}$$

Here $L(\psi^{-k}\overline{\psi}^{-j}\chi^{-1}, s)$ denotes the complex Hecke L-function, and A denotes an explicit, non-zero factor whose precise description we shall not need.

For any character $\phi : \mathrm{Gal}(\overline{K}/K) \to \mathbf{Z}_p^{\times}$, we write $\langle \phi \rangle$ for the composition of ϕ with the natural projection $\mathbf{Z}_p^{\times} \to \mathbf{Z}_p$, and we define

$$L_{\mathfrak{p}}(\phi, s) := \mathcal{L}_{\mathfrak{p}}(\phi \langle \phi \rangle^{s-1}).$$

If ϕ lies within the range of p-adic interpolation of $\mathcal{L}_{\mathfrak{p}}$, then the behaviour of $\mathcal{L}_{\mathfrak{p}}$ at ϕ (i.e. the behaviour of $L_{\mathfrak{p}}(\phi, s)$ at $s = 1$) is predicted by various p-adic generalisations of conjectures of Birch and Swinnerton-Dyer type due to several people. On the other hand, the behaviour of $\mathcal{L}_{\mathfrak{p}}$ outside the range on interpolation is much less well-understood. Variants of the p-adic Birch and Swinnerton-Dyer conjecture involving special values of $\mathcal{L}_{\mathfrak{p}}$ lying outside the range of interpolation were first introduced and studied by Rubin in [23, 24], with some subsequent work by the present author in [1, 2]. (See also [4] for recent work related to this topic, using a very different approach.) In this paper we shall generalise the framework introduced in [1, 2]; this will enable us to analyse a broad class of special values of $\mathcal{L}_{\mathfrak{p}}$ in a uniform manner.

For any integer $r \geq 0$, we write

$$\mathcal{L}_{\mathfrak{p}}^{(r)}(\phi) := \lim_{s \to 1} \frac{L_{\mathfrak{p}}(\phi, s)}{(s-1)^r}.$$

Let χ_{cyc} denote the p-adic cyclotomic character of $\mathrm{Gal}(\overline{K}/K)$, and define $\phi^* := \phi^{-1}\chi_{\mathrm{cyc}}$. Set $T := \mathbf{Z}_p(\phi)$ and $W := T \otimes_{\mathbf{Z}_p} (\mathbf{Q}_p/\mathbf{Z}_p)$. Let $\mathcal{K}_{\infty}$ be the smallest extension of K such that $\mathrm{Gal}(\overline{K}/\mathcal{K}_{\infty})$ acts trivially on T. Define T^*, W^*, and $\mathcal{K}_{\infty}^*$ analogously.

In order to study the behaviour of $\mathcal{L}_{\mathfrak{p}}$ at ϕ, we introduce an Iwasawa module that is naturally associated to $L_{\mathfrak{p}}(\phi, s)$ via the two-variable main conjecture. The Iwasawa module $X_{\mathfrak{p}}(\mathcal{K}_{\infty}, W)$ that we consider is the Pontryagin dual of a certain *restricted Selmer group* $\Sigma_{\mathfrak{p}}(\mathcal{K}_\infty, W)$. This restricted Selmer group is equal to the classical (or Bloch-Kato) Selmer group when ϕ lies within the range of interpolation of $\mathcal{L}_{\mathfrak{p}}$; in general however, the two Selmer groups are different. The two-variable main conjecture shows that a characteristic power series of $X_{\mathfrak{p}}(\mathcal{K}_\infty, W)$ may be viewed as being an algebraic p-adic L-function associated to $L_{\mathfrak{p}}(\phi, s)$.

We define corresponding compact restricted Selmer groups $\Sigma_{\mathfrak{p}}(K, T) \subseteq H^1(K, T)$ and $\Sigma_{\mathfrak{p}^*}(K, T^*) \subseteq H^1(K, T^*)$, and we construct a p-adic height pairing

$$[-,-]^{\phi^*}_{K,\mathfrak{p}^*} : \Sigma_{\mathfrak{p}}(K, T) \times \Sigma_{\mathfrak{p}^*}(K, T) \to \mathbf{Z}_p$$

together with an associated regulator $\mathcal{R}^{(\phi^*)}_{K,\mathfrak{p}^*}$.

Set

$$n_{\mathfrak{p}}(\phi) := \mathrm{rank}_{\mathbf{Z}_p}[\Sigma_{\mathfrak{p}}(K, T)],$$

and let $\Sigma_{\mathfrak{p}}(K, W)_{/\,\mathrm{div}}$ denote the quotient of $\Sigma_{\mathfrak{p}}(K, W)$ by its the maximal divisible subgroup. Write $\Sigma_{\mathfrak{p}}(K, T)_{\mathrm{tors}}$ for the torsion subgroup of $\Sigma(K, T)$. The following result is a special case of Theorem 8.2 of the main text.

Theorem A. *Let ϕ be of infinite order, with $\phi \neq \chi_{\mathrm{cyc}}$. Suppose that $\mathcal{R}^{(\phi^*)}_{K,\mathfrak{p}^*} \neq 0$. Then*

$$\mathrm{ord}_{s=1} L_{\mathfrak{p}}(\phi, s) = n_{\mathfrak{p}}(\phi),$$

and

$$\mathcal{L}_{\mathfrak{p}}^{(n_{\mathfrak{p}}(\phi))}(\phi) \sim |\Sigma_{\mathfrak{p}}(K, W)_{/\,\mathrm{div}}| \cdot |\Sigma_{\mathfrak{p}}(K, T)_{\mathrm{tors}}| \cdot \mathcal{R}^{(\phi^*)}_{K,\mathfrak{p}^*},$$

where the symbol '$\sim$' denotes equality up to multiplication by a p-adic unit.

By using duality theorems to study $n_{\mathfrak{p}}(\phi)$ (see Proposition 9.4 of the main text), we show the following result.

Theorem B. *Suppose that ϕ is of infinite order, with $\phi \neq \chi_{\mathrm{cyc}}$. Then*

$$|n_{\mathfrak{p}}(\phi) - n_{\mathfrak{p}}(\phi^*)| = 1.$$

Hence, if in addition $\mathcal{R}^{(\phi^*)}_{K,\mathfrak{p}^*} \neq 0$, *then*

$$|\operatorname{ord}_{s=1}[L_{\mathfrak{p}}(\phi, s)] - \operatorname{ord}_{s=1}[L_{\mathfrak{p}}(\phi^*, s)]| = 1.$$

In order to be able to obtain exact special value formulae, we need to impose a further condition on the characters ϕ that we consider, namely that of being *locally Lubin-Tate (LLT) at* p (see Definition 6.7 of the main text). Roughly speaking, this means that the restriction of ϕ to a decomposition group at a prime $\mathfrak{q}$ above p is an integral power $m_{\mathfrak{q}}(\phi)$ of a character associated to a Lubin-Tate formal group. When ϕ is LLT at p, it is possible to obtain exact expressions for $\mathcal{L}^{(n_{\mathfrak{p}}(\phi))}_{\mathfrak{p}}(\phi)$ by applying suitable explicit reciprocity laws to canonical elements $y(\phi) \in \Sigma_{\mathfrak{p}}(K, T)$ that are constructed using twisted Euler systems of elliptic units (see Section 11 below).

Let us illustrate a special case of our results in the setting of characters associated to CM modular forms of higher weight. Consider the characters

$$\phi_k := \psi^{k+1}\psi^{*-k}, \quad \phi^*_k := \psi^{-k}\psi^{*k+1}, \quad (k \geq 0).$$

The character ϕ_k is naturally associated to the CM modular form of weight $2k+2$ attached to ψ, and it lies within the range of interpolation of $\mathcal{L}_{\mathfrak{p}}$. The behaviour of $L_{\mathfrak{p}}(\phi_k, s)$ at $s = 1$ is conjecturally well-understood in terms of generalisations of the p-adic Birch and Swinnerton-Dyer conjecture to the case of modular forms of higher weight. On the other hand, the character ϕ^*_k lies outside the range of interpolation of $\mathcal{L}_{\mathfrak{p}}$, and the behaviour of $L_{\mathfrak{p}}(\phi_k, s)$ at $s = 1$ for arbitrary k is less well understood. When $k = 0$ and $n_{\mathfrak{p}}(\phi_k) \geq 1$, the function $L_{\mathfrak{p}}(\phi^*_k, s)$ was first studied by K. Rubin, who formulated a version of the p-adic Birch and Swinnerton-Dyer conjecture in this setting (see [23, 24]). This work was subsequently extended to the cover the case $n_{\mathfrak{p}}(\phi_k) = 0$ by the present author (see [1, 2]). When $k \geq 1$, the function $L_{\mathfrak{p}}(\phi^*_k, s)$ has not previously been studied.

Set

$$T_k := \mathbf{Z}_p(\phi_k), \quad T_k^* := \mathbf{Z}_p(\phi_k^*),$$
$$V_k := T_k \otimes \mathbf{Q}_p, \quad V_k^* := T_k^* \otimes \mathbf{Q}_p.$$

Write

$$\mathrm{Exp}^*_{V_k} : H^1(K_{\mathfrak{p}^*}, V_k) \to \mathbf{Q}_p,$$
$$\mathrm{Exp}^*_{V_k^*} : H^1(K_{\mathfrak{p}}, V_k^*) \to \mathbf{Q}_p$$

for the Bloch-Kato dual exponential maps associated to V_k and V_k^*, and

$$\mathrm{Log}_{V_k} : H^1(K_{\mathfrak{p}}, V_k) \to \mathbf{Q}_p,$$
$$\mathrm{Log}_{V_k^*} : H^1(K_{\mathfrak{p}^*}, V_k^*) \to \mathbf{Q}_p$$

for the corresponding Bloch-Kato logarithm maps. For each place v of K, we let

$$\mathrm{loc}_v : H^1(K, T_k) \to H^1(K_v, T_k), \quad \mathrm{loc}_v : H^1(K, T_k^*) \to H^1(K_v, T_k^*)$$

denote the obvious localisation maps at v.

Suppose that $\mathfrak{q} \in \{\mathfrak{p}, \mathfrak{p}^*\}$ and that $m \in \mathbf{Z}$. Let $\mathrm{Fr}_{\mathfrak{q}}$ denote a Frobenius element of $\mathrm{Gal}(\overline{K}/K)$ at $\mathfrak{q}$. For any character $\phi : \mathrm{Gal}(\overline{K}/K) \to \mathbf{Z}_p^\times$ we define an Euler factor $\mathrm{Eul}_{\mathfrak{q}}(\phi, m)$ by

$$\mathrm{Eul}_{\mathfrak{q}}(\phi, m) := \left(1 - (\phi\chi_{\mathrm{cyc}}^{-m})(\mathrm{Fr}_{\mathfrak{q}})\right)^{-1} \cdot (1 - \phi(\mathrm{Fr}_{\mathfrak{q}}))^{-1}$$
$$\times \left(1 - [(p^{-1}\chi_{\mathrm{cyc}})^m \phi^{-1}](\mathrm{Fr}_{\mathfrak{q}})\right) \cdot \left(1 - [p^{-m}\phi^{-1}](\mathrm{Fr}_{\mathfrak{q}})\right).$$

The following result is a special case of Theorems 11.6 and 12.3 of the main text.

Theorem C. *Suppose that ϕ_k and ϕ_k^* are LLT at $\mathfrak{p}$, and that $\mathcal{L}_{\mathfrak{p}}(\phi_k) \neq 0$. Then $\mathcal{R}_{K,\mathfrak{p}}^{(\phi_k)} \neq 0$, and we have the following equality in $\mathbf{Q}_p$:*

$$\mathrm{Eul}_{\mathfrak{p}}(\phi_k^{-1}, k+1)^{-1}\,\mathrm{Eul}_{\mathfrak{p}^*}(\phi_k^{-1}, k)^{-1} \cdot \mathcal{L}_{\mathfrak{p}}(\phi_k) =$$
$$\frac{\Omega(\phi_{k,\mathfrak{p}^*}^{-1})}{\Omega(\phi_{k,\mathfrak{p}}^{-1})} \cdot \frac{[y(\phi_k^*), y(\phi_k)]_{K,\mathfrak{p}^*}^{(\phi_k)}}{\mathrm{Exp}_{V_k}^*(\mathrm{loc}_{\mathfrak{p}^*}(y(\phi_k)))\,\mathrm{Exp}_{V_k^*}^*(\mathrm{loc}_{\mathfrak{p}}(y(\phi_k^*)))} \cdot \mathcal{L}_{\mathfrak{p}^*}^{(1)}(\phi_k).$$

(We refer the reader to Section 6 for the precise definitions of the periods $\Omega(\phi_{k,\mathfrak{p}^*}^{-1})$ and $\Omega(\phi_{k,\mathfrak{p}}^{-1})$.)

Theorem C, (which is a generalisation of [2, Theorem A] to modular forms of higher weight), relates the *value* of $\mathcal{L}_{\mathfrak{p}}$ at the point ϕ_k lying within the range of interpolation to the *derivative* of $\mathcal{L}_{\mathfrak{p}}$ at the point ϕ_k^* lying outside the range on interpolation. It may be viewed as being an analogue of the well-known exceptional zero phenomenon observed in the work of Mazur, Tate and Teitelbaum in the setting of elliptic curves *without* complex multiplication (see [14, especially Conjecture 2], [16, especially page 38]).

If $\mathcal{L}_{\mathfrak{p}}(\phi_k) = 0$, then Theorems 11.6 and 12.3 below also yield the following generalisation of [23, Theorem 10.1] to the higher weight case, which again illustrates the phenomenon alluded to above.

Theorem D. *Assume that ϕ_k and ϕ_k^* are LLT above p. Suppose also that $\mathcal{L}_{\mathfrak{p}}(\phi_k) = 0$ and that $\mathcal{L}_{\mathfrak{p}}^{(1)}(\phi_k) \neq 0$. Then $\mathcal{L}_{\mathfrak{p}}(\phi_k^*) \neq 0$, and the following equality holds in $\mathbf{Q}_p$:*

$$\mathrm{Eul}_{\mathfrak{p}}(\phi_k^{*-1}, k)^{-1}\,\mathrm{Eul}_{\mathfrak{p}^*}(\phi_k^{*-1}, k+1)^{-1} \cdot \mathcal{L}_{\mathfrak{p}^*}^{(1)}(\phi_k^*) =$$
$$\frac{\Omega(\phi_{k,\mathfrak{p}}^{*-1})}{\Omega(\phi_{k,\mathfrak{p}^*}^{*-1})} \cdot \frac{[y(\phi_k), y(\phi_k^*)]_{k,\mathfrak{p}^*}^{(\phi_k^*)}}{\mathrm{Log}_{V_k^*}(\mathrm{loc}_{\mathfrak{p}^*}(y(\phi_k^*)))\,\mathrm{Log}_{V}(\mathrm{loc}_{\mathfrak{p}}(y(\phi_k)))} \cdot \mathcal{L}_{\mathfrak{p}}(\phi_k^*).$$

A brief outline of the contents of this paper is as follows. In Section 2, we establish certain notation and conventions that will apply throughout this paper. We then recall some general facts about twists of Iwasawa modules and derivatives of their characteristic power series in Section 3, and we explain how these facts may be applied to the Katz two-variable p-adic L-function. In Section 4, we define various Selmer groups that we need, and we prove a control theorem for restricted Selmer groups. In Section 5, we describe how elements in restricted Selmer groups may be constructed using twisted units, and we establish certain basic properties of elements constructed in this way.

In Section 6, we recall certain results concerning explicit reciprocity laws on Lubin-Tate formal groups, and we calculate the Bloch-Kato logarithms and dual exponentials of the elements in restricted Selmer constructed in Section 5. We construct the p-adic height pairing on restricted Selmer groups in Section 7, and we describe how to evaluate the p-adic heights of elements in restricted Selmer groups constructed via twisted units. In Section 8, under the assumption that the p-adic height pairing constructed in Section 7 is non-degenerate, we prove a very general leading term formula for a characteristic power series of a restricted Selmer group over an arbitrary finite extension of K. We compare different restricted Selmer groups over K in Section 9, and we describe the relationship between the leading terms of the relevant characteristic power series (see Theorem 9.7).

We recall some basic facts concerning elliptic units and the construction of the Katz two-variable p-adic L-function $\mathcal{L}_{\mathfrak{q}}$ in Section 10. In Section 11, we apply our previous results to construct canonical elements in restricted Selmer groups over K using twisted elliptic units, and to prove a very general exact leading term formula for $\mathcal{L}_{\mathfrak{q}}$ (see especially Theorem 11.6). Finally, in Section 12, we specialise the results of Section 11 to the case of complex conjugate characters, and we prove a result (see Theorem 12.3) which implies Theorems C and D above.

2. Notation and conventions

If L is any field, we write O_L for its ring of integers and L^{ab} for its maximal abelian extension. We let $\overline{L}$ denote an algebraic closure of L.

Let K be an imaginary quadratic field of class number one, and let E/K be a fixed elliptic curve with complex multiplication by the ring of integers O_K of K. We write $\mathfrak{f}$ for the conductor of E. We fix a prime $p > 3$ of good, ordinary reduction for E, so that $pO_K = \mathfrak{p}\mathfrak{p}^*$. Let

$$\psi : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(E_{\mathfrak{p}^\infty}) \xrightarrow{\sim} O_{K,\mathfrak{p}}^\times \xrightarrow{\sim} \mathbf{Z}_p^\times,$$
$$\psi^* : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(E_{\mathfrak{p}^{*\infty}}) \xrightarrow{\sim} O_{K,\mathfrak{p}^*}^\times \xrightarrow{\sim} \mathbf{Z}_p^\times$$

denote the natural $\mathbf{Z}_p^\times$-valued characters of $\mathrm{Gal}(\overline{K}/K)$ arising via Galois action on $E_{\mathfrak{p}^\infty}$ and $E_{\mathfrak{p}^{*\infty}}$ respectively. We may identify ψ with the Grossecharacter associated to E (and ψ^* with the complex conjugate $\overline{\psi}$ of this Grossencharacter), as described, for example, in [23, p. 325].

The symbol $\mathfrak{q}$ will always denote a prime of O_K lying above p, and we write $i_{\mathfrak{q}} : \overline{K} \hookrightarrow \overline{K}_{\mathfrak{q}}$ for the natural embedding afforded by $\mathfrak{q}$.

We write $\chi_{\mathrm{cyc}} : \mathrm{Gal}(\overline{K}/K) \to \mathbf{Z}_p^\times$ for the p-adic cyclotomic character of $\mathrm{Gal}(\overline{K}/K)$. If $\chi : \mathrm{Gal}(\overline{K}/K) \to \mathbf{Z}_p^\times$ is any character of $\mathrm{Gal}(\overline{K}/K)$, we set $\chi^* := \chi^{-1}\chi_{\mathrm{cyc}}$ and $\mathbf{Z}_p(\chi) := \mathbf{Z}_p \otimes \chi$. We write $\langle \chi \rangle : \mathrm{Gal}(\overline{K}/K) \to 1 + p\mathbf{Z}_p$ for the composition of χ with the natural surjection $\mathbf{Z}_p^\times \to 1 + p\mathbf{Z}_p$.

Throughout this paper $\phi : \mathrm{Gal}(\overline{K}/K) \to \mathbf{Z}_p^\times$ denotes a character of infinite order. (We shall impose further conditions on ϕ as the need arises.) We let

$$T := \mathbf{Z}_(\phi), \quad T^* := \mathbf{Z}_p(\phi^*);$$

so T and T^* are free, rank one $\mathbf{Z}_p$-modules on which $\mathrm{Gal}(\overline{K}/K)$ acts via ϕ and ϕ^* respectively. Set

$$V := T \otimes_{\mathbf{Z}_p} \mathbf{Q}_p, \quad W := V/T,$$
$$V^* := T^* \otimes_{\mathbf{Z}_p} \mathbf{Q}_p, \quad W^* := V^*/T^*,$$

and write W_{p^n} and $W^*_{p^n}$ for the p^n-torsion subgroups of W and W^* respectively. We view $T = \varprojlim W_{p^n}$, $T^* = \varprojlim W^*_{p^n}$, (where the inverse limits are taken with respect to the obvious multiplication-by-p maps), and we let $w = [w_n]$, $w^* = [w_n^*]$ denote fixed generators of T and T^* respectively, chosen to satisfy the condition 2.1 below.

For each integer $n \geq 1$, we let

$$e_n : W_{p^n} \times W^*_{p^n} \to \mu_{p^n}$$

denote the pairing afforded by Cartier duality via viewing W_{p^n} and $W^*_{p^n}$ as group schemes over $\mathrm{Spec}(K)$. This pairing satisfies the identity

$$e_n(pw_n, w_n^*) = e_n(w_n, pw_n^*).$$

We fix once and for all a generator $\zeta = [\zeta_n]$ of $\mathbf{Z}_p(1)$, and we assume that w and w^* are chosen to satisfy

$$e_n(w_n, w_n^*) = \zeta_n \tag{2.1}$$

for all $n \geq 1$.

We write

$$\mathcal{K}_n := K(W_{p^n}), \quad \mathcal{K}_n^* := K(W^*_{p^n}), \quad \mathfrak{K}_n := \mathcal{K}_n \cdot \mathcal{K}_n^*,$$

and

$$\mathcal{K}_\infty := \cup_{n\geq 1}\mathcal{K}_n, \quad \mathcal{K}_\infty^* := \cup_{n\geq 1}\mathcal{K}_n^*, \quad \mathfrak{K}_\infty := \cup_{n\geq 1}\mathfrak{K}_n.$$

We denote the unique $\mathbf{Z}_p$-extension contained in $\mathcal{K}_\infty$ by K_∞. For any finite extension F/K, we set

$$\mathcal{F}_n := F \cdot \mathcal{K}_n, \quad \mathcal{F}_n^* := F \cdot \mathcal{K}_n^*, \quad \mathfrak{F}_n := F \cdot \mathfrak{K}_n,$$

and

$$\mathcal{F}_\infty := F \cdot \mathcal{K}_\infty, \quad F_\infty := F \cdot K_\infty, \quad \mathcal{F}_\infty^* := F \cdot \mathcal{K}_\infty^*, \quad \mathfrak{F}_\infty := F \cdot \mathfrak{F}_\infty.$$

The symbol $\mathcal{O}$ denotes the completion of the ring of integers of the maximal unramified extension of $\mathbf{Q}_p$.

Suppose that $\mathfrak{q} \in \{\mathfrak{p}, \mathfrak{p}^*\}$. If F/K is a finite extension, we set

$$U_{\mathfrak{q}}(F) := \text{units in } F_{\mathfrak{q}} \text{ congruent to 1 modulo } \mathfrak{q}.$$

We also set

$$\mathcal{E}(F) := \text{global units of } F;$$
$$\overline{\mathcal{E}}_{\mathfrak{q}}(F) := \text{the closure of the projection of } \mathcal{E}(F) \text{ into } U_{\mathfrak{q}}(F).$$

If F/K is an infinite extension with $F = \cup_{n\geq 0} F_n$ (where each F_n is a finite extension of K), then we write

$$U_{\mathfrak{q}}(F) := \varprojlim U_{\mathfrak{q}}(F_n), \quad \mathcal{E}(F) := \varprojlim \mathcal{E}(F_n), \quad \overline{\mathcal{E}_{\mathfrak{q}}}(F) := \varprojlim \overline{\mathcal{E}_{\mathfrak{q}}}(F_n),$$

where the inverse limits are taken with respect to the obvious norm maps.

Remark 2.1. Note that since the strong Leopoldt conjecture holds for all finite extensions of K, we have that

$$\overline{\mathcal{E}_{\mathfrak{q}}}(F) \simeq \mathcal{E}(F) \otimes_{\mathbf{Z}} \mathbf{Z}_p$$

whenever F/K is finite. Hence, for any algebraic extension F/K, we may also view $\overline{\mathcal{E}_{\mathfrak{q}}}(F)$ as being a submodule of $U_{\mathfrak{q}^*}(F)$. We shall do this without further comment several times in what follows. □

For any extension L/K, we set

$$\Lambda(L) := \Lambda(\mathrm{Gal}(L/K)) := \mathbf{Z}_p[[\mathrm{Gal}(L/K)]], \quad \Lambda(L)_{\mathcal{O}} := \mathcal{O}[[\mathrm{Gal}(L/K)]].$$

If F/K is a finite extension and $\chi : \mathrm{Gal}(\overline{F}/F) \to \mathbf{Z}_p^{\times}$ is a character of infinite order, we often write $F^{(\chi)}/F$ for the extension of F cut out by χ. We set

$$\mathcal{I}_{\chi}(F) := \mathrm{Ker}[\chi : \Lambda(\mathcal{F}^{(\chi)}) \to \mathbf{Z}_p],$$

and we define a generator $\vartheta_{\chi} = \vartheta_{\chi}(F)$ as follows. We choose a topological generator $\gamma_{\chi} = \gamma_{\chi}(F)$ such that

$$\log_p(\chi(\gamma_{\chi})) = p,$$

and we set

$$\vartheta_{\chi}(F) := \chi(\gamma_{\chi}^{-1})\gamma_{\chi} - 1.$$

For any extension L/K we write $\mathcal{M}^{\mathfrak{q}}(L)$ for the maximal abelian pro-p extension of L which is unramified away from $\mathfrak{q}$, and we set $\mathcal{X}^{\mathfrak{q}}(L) := \mathrm{Gal}(\mathcal{M}^{\mathfrak{q}}(L)/L)$. We let $\mathcal{B}^{\mathfrak{q}}(L)$ denote the maximal abelian pro-p extension of L which is unramified away from $\mathfrak{q}$ and totally split at all places of L lying above $\mathfrak{q}^*$, and we write $\mathcal{Y}^{\mathfrak{q}}(L) := \mathrm{Gal}(\mathcal{B}^{\mathfrak{q}}(L)/L)$.

If M is any $\mathbf{Z}_p$-module, then M_{div} denotes the maximal divisible submodule of M, and we set $M_{/\,\mathrm{div}} := M/M_{\mathrm{div}}$. We write M_{tors} for the torsion submodule of M, and $M^{\wedge}$ for the Pontryagin dual of M. If M is a torsion $\mathbf{Z}_p$-module, then we write $T_p(M)$ for the p-adic Tate module of M.

3. Characteristic power series

Our goal in this section is to recall (following [1], but in slightly greater generality) some basic facts concerning twists of Iwasawa modules and derivatives of characteristic power series. We shall then apply these results to twists of the two-variable p-adic L-function $\mathcal{L}_{\mathfrak{q}}$ (where $\mathfrak{q} \in \{\mathfrak{p}, \mathfrak{p}^*\}$) by characters of $\mathrm{Gal}(\mathfrak{K}_\infty/K)$ of infinite order. This will later enable us to apply the two-variable main conjecture to relate special values of $\mathcal{L}_{\mathfrak{q}}$ to the arithmetic of certain Selmer groups.

Suppose that F/K is any finite extension. Let $\mathcal{G}_F := \mathrm{Gal}(\mathfrak{F}_\infty/F)$, and suppose that $\rho : \mathcal{G}_F \to \mathbf{Z}_p^\times$ is any character. Then there is a twisting map

$$\mathrm{Tw}_\rho : \Lambda(\mathcal{G}_F) \to \Lambda(\mathcal{G}_F)$$

associated to ρ which is induced by the map $g \mapsto \rho(g)g$ for all $g \in \mathcal{G}_F$. It is easy to see that if $f \in \Lambda(\mathcal{G}_F)$, then

$$f(\rho) = [\mathrm{Tw}_\rho(f)](\mathbf{1}).$$

If M is any finitely generated $\Lambda(\mathcal{G}_F)$-module which characteristic power series $f_M \in \Lambda(\mathcal{G}_F)$, then a routine computation shows that $\mathrm{Tw}_\rho(f_M)$ is a characteristic power series of $M(\rho^{-1}) := M \otimes \rho^{-1}$.

Set $\mathcal{H} := \mathrm{Ker}(\rho)$. Then there is a natural quotient map

$$\Pi_{\mathcal{G}_F/\mathcal{H}} : \Lambda(\mathcal{G}_F) \to \Lambda(\mathcal{G}_F/\mathcal{H}),$$

and $\Pi_{\mathcal{G}/\mathcal{H}}(\mathrm{Tw}_\rho(f_M))$ is a characteristic power series of the $\Lambda(\mathcal{G}_F/\mathcal{H})$-module $M(\rho^{-1}) \otimes_{\Lambda(\mathcal{G}_F)} \Lambda(\mathcal{G}_F/\mathcal{H})$. If $\rho_1 : \mathcal{G}_F \to \mathbf{Z}_p^\times$ is any character which factors through $\mathcal{G}_F/\mathcal{H}$, then

$$[\mathrm{Tw}_\rho(f_M)](\rho_1) = [\Pi_{\mathcal{G}_F/\mathcal{H}}(\mathrm{Tw}_\rho(f_M))](\rho_1),$$

and there is an isomorphism

$$M(\rho^{-1}) \otimes_{\Lambda(\mathcal{G}_F)} \Lambda(\mathcal{G}_F/\mathcal{H}) \simeq (M \otimes_{\Lambda(\mathcal{G}_F)} \Lambda(\mathcal{G}_F/\mathcal{H}))(\rho^{-1})$$

of $\Lambda(\mathcal{G}_F/\mathcal{H})$-modules. Hence we see that we may study the values of $\mathrm{Tw}_\rho(f_M)$ at characters ρ_1 which factor through $\mathcal{G}_F/\mathcal{H}$ by studying the values of the element $\Pi_{\mathcal{G}_F/\mathcal{H}}(\mathrm{Tw}_\rho(f_M))$ at such characters.

Suppose now that ρ is of infinite order, and let M_1 be a finitely generated $\Lambda(\mathcal{G}_F/\mathcal{H})$-module. Let $f_{M_1} \in \Lambda(\mathcal{G}_F/\mathcal{H})$ be a characteristic power series of M_1. We may write

$$\mathcal{G}_F/\mathcal{H} \simeq \Delta_{\mathcal{H}} \times G_{\mathcal{H}},$$

where $\Delta_{\mathcal{H}}$ is of finite order prime to p, and $G_{\mathcal{H}} \simeq \mathbf{Z}_p$. Let $\gamma_{\mathcal{H}}$ be a fixed topological generator of $\mathcal{G}_F/\mathcal{H}$, and let $\Pi_{G_{\mathcal{H}}} : \Lambda(\mathcal{G}_F/\mathcal{H}) \to \Lambda(G_{\mathcal{H}})$ be the natural quotient map. We identify $\Lambda(G_{\mathcal{H}})$ with the power series ring $\mathbf{Z}_p[[X]]$ in one variable in the usual way via the map $\Pi_{G_{\mathcal{H}}}(\gamma_{\mathcal{H}}) \mapsto 1 + X$.

Let $I_{\mathcal{G}_F/\mathcal{H}}$ denote the augmentation ideal of $\Lambda(\mathcal{G}_F/\mathcal{H})$, and suppose that $n \geq 0$ is the smallest integer such that the image of f_{M_1} in $I^n_{\mathcal{G}_F/\mathcal{H}}/I^{n+1}_{\mathcal{G}/\mathcal{H}}$ is non-zero. It is not hard to check that $\Pi_{G_{\mathcal{H}}}(f_{M_1})$ is a characteristic power series of the $\Lambda(G_{\mathcal{H}})$-module $M_1^{\Delta_{\mathcal{H}}}$, and that

$$((\gamma_{\mathcal{H}} - 1)^{-n} f_{M_1})(\mathbf{1}) = \left.\frac{\Pi_{G_{\mathcal{H}}}(f_{M_1})}{X^n}\right|_{X=0}, \tag{3.1}$$

where $\mathbf{1}$ denotes the identity character of $\mathcal{G}_F/\mathcal{H}$.

For any character $\nu : \mathcal{G}_F/\mathcal{H} \to \mathbf{Z}_p^\times$, we set $\vartheta_\nu := \nu(\gamma_{\mathcal{H}})^{-1}\gamma_{\mathcal{H}} - 1$. Then if $m \geq 0$ is any integer, it follows from the definitions that we have

$$(\vartheta_\nu^{-m} f_{M_1})(\nu) = [(\gamma_{\mathcal{H}} - 1)^{-m} \operatorname{Tw}_\nu(f_{M_1})](\mathbf{1}), \tag{3.2}$$

where $\operatorname{Tw}_\nu : \Lambda(\mathcal{G}_F/\mathcal{H}) \to \Lambda(\mathcal{G}_F/\mathcal{H})$ is the twisting map associated to ν.

Let us now explain how (3.2) is related to derivatives of certain p-adic analytic functions (see [23, §7]). Recall that we write $< \nu >: \mathcal{G}_F/\mathcal{H} \to \mathbf{Z}_p^\times$ for the composition of ν with the natural projection $\mathbf{Z}_p^\times \to 1 + p\mathbf{Z}_p$. Suppose that $\chi : \mathcal{G}_F/\mathcal{H} \to \mathbf{Z}_p^\times$ is any character of order prime to p. Then the map from $\mathbf{Z}_p$ to $\mathbf{C}_p$ given by $s \mapsto f_{M_1}(\nu\chi < \nu >^{s-1})$ defines an analytic function on $\mathbf{Z}_p$. Define

$$\operatorname{ord}_{\nu\chi}(f_{M_1}) := \operatorname{ord}_{s=1} f_{M_1}(\nu\chi < \nu >^{s-1}),$$

and set

$$\mathbf{D}^{(m)} f_{M_1}(\nu\chi) := \frac{1}{m!}\left(\frac{d}{ds}\right)^m f_{M_1}(\nu\chi < \nu >^{s-1})\bigg|_{s=1}.$$

We write

$$f_{M_1}^{(m)}(\nu\chi) := \mathbf{D}^{(m)} f_{M_1}(\nu\chi),$$

and we extend these definitions to $\Lambda(\mathcal{G}_F)$ via the quotient map $\Pi_{\mathcal{G}_F/\mathcal{H}}$. A routine calculation shows that we have

$$\mathbf{D}^{(m)}(\vartheta_\nu^m(\nu\chi)) = \{\log_p(\nu(\gamma_{\mathcal{H}}))\}^m,$$

and

$$\begin{aligned}\mathbf{D}^{(m)}(\vartheta_\nu^m f_{M_1})(\nu\chi) &= \{\log_p(\nu(\gamma_{\mathcal{H}}))\}^m f_{M_1}(\nu\chi) \\ &= [\{\log_p(\nu(\gamma_{\mathcal{H}}))\}^m \operatorname{Tw}_\nu(f_{M_1})](\chi).\end{aligned} \tag{3.3}$$

We can now see from (3.1), (3.2) and (3.3) that if $n_\nu := \mathrm{ord}_\nu(f_{M_1})$, then we may write $f_{M_1} = \vartheta_\nu^{n_\nu} F_\nu$ with $F_\nu \in \Lambda(\mathcal{G}_F/\mathcal{H})$, and we have

$$\begin{aligned} f_{M_1}^{(n_\nu)}(\nu) &= \lim_{s\to 1} \frac{f_{M_1}(\nu < \nu >^{s-1})}{(s-1)^{n_\nu}} \\ &= \mathbf{D}^{(n_\nu)}(\vartheta_\nu^{n_\nu} F_\nu)(\nu) \\ &= [\{\log_p(\nu(\gamma_{\mathcal{H}}))\}^{n_\nu}\, \mathrm{Tw}_\nu(F_\nu)](\mathbf{1}) \\ &= \{\log_p(\nu(\gamma_{\mathcal{H}}))\}^{n_\nu} \cdot \Pi_G(\mathrm{Tw}_\nu(F_\nu))(0) \\ &= \{\log_p(\nu(\gamma_{\mathcal{H}}))\}^{n_\nu} \cdot \left.\frac{\Pi_G(\mathrm{Tw}_\nu(f_{M_1}))}{X^{n_\nu}}\right|_{X=0}. \end{aligned} \tag{3.4}$$

We shall now apply the above discussion to the case in which $F = K$, $M = \mathcal{X}_\mathfrak{p}(\mathfrak{K}_\infty)$, $\rho = \nu$ is any character of infinite order, and $\chi = \mathbf{1}$.

Set $\mathcal{D}_\infty := \mathfrak{K}_\infty^{\mathcal{H}}$, the fixed field of $\mathcal{H}$, and write $D_\infty := \mathcal{D}_\infty^{\Delta_\mathcal{H}}$; then $\mathrm{Gal}(D_\infty/K) = G_\mathcal{H} \simeq \mathbf{Z}_p$. Recall that the two-variable main conjecture asserts that if $\mathfrak{q} \in \{\mathfrak{p}, \mathfrak{p}^*\}$, then $\mathcal{X}_\mathfrak{q}(\mathfrak{K}_\infty)$ is a torsion $\Lambda(\mathfrak{K}_\infty)$-module, and that the Katz two-variable p-adic L-function $\mathcal{L}_\mathfrak{q}$ is a characteristic power series of $\mathcal{X}_\mathfrak{q}(\mathfrak{K}_\infty)$ in $\Lambda(\mathfrak{K}_\infty)_\mathcal{O}$. We therefore see that $\mathrm{Tw}_\rho(\mathcal{L}_\mathfrak{q}) \in \Lambda(\mathfrak{K}_\infty)_\mathcal{O}$ is a characteristic power series of $\mathcal{X}_\mathfrak{q}(\mathfrak{K}_\infty)(\rho^{-1})$.

Let I_{D_∞} denote the kernel of the natural map $\Lambda(\mathfrak{K}_\infty) \to \Lambda(D_\infty)$. Fix any characteristic power series $H_{\mathfrak{q},\rho}^{(K)}$ of the $\Lambda(D_\infty)$-module

$$\mathcal{X}_\mathfrak{q}(\mathfrak{K}_\infty)(\rho^{-1}) \otimes_{\Lambda(\mathfrak{K}_\infty)} (\Lambda(\mathfrak{K}_\infty)/I_{D_\infty}) \simeq \mathcal{X}_\mathfrak{q}(\mathfrak{K}_\infty)(\rho^{-1})/I_{D_\infty}\mathcal{X}_\mathfrak{q}(\mathfrak{K}_\infty)(\rho^{-1}).$$

Set

$$L_\mathfrak{q}(\rho, s) := \mathcal{L}_\mathfrak{q}(\rho\langle\rho\rangle^{s-1}),$$

and write

$$n_{\mathfrak{q},\rho} := \mathrm{ord}_{s=1} L_\mathfrak{p}(\rho, s).$$

Definition 3.1. For any non-negative integer m, we define

$$\mathcal{L}_\mathfrak{q}^{(m)}(\rho) := \lim_{s\to 1} \frac{L_\mathfrak{p}(\rho, s)}{(s-1)^m}. \tag{3.5}$$

□

Proposition 3.2. *With the above notation, we have*

$$n_{\mathfrak{q},\rho} = \operatorname{ord}_{X=0} H_{\mathfrak{q},\rho}^{(K)}, \tag{3.6}$$

and

$$\mathcal{L}_{\mathfrak{q}}^{(n_{\mathfrak{q},\rho})}(\rho) = \lim_{s \to 1} \frac{L_{\mathfrak{p}}(\rho, s)}{(s-1)^{n_{\mathfrak{q},\rho}}} \sim \{\log_p(\rho(\gamma_{\mathcal{H}}))\}^{n_{\mathfrak{q},\rho}} \cdot \left.\frac{H_{\mathfrak{q},\rho}^{(K)}}{X^{n_{\mathfrak{q},\rho}}}\right|_{X=0}, \tag{3.7}$$

where '$\sim$' denotes equality up to multiplication by a p-adic unit (which, in this case, lies in $\mathcal{O}^\times$).

Proof. This follows from (3.1), (3.2), and (3.4). □

We therefore see that the order of vanishing $n_{\mathfrak{q},\rho}$ of $\mathcal{L}_{\mathfrak{q}}$ at ρ and the p-adic valuation of $\mathcal{L}_{\mathfrak{q}}^{(n_{\mathfrak{q},\rho})}(\rho)$ may be determined by studying $H_{\mathfrak{q},\rho}^{(K)}$, and that this may be done algebraically.

4. Selmer groups

In this section we shall define various Selmer groups that we require, and we shall establish some of their properties.

Suppose that F is a finite extension of K.

Definition 4.1. For each finite place v of F, we write $H^1_f(F, V)$ for the Bloch-Kato cohomology group at v associated to V. Hence

$$H^1_f(F_v, V) = \begin{cases} \operatorname{Ker}[H^1(F_v, V) \to H^1(\operatorname{Gal}(\overline{F}_v/F_v^{nr}, V))] & \text{if } v \nmid p; \\ \operatorname{Ker}[H^1(F_v, V) \to H^1(F_v, B_{\text{crys}} \otimes_{\mathbf{Q}_p} V)] & \text{if } v \mid p, \end{cases}$$

where F_v^{nr} is the maximal unramified extension of F_v, and B_{crys} denotes Fontaine's ring of crystalline periods.

There is a tautological exact sequence

$$0 \to T \to V \to W \to 0, \tag{4.1}$$

and we define $H^1_f(F_v, T)$ and $H^1(F_v, V)$ to be the pre-image and image respectively of $H^1(F_v, V)$ under the maps on cohomology groups induced by the exact sequence (4.1).

For each positive integer n, there is an exact sequence

$$0 \to W_{p^n} \to W \xrightarrow{\times p^n} W \to 0, \tag{4.2}$$

and we define $H^1_f(F_v, W_{p^n})$ to be the inverse image of $H^1(F_v, W)$ under the map on cohomology induced by (4.2).

We define similar groups with V replaced by V^* in an entirely analogous manner. $\square$

Example 4.2. Suppose that $\phi = \psi^i \psi^{*j}$. For each place v of F lying above p, we set

$$m_v(\phi) = \begin{cases} i & \text{if } v \mid \mathfrak{p}; \\ j & \text{if } v \mid \mathfrak{p}^*. \end{cases}$$

The following table lists the groups $H^1_f(F_v, -)$ for $v \mid p$:

	$m_v(\phi) < 0$	$m_v(\phi) = 0$	$m_v(\phi) > 0$
V	0	0	$H^1(F_v, V)$
T	$H^1(F, T)_{\mathrm{tors}}$	$H^1(F_v, T)_{\mathrm{tors}}$	$H^1(F_v, T)$
W	0	$H^1(F_v, W)_{\mathrm{div}}$	$H^1(F_v, W)_{\mathrm{div}}$

If $v \nmid p$, then we have

$$H^1_f(F_v, V) = H^1_f(F_v, W) = 0;$$
$$H^1_f(F_v, T) = H^1(F_v, T)_{\mathrm{tors}},$$

irrespective of the values of i and j. $\square$

Definition 4.3. Suppose that $M \in \{W, W^*, W_{p^n}, W^*_{p^n}\}$ and that $\mathfrak{q} \in \{\mathfrak{p}, \mathfrak{p}^*\}$. If $c \in H^1(F, M)$, then we write $\mathrm{loc}_v(c)$ for the image of c in $H^1(F_v, M)$. We define

- the *true Selmer group* $\mathrm{Sel}(F, M)$ by

$$\mathrm{Sel}(F, M) = \left\{ c \in H^1(F, M) \mid \mathrm{loc}_v(c) \in H^1_f(F_v, M) \, \text{for all } v \right\};$$

- the *relaxed Selmer group* $\mathrm{Sel}_{\mathrm{rel}}(F, M)$ by

$$\mathrm{Sel}_{\mathrm{rel}}(F, M) = \left\{ c \in H^1(F, M) \mid \mathrm{loc}_v(c) \in H^1_f(F_v, M) \, \text{for all } v \text{ not dividing } p \right\};$$

- the *strict Selmer group* $\mathrm{Sel}_{\mathrm{str}}(L, M)$ by

$$\mathrm{Sel}_{\mathrm{str}}(F, M) = \{ c \in \mathrm{Sel}(F, M) \mid \mathrm{loc}_v(c) = 0 \, \text{for all } v \text{ dividing } p \};$$

- the $\mathfrak{q}$-*strict Selmer group* $\mathrm{Sel}_{\mathrm{str}(\mathfrak{q})}(F, M)$ by

$$\mathrm{Sel}_{\mathrm{str}(\mathfrak{q})}(F, M) = \{ c \in \mathrm{Sel}(F, M) \mid \mathrm{loc}_v(c) = 0 \, \text{for all } v \text{ dividing } \mathfrak{q} \};$$

- the $\mathfrak{q}$-*restricted Selmer group* (or simply *restricted Selmer group* for short when $\mathfrak{q}$ is understood) $\Sigma_{\mathfrak{q}}(F, M)$ by

$$\Sigma_{\mathfrak{q}}(F, M) = \{ c \in \mathrm{Sel}_{\mathrm{rel}}(F, M) \mid \mathrm{loc}_v(c) = 0 \, \text{for all } v \nmid \mathfrak{q} \}.$$

We also define

$$\check{\mathrm{Sel}}_?(F, T) := \varprojlim_n \mathrm{Sel}_?(F, W_{p^n}), \quad \check{\mathrm{Sel}}_?(F, T^*) := \varprojlim_n \mathrm{Sel}_?(F, W^*_{p^n}),$$
$$\check{\Sigma}_{\mathfrak{q}}(F, T) := \varprojlim_n \Sigma_{\mathfrak{q}}(F, W_{p^n}), \quad \check{\Sigma}_{\mathfrak{q}}(F, T^*) := \varprojlim_n \Sigma_{\mathfrak{q}}(F, W^*_{p^n}).$$

If L/K is an infinite extension, we define

$$\mathrm{Sel}_?(L, M) = \varinjlim \mathrm{Sel}_?(L', M), \quad \Sigma_{\mathfrak{q}}(L, M) = \varinjlim \Sigma_{\mathfrak{q}}(L', M),$$
$$\check{\mathrm{Sel}}_?(L, T) = \varinjlim \check{\mathrm{Sel}}_?(L', T), \quad \check{\mathrm{Sel}}_?(L, T^*) = \varinjlim \check{\mathrm{Sel}}_?(L', T^*),$$

where the direct limits are taken with respect to restriction over all subfields $L' \subset L$ finite over K.

For any extension L/K, we set

$$\mathrm{Sel}_?(L, M)^\wedge = X_?(L, M), \qquad \Sigma_{\mathfrak{q}}(L, M)^\wedge = X_{\mathfrak{q}}(L, M).$$

$\square$

Example 4.4. Suppose that $\phi = \psi^i \psi^{*j}$. By using the table given in Example 4.2, it is not hard to describe the true Selmer group $H^1_f(K,W)$ as i and j vary:

	$j<0$	$j=0$	$j>0$
$i<0$	$\mathrm{Sel}_{\mathrm{str}}(K,W)$	$\mathrm{Sel}_{\mathrm{str}}(K,W)$	$\Sigma_{\mathfrak{p}^*}(K,W)$
$i=0$	$\mathrm{Sel}_{\mathrm{str}}(K,W)$	0	$\Sigma_{\mathfrak{p}^*}(K,W)$
$i>0$	$\Sigma_{\mathfrak{p}}(K,W)$	$\Sigma_{\mathfrak{p}}(K,W)$	$\mathrm{Sel}_{\mathrm{rel}}(K,W)$

The reader may find it helpful to draw a diagram of the $i-j$ plane to illustrate the table above. $\square$

The following result is an analogue for restricted Selmer groups of a well known theorem of Coates about true Selmer groups associated to torsion points on CM elliptic curves [7, Theorem 12].

Theorem 4.5. *Let L be any field such that $\mathcal{F}_\infty \subseteq L \subseteq \mathfrak{F}_\infty$, and suppose that $\mathfrak{q} \in \{\mathfrak{p}, \mathfrak{p}^*\}$. Then there is an isomorphism*

$$X_{\mathfrak{q}}(L,W) \simeq \mathcal{X}^{(\mathfrak{q})}(L)(\phi^{-1})$$

of $\Lambda(L)$-modules. In particular, $X_{\mathfrak{q}}(L,W)$ is a torsion $\Lambda(L)$-module.

Proof. The proof of this result is very similar to that of [7, Theorem 12]. We begin by observing that , since $\mathcal{F}_\infty \subseteq L$, there are $\Lambda(L)$-module isomorphisms

$$\mathcal{X}^{(\mathfrak{q})}(L)(\phi^{-1}) \simeq \mathrm{Hom}(T, \mathcal{X}^{(\mathfrak{q})}(L)), \quad \mathcal{X}^{(\mathfrak{q})}(L)(\phi^{-1})^{\wedge} \simeq \mathrm{Hom}(\mathcal{X}^{(\mathfrak{q})}(L), W).$$

Therefore, in order to establish the desired result, it suffices to show that there is a natural isomorphism

$$\Sigma_{\mathfrak{q}}(L,W) \xrightarrow{\sim} \mathrm{Hom}(\mathcal{X}^{(\mathfrak{q})}(L), W). \tag{4.3}$$

This follows via an argument entirely analogous to that used to establish [7, Theorem 12]. $\square$

We now state a 'control theorem' for restricted Selmer groups.

Theorem 4.6. *Suppose that* $\mathfrak{q} \in \{\mathfrak{p}, \mathfrak{p}^*\}$.

(a) Let $I_{\mathcal{F}_\infty}$ *denote the kernel of the quotient map*

$$\Pi_{\mathcal{F}_\infty} : \Lambda(\mathfrak{F}_\infty) \to \Lambda(\mathcal{F}_\infty).$$

Then the kernel of the restriction map

$$\Sigma_{\mathfrak{q}}(\mathcal{F}_\infty, W) \to \Sigma_{\mathfrak{q}}(\mathfrak{F}_\infty, W)[I_{\mathcal{F}_\infty}]$$

is finite. A characteristic power series in $\Lambda(\mathcal{F}_\infty)$ *of the Pontryagin dual of the cokernel of this restriction map is given by*

$$e_F = (\gamma - \phi^{-1}(\gamma))^{-1} \prod_{v|\mathfrak{q}} (\gamma_v - \phi^{-1}(\gamma_v)),$$

where γ *is a topological generator of* $\mathrm{Gal}(\mathcal{F}_\infty/F)$*, and, for each place* v *of* $\mathcal{F}_\infty$ *lying above* $\mathfrak{q}$*,* γ_v *denotes a topological generator of* $\mathrm{Gal}(\mathcal{F}_{\infty,v}/F_v) \leq \mathrm{Gal}(\mathcal{F}_\infty/F)$.

Hence if $f \in \Lambda(\mathfrak{F}_\infty)$ *is a characteristic power series of* $X_{\mathfrak{q}}(\mathcal{F}_\infty, W)$*, then* $e_F^{-1}\Pi_{\mathcal{F}_\infty}(f) \in \Lambda(\mathcal{F}_\infty)$ *is a characteristic power series of* $X_{\mathfrak{q}}(\mathcal{F}_\infty, W)$.

(b) Suppose that L *is any field such that* $F \subseteq L \subseteq \mathcal{F}_\infty$*, and write* I_L *for the kernel of the quotient map* $\Lambda(\mathcal{F}_\infty) \to \Lambda(L)$*. Then the restriction map*

$$\Sigma_{\mathfrak{q}}(L, W) \to \Sigma_{\mathfrak{q}}(\mathcal{F}_\infty, W)[I_L]$$

is an isomorphism.

Hence the dual of this restriction map is an isomorphism of $\Lambda(L)$*-modules:*

$$X_{\mathfrak{q}}(\mathcal{F}_\infty, W)/I_L X_{\mathfrak{q}}(\mathcal{F}_\infty, W) \xrightarrow{\sim} X_{\mathfrak{q}}(L, W).$$

Proof. Let $\mathcal{N}$ denote the maximal extension of $\mathfrak{F}_\infty$ that is unramified away from all places of $\mathfrak{F}_\infty$ lying above p. Consider the following commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & \Sigma_{\mathfrak{q}}(\mathcal{F}_\infty, W) \arrow[r] \arrow[d, "\alpha"'] & H^1(\mathcal{N}/\mathcal{F}_\infty, W) \arrow[r, "\mathrm{loc}_{\mathfrak{q}^*}"] \arrow[d] & \prod_{v|\mathfrak{q}^*} H^1(\mathcal{N}_v/\mathcal{F}_{\infty,v}, W) \arrow[d] \\
0 \arrow[r] & \Sigma_{\mathfrak{q}}(\mathfrak{F}_\infty, W)[I_{\mathcal{F}_\infty}] \arrow[r] & H^1(\mathcal{N}/\mathfrak{F}_\infty, W)[I_{\mathcal{F}_\infty}] \arrow[r, "\mathrm{loc}_{\mathfrak{q}^*}"] & \prod_{v|\mathfrak{q}^*} H^1(\mathcal{N}_v/\mathfrak{F}_{\infty,v}, W)
\end{tikzcd}$$

in which the vertical arrows are the obvious restriction maps.

Applying the Snake Lemma (together with the inflation-restriction exact sequence) to this diagram yields the exact sequence

$$\begin{aligned} 0 \to \mathrm{Ker}(\alpha) \to H^1(\mathfrak{F}_\infty/\mathcal{F}_\infty, W) \xrightarrow{g_1} \prod_{v|\mathfrak{q}^*} H^1(\mathfrak{F}_{\infty,v}/\mathcal{F}_{\infty,v}, W^*) \to \\ \to \mathrm{Coker}(\alpha) \to H^2(\mathfrak{F}_\infty/\mathcal{F}_\infty, W) \xrightarrow{g_2} \prod_{v|\mathfrak{q}^*} H^2(\mathfrak{F}_{\infty,v}/\mathcal{F}_{\infty,v}, W) \to 0. \end{aligned} \tag{4.4}$$

Now,

$$\begin{aligned} &H^1(\mathfrak{F}_\infty/\mathcal{F}_\infty, W) \simeq \mathrm{Hom}(\mathrm{Gal}(\mathfrak{F}_\infty/\mathcal{F}_\infty), W), \\ &\prod_{v|\mathfrak{q}^*} H^1(\mathfrak{F}_{\infty,v}/\mathcal{F}_{\infty,v}, W) \simeq \prod_{v|\mathfrak{q}^*} \mathrm{Hom}(\mathrm{Gal}(\mathfrak{F}_{\infty,v}/\mathcal{F}_{\infty,v}), W), \end{aligned} \tag{4.5}$$

and, as $\mathrm{Gal}(\mathfrak{F}_\infty/\mathcal{F}_\infty) \simeq \Delta \times \mathbf{Z}_p$ with $p \nmid \Delta$, we have

$$\begin{aligned} &H^2(\mathfrak{F}_\infty/\mathcal{F}_\infty, W) \simeq H^0(\mathfrak{F}_\infty/\mathcal{F}_\infty, W) \simeq W, \\ &\prod_{v|\mathfrak{q}^*} H^2(\mathfrak{F}_{\infty,v}/\mathcal{F}_{\infty,v}, W) \simeq \prod_{v|\mathfrak{q}^*} H^0(\mathfrak{F}_{\infty,v}/\mathcal{F}_{\infty,v}, W) \simeq \prod_{v|\mathfrak{q}^*} W. \end{aligned}$$

We now deduce that g_1 is non-zero, and therefore has finite kernel (since $H^1(\mathfrak{F}_\infty/\mathcal{F}_\infty, W)$ is divisible), and that g_2 is injective. It follows from (4.4) that $\mathrm{Ker}(\alpha)$ is finite, and that there is an exact sequence

$$0 \to \mathrm{Ker}(\alpha) \to H^1(\mathfrak{F}_\infty/\mathcal{F}_\infty, W) \xrightarrow{g_1} \prod_{v|\mathfrak{q}^*} H^1(\mathfrak{F}_{\infty,v}/\mathcal{F}_{\infty,v}, W) \to \mathrm{Coker}(\alpha) \to 0. \tag{4.6}$$

It follows from (4.5) that

$$\mathrm{Char}_{\Lambda(\mathcal{F}_\infty)}\left(H^1(\mathfrak{F}_\infty/\mathcal{F}_\infty, W)\right)^\wedge = \gamma - \phi^{-1}(\gamma);$$
$$\mathrm{Char}_{\Lambda(\mathcal{F}_\infty)}\left(\prod_{v \mid \mathfrak{q}^*} H^1(\mathfrak{F}_{\infty,v}/\mathcal{F}_{\infty,v}, W)\right)^\wedge = \prod_{v \mid \mathfrak{q}^*}(\gamma_v - \phi^{-1}(\gamma_v)).$$

Hence we deduce from (4.6) that

$$\mathrm{Char}_{\Lambda(\mathcal{F}_\infty)}(\mathrm{Coker}(\alpha))^\wedge = e_F = (\gamma - \phi^{-1}(\gamma))^{-1}\prod_{v \mid \mathfrak{q}^*}(\gamma_v - \phi^{-1}(\gamma_v)),$$

as asserted.

(b) In this case we consider the commutative diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & \Sigma_{\mathfrak{q}}(L, W) & \longrightarrow & H^1(\mathcal{N}/L, W) & \xrightarrow{\mathrm{loc}_{\mathfrak{q}^*}} & \prod_{v \mid \mathfrak{q}^*} H^1(\mathcal{N}_v/L_v, W) \\
 & & \Big\downarrow{\scriptstyle \beta_1} & & \Big\downarrow{\scriptstyle \beta_2} & & \Big\downarrow{\scriptstyle \beta_3} \\
0 & \longrightarrow & \Sigma_{\mathfrak{q}}(\mathcal{F}_\infty, W)[I_L] & \longrightarrow & H^1(\mathcal{N}/\mathcal{F}_\infty, W) & \xrightarrow{\mathrm{loc}_{\mathfrak{q}^*}} & \prod_{v \mid \mathfrak{q}^*} H^1(\mathcal{N}/\mathcal{F}_{\infty,v}, W)
\end{array}$$

We have that

$$\mathrm{Ker}(\beta_2) = H^1(\mathcal{F}_\infty/L, W) = 0,$$
$$\mathrm{Ker}(\beta_3) = \prod_{v \mid \mathfrak{q}^*} H^1(\mathcal{F}_{\infty,v}/L_v, W) = 0,$$
$$\mathrm{Coker}(\beta_2) = H^2(\mathcal{F}_\infty/L, W) = 0,$$

(cf. [20, p. 40], for example), and so the Snake Lemma implies that β_1 is an isomorphism, as claimed. □

Corollary 4.7. *For any field L with $F \subseteq L \subseteq \mathcal{F}_\infty$, we have an isomorphism*

$$X_{\mathfrak{q}}(L, T) \simeq \mathcal{X}_{\mathfrak{q}}(\mathcal{F}_\infty)(\phi^{-1})/I_L(\mathcal{X}_{\mathfrak{q}}(\mathcal{F}_\infty)(\phi^{-1})) \tag{4.7}$$

of $\Lambda(L)$-modules.

Proof. This follows directly from Proposition 4.6 and Theorem 4.5. □

Remark 4.8. If we take $F = K$ in Proposition 4.6, then it is easy to check that $e_K \in \Lambda(\mathcal{K}_\infty)^\times$. We therefore see from Proposition 4.6(a) and Corollary 4.7 that the element $H^{(K)}_{\mathfrak{q},\rho} \in \Lambda(K_\infty)$ fixed in Section 3 is a characteristic power series of $X_{\mathfrak{q}}(K_\infty, W)$. Let us also remark that as $\mathcal{L}_{\mathfrak{q}} \in \Lambda(\mathfrak{K}_\infty)_{\mathcal{O}}$ is a characteristic power series of $\mathcal{X}_{\mathfrak{q}}(\mathfrak{K}_\infty)$, it follows that $\mathrm{Tw}_\phi(\mathcal{L}_{\mathfrak{q}})$ is a characteristic power series of $X_{\mathfrak{q}}(\mathfrak{K}_\infty, W)$. □

5. Kummer Theory

In this section we shall explain how to construct elements in restricted Selmer groups using twisted units. We begin by recording the following standard cohomological result.

Lemma 5.1. *Let F/K be any finite extension, and set $\mathcal{N}_n := \mathcal{F}^*_n\mathcal{K}_\infty$. Suppose that L and M are fields with $F \subseteq L \subseteq M \subseteq \mathcal{N}_n$. Then for every integer $m \geq 1$, the restriction maps*

$$H^1(L, W_{p^m}) \to H^1(M, W_{p^m}), \quad H^1(L, \mu_{p^m}) \to H^1(M, \mu_{p^m})$$

are injective, and they induce isomorphisms

$$H^1(L, W_{p^m}) \simeq H^1(M, W_{p^m})^{\mathrm{Gal}(M/L)}, \quad H^1(L, \mu_{p^m}) \simeq H^1(M, \mu_{p^m})^{\mathrm{Gal}(M/L)}.$$

A similar result holds if L and M are replaced by L_v and M_v with

$$F_v \subseteq L_v \subseteq M_v \subseteq \mathcal{N}_{m,v}$$

for any finite place v of F.

Proof. See, for example, [20, page 140]. □

We now recall some basic facts about twisting cohomology classes by Galois characters [26, II.4 and VI].

Fix generators $w = [w_n]$ of T and $w^* = [w^*_n]$ of T^*. Set

$$\zeta = [\zeta_n] = [e_n(w_n, w^*_n)] \in \mathbf{Z}_p(1).$$

Write $T^{*-1} := \mathrm{Hom}(T^*, \mathbf{Z}_p)$, and let $w^{*-1} = [w_n^{*-1}] \in T^{*-1}$ be the generator of T^{*-1} defined by $w_n^{*-1} : w_n^* \mapsto 1$. Observe that we have

$$T^{*-1} \otimes \mathbf{Z}_p(-1) = \mathrm{Hom}(T^*, \mathbf{Z}_p) \otimes \mathbf{Z}_p(1) \simeq \mathrm{Hom}(T^*, \mathbf{Z}_p(1)) \simeq T,$$

and that the image of $w^{*-1} \otimes \zeta \in T^{*-1} \otimes \mathbf{Z}_p(1)$ in $\mathrm{Hom}(T^*, \mathbf{Z}_p(1))$ is the map $w^* \mapsto \zeta$, which is in turn identified with $w \in T$ via the e_n-pairings.

Let F/K be a finite extension.

Lemma 5.2. *For each integer $n \geq 1$, the map*

$$\mu_{p^n} \to W_{p^n}; \quad \zeta_n \mapsto w_n$$

induces an isomorphism

$$\mathrm{Tw}^{(n)}_{\phi^{*-1}} : H^1(\mathcal{F}_n^*, \mu_{p^n}) \xrightarrow{\sim} H^1(\mathcal{F}_n^*, W_{p^n}).$$

Proof. This is straightforward, and follows immediately from the fact that $\mathrm{Gal}(\bar{F}/\mathcal{F}_n^*)$ acts trivially on w_n^*. □

Lemma 5.3. *Suppose that $c \in H^1(\mathcal{F}_n^*, \mathbf{Z}_p(1))$. Then the image of c under the composition of maps*

$$H^1(\mathcal{F}_n^*, W_{p^n}) \xrightarrow{(\mathrm{Tw}^{(n)}_{\phi^{*-1}})^{-1}} H^1(\mathcal{F}_n^*, \mu_{p^n}) \xrightarrow{\mathrm{Cores}} H^1(F, \mu_{p^n}) \xrightarrow{\mathrm{Tw}^{(n)}_{\phi^{*-1}}} H^1(\mathcal{F}_n^*, W_{p^n})$$

is equal to $\sum_{\sigma \in \mathrm{Gal}(\mathcal{F}_n^*/F)} \phi^{*-1}(\sigma) c^{\sigma}$.

Proof. See [26, Lemma II.4.3]. □

For each integer $n \geq 1$, let $\alpha_n : H^1(\mathcal{F}_n^*, W_{p^n}) \to H^1(\mathcal{F}_{n-1}^*, W_{p^{n-1}})$ be the composition of maps

$$H^1(\mathcal{F}_n^*, W_{p^n}) \xrightarrow{\mathrm{Cores}} H^1(\mathcal{F}_{n-1}^*, W_{p^n}) \xrightarrow{\times p} H^1(\mathcal{F}_{n-1}^*, W_{p^{n-1}}).$$

Lemma 5.4. *(a) There is a natural isomorphism*

$$\varprojlim H^1(\mathcal{F}_n^*, W_{p^n}) \simeq \varprojlim H^1(\mathcal{F}_n^*, T),$$

where the left-hand inverse limit is taken with respect to the maps α_n, and the right-hand inverse limit is taken with respect to the obvious corestriction maps.

(b) Suppose that $u = [u_n] \in \varprojlim H^1(\mathcal{F}_n^*, \mathbf{Z}_p(1))$, and, for each n, write $\mathrm{Tw}_{\phi^{*-1}}^{(n)}(u_n) \in H^1(\mathcal{F}_n^*, W_{p^n})$ for the image of u_n under the sequence of maps

$$H^1(\mathcal{F}_n^*, \mathbf{Z}_p(1)) \to H^1(\mathcal{F}_n^*, \mu_{p^n}) \xrightarrow{\mathrm{Tw}_{\phi^{*-1}}^{(n)}} H^1(\mathcal{F}_n^*, W_{p^n}).$$

Then

$$\alpha_n(\mathrm{Tw}_{\phi^{*-1}}^{(n)}(u_n)) = \mathrm{Tw}_{\phi^{*-1}}^{(n-1)}(u_{n-1}).$$

Hence it follows from part (a) above that the maps $\mathrm{Tw}_{\phi^{*-1}}^{(n)}$ induce a homomorphism

$$\begin{aligned} \mathrm{Tw}_{\phi^{*-1}} : \varprojlim H^1(\mathcal{F}_n^*, \mathbf{Z}_p(1)) &\to \varprojlim H^1(\mathcal{F}_n^*, T) \\ u &\mapsto \mathrm{Tw}_{\phi^{*-1}}(u) = [\mathrm{Tw}_{\phi^{*-1}}(u)_n] \end{aligned}$$

Proof. (a) See [26, Proposition VI.2.1].

(b) This follows via a routine computation. □

Definition 5.5. For each $u = [u_n] \in \varprojlim H^1(\mathcal{F}_n^*, \mathbf{Z}_p(1))$, we define $P_u(\phi) \in H^1(F, T)$ by

$$P_u(\phi) := \mathrm{Tw}_{\phi^{*-1}}(u)_0. \tag{5.1}$$

□

We shall study the behaviour of $P_u(\phi)$ using Kummer theory on the multiplicative group. The main result that we shall use to do this is the following.

Proposition 5.6. *(a) There is an isomorphism of $\mathrm{Gal}(\mathcal{F}_n^*/F)$-modules*

$$H^1(\mathcal{F}_n^*, W_{p^n}) \xrightarrow{\sim} \mathrm{Hom}(W_{p^n}^*, \mathcal{F}_n^{*\times}/\mathcal{F}_n^{*\times p^n}); \quad f \mapsto \tilde{f}. \tag{5.2}$$

For each place v of $\mathcal{F}_n^*$, there is also a corresponding local isomorphism

$$H^1(\mathcal{F}_{n,v}^*, W_{p^n}) \xrightarrow{\sim} \mathrm{Hom}(W_{p^n}^*, \mathcal{F}_{n,v}^{*\times}/\mathcal{F}_{n,v}^{*\times p^n}).$$

(b) There is an injective homomorphism

$$\kappa_\phi : H^1(F,T) \to \varprojlim H^1(\mathcal{F}_n^*, \mathbf{Z}_p(1)),$$

where the inverse limit is taken with respect to the obvious corestriction maps.

Proof. (a) The isomorphism (5.2) is defined as follows. We first identify $\mathcal{F}_n^{*\times}/\mathcal{F}_n^{*\times p^n}$ via Kummer theory, and then we define $\tilde{f}$ by $\tilde{f}(w_n^*) = \mathrm{Tw}^{(n)}_{\phi^{*-1}}(f)$. It is not hard to check that the map $f \mapsto \tilde{f}$ is a $\mathrm{Gal}(\mathcal{F}_n^*/F)$-isomorphism.

(b) Suppose that $c = [c_n] \in \varprojlim H^1(F, W_{p^n}) \simeq H^1(F,T)$, and consider the composition of maps

$$H^1(\mathcal{F}_{n+1}^*, \mu_{p^{n+1}}) \to H^1(\mathcal{F}_n^*, \mu_{p^{n+1}}) \to H^1(\mathcal{F}_n^*, \mu_{p^n}), \tag{5.3}$$

where the first arrow is given by corestriction and the second arrow is induced by the natural map $\mu_{p^{n+1}} \to \mu_{p^n}$. Recall from Lemma 5.1 that there is an isomorphism $H^1(F, W_{p^n}) \simeq H^1(\mathcal{F}_n^*, W_{p^n})^{\mathrm{Gal}(\mathcal{F}_n^*/F)}$. It is not dificult to check that (5.3) maps $\tilde{c}_{n+1}(w_{n+1}^*)$ to $\tilde{c}_n(w_n^*)$. We may therefore define

$$\tilde{c}(w) := [\tilde{c}_n(w_n^*)] \in \varprojlim H^1(\mathcal{F}_n^*, \mu_{p^n}),$$

where the inverse imit is taken with respect to the maps (5.3). Since

$$\varprojlim H^1(\mathcal{F}_n^*, \mu_{p^n}) \simeq \varprojlim H^1(\mathcal{F}_n^*, \mathbf{Z}_p(1)),$$

where the right-hand inverse limit is taken with respect to the obvious corestriction maps (see e.g. [26, Appendix B, Section B3]), we may therefore view $\tilde{c}(w^*)$ as being an element of $\varprojlim H^1(\mathcal{F}_n^*, \mathbf{Z}_p(1))$, and we write

$$\kappa_\phi(c) = [\kappa_\phi(c)_n] \in \varprojlim H^1(\mathcal{F}_n^*, \mathbf{Z}_p(1))$$

for this element.

It follows from the construction of κ_ϕ that for each integer $n \geq 1$, we have

$$\kappa_\phi(c)_n \equiv \mathrm{Tw}_{\phi^{*-1}}(c_n) \pmod{\mathcal{F}_n^{*\times p^n}}$$

in $H^1(\mathcal{F}_n^*, \mu_{p^n}) \simeq \mathcal{F}_n^{*\times}/\mathcal{F}_n^{*\times p^n}$. This implies that κ_ϕ is injective. $\square$

Corollary 5.7. *Suppose that $u = [u_n] \in \varprojlim H^1(\mathcal{F}_n^*, \mathbf{Z}_p(1))$. Then we have*

$$\kappa_\phi(P_u(\phi))_n \equiv \left(\sum_{\sigma \in \mathrm{Gal}(\mathcal{F}_n^*/F)} \phi^{*-1}(\sigma)\sigma \right) u_n \pmod{\mathcal{F}_n^{*\times p^n}}$$

in $H^1(\mathcal{F}_n^*, \mu_{p^n}) \simeq \mathcal{F}_n^{*\times}/\mathcal{F}_n^{*\times p^n}$.

Proof. This follows directly from Lemma 5.3 and the definition of κ_ϕ. $\square$

We remind the reader that for each construction we have carried out in this section, there are corresponding local constructions in which F is replaced by F_v for any finite place v of F.

Now set

$$\mathcal{I}_F^{(\phi^*)} := \mathrm{Ker}[\phi^* : \Lambda(\mathcal{F}_\infty^*) \to \mathbf{Z}_p],$$

and put

$$\vartheta_F^{(\phi^*)} := \gamma^* \phi^*(\gamma^{*-1}) - 1,$$

where γ^* is any topological generator of $\mathrm{Gal}(\mathcal{F}_\infty^*/F)$ such that $\log_p(\gamma^*) = p$. Then $\vartheta_F^{(\phi^*)}$ is a generator of the ideal $\mathcal{I}_F^{(\phi^*)}$.

For each integer $n \geq 1$, let $\vartheta_{F,n}^{(\phi^*)}$ denote the projection of $\vartheta_F^{(\phi^*)}$ into $\mathbf{Z}_p[\mathrm{Gal}(\mathcal{F}_n^*/F)]$.

Lemma 5.8. *We have*

$$\vartheta_{F,n}^{(\phi^*)} \cdot \sum_{\sigma \in \mathrm{Gal}(\mathcal{F}_n^*/F)} \phi^{*-1}(\sigma)\sigma \equiv -(p-1)p^n \mod p^n \mathcal{I}_F^{(\phi^*)} \mathbf{Z}_p[\mathrm{Gal}(\mathcal{F}_n^*/F)].$$

Proof. The proof of this assertion is identical to that of [23, Lemma 6.3]. $\square$

Proposition 5.9. *Suppose that $u = [u_n]$ and $\nu = [\nu_n]$ are elements of $\varprojlim H^1(\mathcal{F}_n^*, \mathbf{Z}_p(1))$ such that $u = \vartheta_F^{(\phi^*)} \cdot \nu$. Then $P_u(\phi) = 0$.*

Proof. Recall that we have an injection

$$\kappa_\phi : H^1(F,T) \to \varprojlim H^1(\mathcal{F}_n^*, \mathbf{Z}_p(1))$$

(see Proposition 5.6(b)), and so to prove the desired result, it suffices to show that $\kappa_\phi(P_u(\phi)) = 0$.

Now for each integer $n \geq 1$, Corollary 5.7 yields

$$\begin{aligned}
\kappa_\phi(P_u(\phi)_n &\equiv \left(\sum_{\sigma \in \mathrm{Gal}(\mathcal{F}_n^*/F)} \phi^{*-1}(\sigma)\sigma \right) u_n \pmod{\mathcal{F}_n^{*\times p^n}} \\
&\equiv \left(\sum_{\sigma \in \mathrm{Gal}(\mathcal{F}_n^*/F)} \phi^{*-1}(\sigma)\sigma \right) \vartheta_{F,n}^{(\phi^*)} \nu_n \pmod{\mathcal{F}_n^{*\times p^n}} \\
&\equiv -(p-1)p^n \nu_n \pmod{\mathcal{F}_n^{*\times p^n}} \\
&\equiv 1 \pmod{\mathcal{F}_n^{*\times p^n}}.
\end{aligned}$$

Hence $\kappa_\phi(P_u(\phi))_n$ is trivial for all n, and so it follows that $\kappa_\phi(P_u(\phi)) = 0$, as required. □

The following result describes how norm-coherent units may be used to construct elements of restricted Selmer groups.

Proposition 5.10. *Let $\mathfrak{q} \in \{\mathfrak{p}, \mathfrak{p}^*\}$, and suppose that $u = [u_n] \in H^1(\mathcal{F}_n^*, \mathbf{Z}_p(1))$. If*

$$\mathrm{loc}_v(u) \in \vartheta_F^{(\phi^*)} \cdot \varprojlim H^1(\mathcal{F}_{n,v}^*, \mathbf{Z}_p(1))$$

for every place v of F lying above $\mathfrak{q}^*$, then $P_u(\phi) \in \Sigma_{\mathfrak{q}}(F,T)$.

Proof. Proposition 5.9 (with F replaced by F_v for $v \mid \mathfrak{q}^*$) implies that

$$\mathrm{loc}_v(P_u(\phi)) = 0$$

for each place v of F lying above $\mathfrak{q}^*$. Since $\mathrm{Tw}_{\phi^{*-1}}(u) \in \varprojlim \mathrm{Sel}_{\mathrm{rel}}(\mathcal{F}_n^*, T)$ (cf. [26, Proposition B.3.3]), the result follows. □

We shall now recall a number of basic facts concerning Kummer pairings and cup products.

Definition 5.11. Suppose that F/K is a finite extension, and that $\mathfrak{q} \in \{\mathfrak{p}, \mathfrak{p}^*\}$. For each integer $n \geq 1$, we define a pairing

$$(-,-)^{(\phi)}_{F_{\mathfrak{q}},n} : H^1(\mathcal{F}_{n,\mathfrak{q}}, \mathbf{Z}_p(1)) \times H^1(F_{\mathfrak{q}}, W_{p^n}) \to W_{p^n} \tag{5.4}$$

by

$$(u_n, y_n)^{(\phi)}_{F_{\mathfrak{q}},n} = y_n([u_n, F^{ab}_{\mathfrak{q}}/F_{n,\mathfrak{q}}]) =: \alpha^{(\phi)}_{\mathfrak{q},n}(u_n, y_n) \cdot w_n,$$

with $\alpha^{(\phi)}_{\mathfrak{q},n}(u_n, y_n) \in \mathbf{Z}/p^n\mathbf{Z}$.

The pairings (5.4) fit together to yield a pairing

$$(-,-)^{(\phi)}_{F_{\mathfrak{q}}} : \varprojlim H^1(\mathcal{F}_{n,\mathfrak{q}}, \mathbf{Z}_p(1)) \times H^1(F_{\mathfrak{q}}, T) \to T$$

that is defined as follows. Suppose that $y = [y_n] \in \varprojlim H^1(F_{\mathfrak{q}}, W_{p^n}) \simeq H^1(F_{\mathfrak{q}}, T)$, and $u = [u_n] \in \varprojlim H^1(\mathcal{F}_{n,\mathfrak{q}}, \mathbf{Z}_p(1))$. Then we set

$$(u, y)^{(\phi)}_{F_{\mathfrak{q}}} = [(u_n, y_n)^{(\phi)}_{F_{\mathfrak{q}},n}] \in \varprojlim W_{p^n} = T.$$

Hence, if we write $\alpha^{(\phi)}_{F_{\mathfrak{q}}}(u, y) = [\alpha^{(\phi)}_{\mathfrak{q},n}(u_n, y_n)] \in \mathbf{Z}_p$, then we have that

$$(u, y)^{(\phi)}_{F_{\mathfrak{q}}} = \alpha^{(\phi)}_{F_{\mathfrak{q}}} \cdot w^*.$$

□

The following result describes the relationship between the Kummer pairing $(-,-)^{(\phi)}_{F_{\mathfrak{q}}}$ and the cup product pairing

$$\cup : H^1(F_{\mathfrak{q}}, T) \times H^1(F_{\mathfrak{q}}, T^*) \to \mathbf{Z}_p. \tag{5.5}$$

Proposition 5.12. *Suppose that $y = [y_n] \in H^1(F_{\mathfrak{q}}, T)$ and $y^* = [y^*_n] \in H^1(F_{\mathfrak{q}}, T^*)$. Then*

$$(\kappa_\phi(y), y^*)^{(\phi^*)}_{F_{\mathfrak{q}}} = (y \cup y^*) \cdot w^*,$$

i.e.

$$\alpha^{(\phi^*)}_{F_{\mathfrak{q}}}(\kappa_\phi(y), y^*) = [\alpha^{(\phi^*)}_{F_{\mathfrak{q}},n}(\kappa_\phi(y), y^*_n)] = (y \cup y^*).$$

Proof. For each integer $n \geq 1$, let

$$\cup : H^1(F_{\mathfrak{q}}, W_{p^n}) \times H^1(F_{\mathfrak{q}}, W^*_{p^n}) \to \mathbf{Z}/p^n\mathbf{Z}$$

be the cup product pairing 'at level n' afforded by (5.5). To prove the desired result, it suffices to show that we have

$$(\kappa_\phi(y)_n, y^*_n)^{(\phi^*)}_{F_n,\mathfrak{q}} = -(y_n \cup y^*_n) \cdot w^*_n$$

for every $n \geq 1$.

Recall that $\mathfrak{F}_{n,\mathfrak{q}} = \mathcal{F}^*_{n,\mathfrak{q}}(\mu_{p^n})$, and that there are $\mathrm{Gal}(F^c_{\mathfrak{q}}/\mathfrak{F}_{n,\mathfrak{q}})$-isomorphisms

$$W_{p^n} \xrightarrow{\sim} \mu_{p^n}; \quad w_n \mapsto e_n(w_n, w^*_n),$$
$$W^*_{p^n} \xrightarrow{\sim} \mu_{p^n}; \quad w^*_n \mapsto e_n(w_n, w^*_n),$$

which in turn induce isomorphisms of cohomology groups

$$H^1(\mathfrak{F}_{n,\mathfrak{q}}, W_{p^n}) \xrightarrow{\sim} H^1(\mathfrak{F}_{n,\mathfrak{q}}, \mu_{p^n}) \simeq \mathfrak{F}^\times_{n,\mathfrak{q}}/\mathfrak{F}^{\times p^n}_{n,\mathfrak{q}},$$
$$H^1(\mathfrak{F}_{n,\mathfrak{q}}, W^*_{p^n}) \xrightarrow{\sim} H^1(\mathfrak{F}_{n,\mathfrak{q}}, \mu_{p^n}) \simeq \mathfrak{F}^\times_{n,\mathfrak{q}}/\mathfrak{F}^{\times p^n}_{n,\mathfrak{q}}.$$

Via these isomorphisms, over $\mathfrak{F}_{n,\mathfrak{q}}$, the Kummer pairing $(-,-)^{(\phi^*)}_{\mathfrak{F}_{\mathfrak{q}},n}$ may be identified with the Hilbert pairing

$$(-,-) : \frac{\mathfrak{F}^\times_{n.\mathfrak{q}}}{\mathfrak{F}^{\times p^n}_{n,\mathfrak{q}}} \times \frac{\mathfrak{F}^\times_{n.\mathfrak{q}}}{\mathfrak{F}^{\times p^n}_{n,\mathfrak{q}}} \to \mu_{p^n}$$

defined by

$$(a, b) = \frac{(b^{1/p^n})^{\sigma_a}}{b^{1/p^n}},$$

where σ_a denotes the local Artin symbol $[a, F^{ab}_{\mathfrak{q}}/\mathfrak{F}_{n,\mathfrak{q}}]$, and b^{1/p^n} is any p^n-th root of b in $F^{ab}_{\mathfrak{q}}$.

We now recall (see e.g. [28, Chapter XIV]) that the Hilbert pairing may in turn be identified with a cup product pairing

$$\cup : H^1(\mathfrak{F}_{n,\mathfrak{q}}, \mu_{p^n}) \times H^1(\mathfrak{F}_{n,\mathfrak{q}}, \mu_{p^n}) \to \mu_{p^n}$$

so that

$$\frac{(b^{1/p^n})^{\sigma_a}}{b^{1/p^n}} = (a \cup b) \cdot \zeta_n.$$

Via functoriality of cup products, we therefore deduce that

$$(\kappa_\phi(y)_n, y_n^*)_{F_n,\mathfrak{q}}^{(\phi^*)} = -(y_n \cup y_n^*) \cdot w_n^*$$

for every $n \geq 1$, as required. $\square$

Corollary 5.13. *Suppose that F/K is a finite extension, and that $\mathfrak{q} \in \{\mathfrak{p}, \mathfrak{p}^*\}$. If $y^* \in H^1(F_\mathfrak{q}, T^*)$, then we have*

$$P_u(\phi) \cup y^* = \alpha_{F_\mathfrak{q}}^{(\phi)}(\mathrm{loc}_\mathfrak{q}(u), y^*).$$

$\square$

6. Formal groups and explicit reciprocity laws

In this section we shall recall various results that we need concerning explicit reciprocity laws, and we shall explain how these may be used to evaluate the cup products $\mathrm{loc}_\mathfrak{q}(P_u(\phi)) \cup y^*$ (cf. Corollary 5.13) in terms of certain p-adic measures associated to u.

6.1. **Formal groups.** Suppose that $\mathfrak{q} \in \{\mathfrak{p}, \mathfrak{p}^*\}$, and let $\mathbf{F}$ be a height one Lubin-Tate formal group defined over $O_{K,\mathfrak{q}}$. Recall that $[\zeta_n]$ denotes the generator of $\mathbf{Z}_p(1)$ that was fixed at the begining of this paper in Section 2. For each n, let $\hat{\zeta}_n$ denote the parameter of ζ_n on the multiplicative formal group $\hat{\mathbf{G}}_m$. We choose an isomorphism

$$\eta_\mathbf{F} : \hat{\mathbf{G}}_m \xrightarrow{\sim} \mathbf{F}; \quad \eta_\mathbf{F}(X) \in \mathcal{O}[[X]] \tag{6.1}$$

over $\mathcal{O}$, and we set

$$\nu_n = \nu_{\mathbf{F},n} := \eta_\mathbf{F}(\hat{\zeta}_n).$$

We write

$$\mathbf{F}[p^n] := O_{K,\mathfrak{q}} \cdot \nu_n$$

(where here $O_{K,\mathfrak{q}}$ acts on ν_n via $\mathbf{F}$) for the group of p^n-torsion points on $\mathbf{F}$. We have that $\nu = \nu_{\mathbf{F}} := [\nu_n]$ is a generator of the p-adic Tate module $T_{\mathbf{F}}$ of $\mathbf{F}$. We write

$$\kappa_{\mathbf{F}} : \mathrm{Gal}(\overline{K}_{\mathfrak{q}}/K_{\mathfrak{q}}) \to \mathbf{Z}_p^{\times}$$

for the formal group character afforded by Galois action on $T_{\mathbf{F}}$, and

$$\Omega_{\eta_{\mathbf{F}}} := \eta'_{\mathbf{F}}(0) \tag{6.2}$$

for the p-adic period associated to our choice of isomorphism $\eta_{\mathbf{F}}$. Then, for each $\sigma \in \mathrm{Gal}(\overline{K}_{\mathfrak{q}}/K_{\mathfrak{q}})$, we have

$$\Omega_{\eta_{\mathbf{F}}}^{\sigma} = (\kappa_{\mathbf{F}} \cdot \chi_{\mathrm{cyc}}^{-1})(\sigma^{-1})\Omega_{\eta_{\mathbf{F}}}. \tag{6.3}$$

We denote the formal group logarithm associated to $\mathbf{F}$ by $\lambda_{\mathbf{F}}(X) \in O_{K,\mathfrak{q}}[[X]]$, and we write $\log_{\mathfrak{q}}$ for the $\mathfrak{q}$-adic logarithm associated to $\mathbf{G}_m$.

For each integer $n \geq 1$, we set $L_n := K_{\mathfrak{q}}(\nu_n)$, and we write H_n for the unique unramified extension of $K_{\mathfrak{q}}$ of degree $p^{n-1}(p-1)$. We put $M_n := L_n H_n$, and we set

$$L_{\infty} := \cup_{n\geq 1} L_n, \quad H_{\infty} := \cup_{n \geq 1} H_n, \quad M_{\infty} := \cup_{n\geq 1} M_n. \tag{6.4}$$

We define $L_0 = H_0 = K_{\mathfrak{q}}$.

For each $n \geq 0$, there is an injective Coleman homomorphism

$$\mathrm{Col}_{H_n L_{\infty}/K_{\mathfrak{q}}} : U(H_n L_{\infty}) \to \Lambda_{\mathcal{O}}(H_n L_{\infty}); \quad \beta \mapsto \mu_{\beta}^{(n)}$$

(see [10, Chapter I]), and these maps combine to yield an injective homomorphism

$$\mathrm{Col}_{M_{\infty}/K_{\mathfrak{q}}} : U(M_{\infty}) \to \Lambda_{\mathcal{O}}(M_{\infty}); \quad \beta \mapsto \mu_{\beta}.$$

The Coleman map $\mathrm{Col}_{M_{\infty}/K_{\mathfrak{q}}}$ is canonical; in particular—and this will be of crucial use to us—it does not depend upon the choice of formal group $\mathbf{F}$ used in its construction (see [10, Proposition I.3.9]).

There is also an 'unramified Coleman map'

$$\mathrm{Col}^{\mathrm{ur}}_{H_{\infty}/K_{\mathfrak{q}}} : U(H_{\infty}) \to \Lambda_{\mathcal{O}}(H_{\infty})$$

that is defined as follows (cf. [23, Theorem 7.2]). Suppose that $\beta = [\beta_n] \in U(H_\infty)$, and write $\mathrm{Fr}_\mathfrak{q} \in \mathrm{Gal}(H_\infty/K_\mathfrak{q})$ for the Frobenius element. Then it follows via local class field theory that there exists

$$\alpha = [\alpha^{(n)}] \in U(M_\infty), \quad \alpha^{(n)} = [\alpha_m^{(n)}] \in U(H_n \cdot L_\infty), \tag{6.5}$$

such that for each n, we have

$$\alpha_0^{(n)} = \beta_n^{1-\mathrm{Fr}_\mathfrak{q}}. \tag{6.6}$$

This in turn implies that

$$[\mathrm{Col}_{H_nL_\infty/K_\mathfrak{q}}(\alpha^{(n)})] \in \varprojlim_n \Lambda_\mathcal{O}(L_\infty \cdot H_n) \simeq \Lambda_\mathcal{O}(M_\infty),$$

and we define

$$\mathrm{Col}^{\mathrm{nr}}_{H_\infty/K_\mathfrak{q}}(\beta) = [\mathrm{Col}_{H_nL_\infty/K_\mathfrak{q}}(\alpha^{(n)})].$$

The map $\mathrm{Col}^{\mathrm{nr}}_{H_\infty/K_\mathfrak{q}}$ is injective and is independent of all choices made in its definition.

We shall apply the above constructions in the setting afforded by the following result.

Proposition 6.1. *Let N_∞ be any totally ramified $\mathbf{Z}_p^\times$ extension of $K_\mathfrak{q}$, and let $\pi(N_\infty)$ be a uniformiser of $O_{K,\mathfrak{q}}$ that generates the group of universal norms of this extension. Then there exists a height one Lubin-Tate formal group $\mathbf{F}(N_\infty)$ associated to $\pi(N_\infty)$, such that $L_\infty = N_\infty$ (using the notation of* (6.4)*).*

Proof. This is a standard result which follows via local class field theory; see [17, Chapter V, §5], for example. ☐

6.2. **Explicit reciprocity laws.** We retain the notation established in the previous subsection.

Definition 6.2. If r is any non-zero integer, then there is a twisting homomorphism

$$\begin{aligned}\mathrm{Tw}_{\kappa_{\mathbf{F}}^r} : \varprojlim H^1(L_n, \mathbf{Z}_p(1)) &\to \varprojlim H^1(L_n, T_{\mathbf{F}}^{\otimes r}(1)) \\ \beta &\mapsto \mathrm{Tw}_{\kappa_{\mathbf{F}}^r}(\beta) = [\mathrm{Tw}_{\kappa_{\mathbf{F}}^r}(\beta)_n].\end{aligned}$$

We define $Q_\beta(\chi_{\mathrm{cyc}}\kappa_{\mathbf{F}}^r) \in H^1(K_{\mathfrak{q}}, T_{\mathbf{F}}^{\otimes r}(1))$ by

$$Q_\beta(\chi_{\mathrm{cyc}}\kappa_{\mathbf{F}}^r) = \mathrm{Tw}_{\kappa_{\mathbf{F}}^r}(\beta)_0. \tag{6.7}$$

□

For each non-zero integer r, we set

$$V_{\mathbf{F}}^{\otimes r}(1) := T^{\otimes r}(1) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p,$$

and we put $\nu^{\otimes r}(1) := \nu^{\otimes r} \otimes \zeta$. We write

$$\mathrm{DR}(V_{\mathbf{F}}^{\otimes r}(1)) := (B_{dR} \otimes_{K_{\mathfrak{q}}} V^{\otimes r}(1))^{\mathrm{Gal}(\overline{K}_{\mathfrak{q}}/K_{\mathfrak{q}})},$$

where B_{dR} denotes the de Rham period ring of Fontaine. We put

$$t_{\mathbf{F}} := \Omega_{\eta_{\mathbf{F}}} \cdot t,$$

where t denotes the canonical element of B_{dR} upon which $\mathrm{Gal}(\overline{K}_{\mathfrak{q}}/K_{\mathfrak{q}})$ acts via the p-adic cyclotomic character χ_{cyc}, and we identify $K_{\mathfrak{q}}$ with $\mathrm{DR}(V_{\mathbf{F}}^{\otimes r}(1))$ via the map

$$\begin{aligned}K_{\mathfrak{q}} &\xrightarrow{\sim} \mathrm{DR}(V_{\mathbf{F}}^{\otimes r}(1)) \\ x &\mapsto x t_{\mathbf{F}}^{-r} \otimes \nu(1)^{\otimes r}.\end{aligned} \tag{6.8}$$

With this identification, let

$$\mathrm{Exp}_{V_{\mathbf{F}}^{\otimes r}(1)} : K_{\mathfrak{q}} \to H^1_f(K_{\mathfrak{q}}, V_{\mathbf{F}}^{\otimes r}(1)) \subseteq H^1(K_{\mathfrak{q}}, V_{\mathbf{F}}^{\otimes r}(1))$$

and

$$\mathrm{Exp}^*_{V_{\mathbf{F}}^{\otimes r}(1)} : H^1(K_{\mathfrak{q}}, V_{\mathbf{F}}^{\otimes r}(1)) \to \frac{H^1(K_{\mathfrak{q}}, V_{\mathbf{F}}^{\otimes r}(1))}{H^1_f(K_{\mathfrak{q}}, V_{\mathbf{F}}^{\otimes r}(1))} \to K_{\mathfrak{q}}$$

denote the Bloch-Kato exponential and dual exponential maps respectively. We have

$$H^1_f(K_{\mathfrak{q}}, V_{\mathbf{F}}^{\otimes r}(1)) = \begin{cases} H^1(K_{\mathfrak{q}}, V_{\mathbf{F}}^{\otimes r}(1)) & \text{if } r \geq 1; \\ 0 & \text{if } r \leq -1. \end{cases}$$

If $r \leq -1$, then $\mathrm{Exp}^*_{V_{\mathbf{F}}^{\otimes r}(1)}$ is an isomorphism, while $\mathrm{Exp}_{V_{\mathbf{F}}^{\otimes r}(1)}$ is the zero map; if $r \geq 1$, then the reverse is true. We write

$$\mathrm{Log}_{V_{\mathbf{F}}^{\otimes r}(1)} : H^1(K_{\mathfrak{q}}, V_{\mathbf{F}}^{\otimes r}(1)) \to K_{\mathfrak{q}}$$

for the inverse of $\mathrm{Exp}_{V_{\mathbf{F}}^{\otimes r}(1)}$ when $r \geq 1$, and we call this map the *Bloch-Kato logarithm* associated to $V_{\mathbf{F}}^{\otimes r}(1)$.

If $y \in H^1(K_{\mathfrak{q}}, V_{\mathbf{F}}^{\otimes r})$ and $y^* \in H^1(K_{\mathfrak{q}}, V_{\mathbf{F}}^{\otimes(-r)}(1))$, then we have (at least up to sign):

$$y \cup y^* = \begin{cases} \mathrm{Log}_{V_{\mathbf{F}}^{\otimes r}}(y) \cdot \mathrm{Exp}^*_{V_{\mathbf{F}}^{\otimes(-r)}(1)}(y^*) & \text{if } r \geq 1 \\ \mathrm{Exp}^*_{V_{\mathbf{F}}^{\otimes r}}(y) \cdot \mathrm{Log}_{V_{\mathbf{F}}^{\otimes(-r)}(1)}(y^*) & \text{if } r \leq -1. \end{cases} \tag{6.9}$$

Definition 6.3. For each non-zero integer r and each character $\rho : \mathrm{Gal}(\overline{K}_{\mathfrak{q}}/K_{\mathfrak{q}}) \to \mathbf{Z}_p^{\times}$, set

$$\begin{aligned} \mathrm{Eul}_{\mathfrak{q}}(\rho, r) := &\left(1 - \left[\frac{\rho}{\chi_{\mathrm{cyc}}}\right]^r (\mathrm{Fr}_{\mathfrak{q}})\right)^{-1} \cdot (1 - \rho^r(\mathrm{Fr}_{\mathfrak{q}}))^{-1} \\ &\times \left(1 - \left[\frac{\chi_{\mathrm{cyc}}}{p \cdot \rho}\right]^r (\mathrm{Fr}_{\mathfrak{q}})\right) \cdot \left(1 - (p \cdot \rho)^{-r}(\mathrm{Fr}_{\mathfrak{q}})\right). \end{aligned}$$

□

Theorem 6.4. *Suppose that $\beta \in U(L_\infty) \subseteq \varprojlim H^1(L_n, \mathbf{Z}_p(1))$.*

(a) If $r \geq 1$, then

$$\mathrm{Log}_{V_{\mathbf{F}}^{\otimes r}(1)}(Q_\beta(\chi_{\mathrm{cyc}} \kappa_{\mathbf{F}}^r)) = (-1)^r \cdot (r-1)! \cdot \mathrm{Eul}_{\mathfrak{q}}(\kappa_{\mathbf{F}}, r) \cdot \Omega_{\eta_{\mathbf{F}}}^{-r} \cdot \int_{\mathcal{G}_{K_{\mathfrak{q}}}} \kappa_{\mathbf{F}}(x)^{-r} d\mu_\beta.$$

(b) If $r \leq -1$, then

$$\mathrm{Exp}^*_{V_{\mathbf{F}}^{\otimes r}(1)}(Q_\beta(\chi_{\mathrm{cyc}} \kappa_{\mathbf{F}}^r)) = \frac{1}{(-r-1)!} \cdot \mathrm{Eul}_{\mathfrak{q}}(\kappa_{\mathbf{F}}, r) \cdot \Omega_{\eta_{\mathbf{F}}}^{r} \cdot \int_{\mathcal{G}_{K_{\mathfrak{q}}}} \kappa_{\mathbf{F}}(x)^{-r} d\mu_\beta.$$

Proof. Part (a) is simply a restatement of [29, Theorem 3.3], in our setting, while part (b) is [29, Theorem 6.2]. These are in turn generalisations of earlier results of Colmez [9]. $\square$

We shall also require an analogue of Theorem 6.4 in which we consider cohomology classes that arise via twisting norm-coherent systems of local units by *unramified* characters of infinite order.

Suppose therefore that $\chi : \mathrm{Gal}(H_\infty/K_\mathfrak{q}) \to \mathbf{Z}_p^\times$ is a surjective character, and set $\chi^* := \chi^{-1} \cdot \chi_{\mathrm{cyc}}$. Then χ^* cuts out a totally ramified $\mathbf{Z}_p^\times$-extension $K_\mathfrak{q}^{(\chi^*)} = \cup_{n\geq 0} K_{\mathfrak{q},n}^{(\chi^*)}$ of $K_\mathfrak{q}$, and

$$\chi^*|_{\mathrm{Gal}(\overline{K}_\mathfrak{q}/K_\mathfrak{q}^{nr})} = \chi_{\mathrm{cyc}}|_{\mathrm{Gal}(\overline{K}_\mathfrak{q}/K_\mathfrak{q}^{nr})}.$$

It follows from Proposition 6.1 that there exists a height one Lubin-Tate formal group $\mathbf{F}(K_\mathfrak{q}^{(\chi^*)})$ defined associated to a uniformiser $\pi(K_\mathfrak{q}^{(\chi^*)})$ of $O_{K_\mathfrak{q}}$, such that the $\pi(K_\mathfrak{q}^{(\chi^*)})$-adic Tate module $T_{\mathbf{F}(K_\mathfrak{q}^{(\chi^*)})}$ of $\mathbf{F}(K_\mathfrak{q}^{(\chi^*)})$ is isomorphic to $\mathbf{Z}_p(\chi^*)$ as a $\mathrm{Gal}(\overline{K}_\mathfrak{q}/K)$-module.

As $\chi^* = \chi^{-1} \cdot \chi_{\mathrm{cyc}}$, there is a twisting homomorphism

$$\mathrm{Tw}_{\chi^{-1}} : U(H_\infty) \to \varprojlim H^1(H_n, T_{\mathbf{F}(K_\mathfrak{q}^{(\chi^*)})}); \quad \beta \mapsto \mathrm{Tw}_{\chi^{-1}}(\beta) = [\mathrm{Tw}_{\chi^{-1}}(\beta)_n].$$

For each $\beta \in U(H_\infty)$, we define $Q_\beta(\chi^*) \in H^1(K_\mathfrak{q}, T_{\mathbf{F}(K_\mathfrak{q}^{\chi^*})})$ by

$$Q_\beta(\chi^*) := \mathrm{Tw}_{\chi^{-1}}(\beta)_0. \tag{6.10}$$

A result of Bloch and Kato [5, Example 3.10.1] implies that if we identify $K_\mathfrak{q}$ with $\mathrm{DR}(V_{\mathbf{F}(K_\mathfrak{q}^{(\chi^*)})})$ as described above (see (6.8)), then the Bloch-Kato logarithm

$$\mathrm{Log}_{V_{\mathbf{F}(K_\mathfrak{q}^{(\chi^*)})}} : H^1(K_\mathfrak{q}, V_{\mathbf{F}(K_\mathfrak{q}^{(\chi^*)})}) \to K_\mathfrak{q}$$

and the formal group logarithm $\lambda_{\mathbf{F}(K_\mathfrak{q}^{(\chi^*)})}$ (extended via linearity to $H^1(K_\mathfrak{q}, V_{\mathbf{F}(K_\mathfrak{q}^{(\chi^*)})})$) are the same. In particular, we have that

$$\mathrm{Log}_{V_{\mathbf{F}(K_\mathfrak{q}^{(\chi^*)})}}(Q_\beta(\chi^*)) = \lambda_{\mathbf{F}(K_\mathfrak{q}^{(\chi^*)})}(\widehat{Q_\beta(\chi^*)}) \tag{6.11}$$

for every $\beta \in U(H_\infty)$.

For each integer $n \geq 1$, the isomorphism

$$\eta_{\mathbf{F}(K_{\mathfrak{q}}^{(\chi^*)})} : \hat{\mathbf{G}}_m \xrightarrow{\sim} \mathbf{F}(K_{\mathfrak{q}}^{(\chi^*)})$$

induces an isomorphism

$$\iota_n : \mu_{p^n} \xrightarrow{\sim} \mathbf{F}(K_{\mathfrak{q}}^{(\chi^*)})[p^n]; \quad \zeta_n \mapsto z_n,$$

say. If we set $\mathcal{N}_n := K_{\mathfrak{q},n}^{(\chi^*)} \cdot H_\infty$, then ι_n induces an isomorphism (which we denote by the the same symbol)

$$\iota_n : H^1(\mathcal{N}_n, \mu_{p^n}) \xrightarrow{\sim} H^1(\mathcal{N}_n, \mathbf{F}(K_{\mathfrak{q}}^{(\chi^*)})[p^n])$$

which is $\mathrm{Gal}(\overline{K}_{\mathfrak{q}}/H_n)$-equivariant. Let $\mathfrak{m}_n$ denote the maximal ideal in the ring of integers of the completion of $\mathcal{N}_n$.

Proposition 6.5. *(a) The following diagram commutes:*

$$\begin{array}{ccccc} H^1(\mathcal{N}_n, \mu_{p^n}) & & \xrightarrow[\sim]{\iota_n} & & H^1(\mathcal{N}_n, \mathbf{F}(K_{\mathfrak{q}}^{(\chi^*)})[p^n]) \\ \uparrow & & & & \uparrow \\ \dfrac{\hat{\mathbf{G}}_m(\mathfrak{m}_n)}{\hat{\mathbf{G}}_m(\mathfrak{m}_n)^{p^n}} & \simeq \dfrac{O_{\mathcal{N}_n}^{\times}}{O_{\mathcal{N}_n}^{\times p^n}} & \xrightarrow[\sim]{\eta_{\mathbf{F}(K_{\mathfrak{q}}^{(\chi^*)})}} & & \dfrac{\mathbf{F}(K_{\mathfrak{q}}^{(\chi^*)})(\mathfrak{m}_n)}{p^n\mathbf{F}(K_{\mathfrak{q}}^{(\chi^*)})(\mathfrak{m}_n)}. \end{array}$$

(Here the vertical arrows denote the natural maps afforded by Kummer theory on $\hat{\mathbf{G}}_m$ and $\mathbf{F}(K_{\mathfrak{q}}^{(\chi^*)})$.)

(b) If $\hat{x} \in \hat{\mathbf{G}}_m(\mathfrak{m}_n)$, then

$$\lambda_{\mathbf{F}(K_{\mathfrak{q}}^{(\chi^*)})}(\eta(\hat{x})) \equiv \Omega_{\mathbf{F}(K_{\mathfrak{q}}^{(\chi^*)})} \cdot \log_{\mathfrak{q}}(\hat{x}) \pmod{\mathfrak{m}_n^{p^n}}$$

on $\hat{\mathbf{G}}_m(\mathfrak{m}_n)/\hat{\mathbf{G}}_m(\mathfrak{m}_n)^{p^n}$.

Proof. (a) This follows directly from the definitions of $\eta_{\mathbf{F}(K_{\mathfrak{q}}^{(\chi^*)})}$ and ι_n.

(b) (cf. [23, Corollary 9.2].) Observe that the map

$$\lambda_{\mathbf{F}(K_{\mathfrak{q}}^{(\chi^*)})} \circ \eta_{\mathbf{F}(K_{\mathfrak{q}}^{(\chi^*)})} : \hat{\mathbf{G}}_m \to \hat{\mathbf{G}}_a$$

is a multiple of the logarithm map $\log_{\mathfrak{q}}(1+X) \in O_{K,\mathfrak{q}}[[X]]$ of $\hat{\mathbf{G}}_m$. Comparing the derivatives of $\lambda_{\mathbf{F}(K_{\mathfrak{q}}^{(\chi^*)})} \circ \eta_{\mathbf{F}(K_{\mathfrak{q}}^{(\chi^*)})}$ and $\log_{\mathfrak{q}}$ at $X = 0$ yields

$$\lambda_{\mathbf{F}(K_{\mathfrak{q}}^{(\chi^*)})} \circ \eta_{\mathbf{F}(K_{\mathfrak{q}}^{(\chi^*)})}(X) = \Omega_{\mathbf{F}(K_{\mathfrak{q}}^{(\chi^*)})} \log_{\mathfrak{q}}(1+X),$$

and this implies the desired result. □

Recall (see (6.4)) that, with our present notation, we have that $M_\infty = K_{\mathfrak{q}}^{(\chi^*)} \cdot H_\infty$.

Theorem 6.6. *Suppose that $\beta \in U(H_\infty)$, and that $\chi : \mathrm{Gal}(H_\infty/K_{\mathfrak{q}}) \to \mathbf{Z}_p^\times$ is surjective. Set $\mu_\beta := \mathrm{Col}^{\mathrm{nr}}_{H_\infty/K_{\mathfrak{q}}}(\beta) \in \Lambda_{\mathcal{O}}(M_\infty)$. Then*

$$\mathrm{Log}_{V_{\mathbf{F}(K_{\mathfrak{q}}^{(\chi^*)})}}(Q_\beta(\chi^*)) = \left(1-\chi(\mathrm{Fr}_{\mathfrak{q}}^{-1})\right)\cdot\left(1-\frac{\chi(\mathrm{Fr}_{\mathfrak{q}})}{p}\right)^{-1}\cdot\Omega_{\mathbf{F}(K_{\mathfrak{q}}^{(\chi^*)})}\cdot\int_{\mathcal{G}_{K_{\mathfrak{q}}}} \chi(x)\cdot d\mu_\beta. \tag{6.12}$$

Proof. From (6.11) and Proposition 6.5(b), and applying (6.5)and (6.6), we obtain the following, where all congruences are taken modulo $\mathfrak{m}_n^{p^n}$:

$$\begin{aligned}
\mathrm{Log}_{V_{\mathbf{F}(K_{\mathfrak{q}}^{(\chi^*)})}}(Q_\beta(\chi^*)) &= \lambda_{\mathbf{F}(K_{\mathfrak{q}}^{(\chi^*)})}(\widehat{Q_\beta(\chi^*)}) \\
&\equiv \sum_{\sigma \in H_n/K_{\mathfrak{q}}} \lambda_{\mathbf{F}(K_{\mathfrak{q}}^{(\chi^*)})}(\widehat{\mathrm{Tw}_{\chi^{-1}}(\beta)_n}) \\
&\equiv \sum_{\sigma \in H_n/K_{\mathfrak{q}}} \left(\Omega_{\mathbf{F}(K_{\mathfrak{q}}^{(\chi^*)})} \cdot \log_{\mathfrak{q}}(\hat{\beta}_n)\right)^\sigma \\
&\equiv \Omega_{\mathbf{F}(K_{\mathfrak{q}}^{(\chi^*)})} \cdot \sum_{\sigma \in H_n/K_{\mathfrak{q}}} \chi^{-1}(\sigma) \cdot \log_{\mathfrak{q}}(\hat{\beta}_n^\sigma) \\
&\equiv \Omega_{\mathbf{F}(K_{\mathfrak{q}}^{(\chi^*)})} \cdot \sum_{\sigma \in H_n/K_{\mathfrak{q}}} \chi^{-1}(\sigma) \cdot \log_{\mathfrak{q}}(\widehat{\alpha_0^{(n)}}^{(1-\mathrm{Fr}_{\mathfrak{q}}^{-1})\sigma}) \\
&\equiv \Omega_{\mathbf{F}(K_{\mathfrak{q}}^{(\chi^*)})} \cdot (1-\chi(\mathrm{Fr}_{\mathfrak{q}}^{-1}))^{-1} \\
&\times \sum_{\sigma \in H_n/K_{\mathfrak{q}}} \chi^{-1}(\sigma) \cdot \log_{\mathfrak{q}}(\widehat{\alpha_0^{(n)}}^{\sigma}).
\end{aligned} \tag{6.13}$$

It follows from [10, II.4.6] that, writing $\mu_{\alpha^{(n)}} = \mathrm{Col}_{K_{\mathfrak{q}}^{(\chi^*)}H_n/K_{\mathfrak{q}}}(\alpha^{(n)})$, we have

$$\left(1 - \frac{\chi(\mathrm{Fr}_{\mathfrak{q}})}{p}\right) \cdot \sum_{\sigma \in H_n/K_{\mathfrak{q}}} \chi^{-1}(\sigma) \cdot \log_{\mathfrak{q}}(\widehat{\alpha_0^{(n)}}^{\sigma}) = \int_{\mathcal{G}_{K_{\mathfrak{q}}}} \chi(x) \cdot d\mu_{\alpha^{(n)}}. \tag{6.14}$$

We therefore deduce from (6.13) and (6.14) that

$$\begin{aligned} \mathrm{Log}_{V_{\mathbf{F}(K_{\mathfrak{q}}^{(\chi^*)})}}(Q_\beta(\chi^*)) &= \Omega_{\mathbf{F}(K_{\mathfrak{q}}^{(\chi^*)})} \cdot (1 - \chi(\mathrm{Fr}_{\mathfrak{q}}))^{-1} \cdot \left(1 - \frac{\chi(\mathrm{Fr}_{\mathfrak{q}})}{p}\right)^{-1} \\ &\times \lim_{n \to \infty} \int_{\mathcal{G}_{K_{\mathfrak{q}}}} \chi(x) \cdot d\mu_{\alpha^{(n)}} \\ &= \Omega_{\mathbf{F}(K_{\mathfrak{q}}^{(\chi^*)})} \cdot (1 - \chi(\mathrm{Fr}_{\mathfrak{q}}))^{-1} \cdot \left(1 - \frac{\chi(\mathrm{Fr}_{\mathfrak{q}})}{p}\right)^{-1} \\ &\times \int_{\mathcal{G}_{K_{\mathfrak{q}}}} \chi(x) \cdot d\mu_\beta, \end{aligned}$$

as asserted. □

6.3. **Global cohomology classes.** We shall now describe how Theorems 6.4 and 6.6 may be applied to the global cohomology classes $P_u(\phi) \in H^1(K, T)$ constructed in the previous section. In order to do this, we have to impose certain conditions on the extension $\mathcal{K}_\infty^*/K$ and upon the character ϕ^* which we shall now explain.

Definition 6.7. Let $\mathfrak{q} \in \{\mathfrak{p}, \mathfrak{p}^*\}$, and suppose that $\chi : \mathrm{Gal}(\overline{K}/K) \to \mathbf{Z}_p^\times$ is a character of infinite order. Write $\chi_{\mathfrak{q}}$ for the restriction of χ to $\mathrm{Gal}(\overline{K}_{\mathfrak{q}}/K_{\mathfrak{q}})$. We shall say that χ is *locally Lubin-Tate (LLT) at* $\mathfrak{q}$ *of type* $m_{\mathfrak{q}}(\chi) \in \mathbf{Z}$ if the following two properties are satisfied:

(a) $\chi_{\mathfrak{q}}$ is surjective;

(b) We have

$$\chi_{\mathfrak{q}} \mid_{\mathrm{Gal}(\overline{K}_{\mathfrak{q}}/K_{\mathfrak{q}}^{\mathrm{nr}})} = \chi_{\mathrm{cyc}}^{m_{\mathfrak{q}}(\chi)} \mid_{\mathrm{Gal}(\overline{K}_{\mathfrak{q}}/K_{\mathfrak{q}}^{\mathrm{nr}})} .$$

Plainly if χ is LLT at $\mathfrak{q}$ of type $m_{\mathfrak{q}}(\chi)$, then χ^{-1} is LLT at $\mathfrak{q}$ of type $-m_{\mathfrak{q}}(\chi)$.

The reason for this terminology is as follows. Let $K_{\mathfrak{q}}^{(\chi_{\mathfrak{q}})}/K_{\mathfrak{q}}$ denote the $\mathbf{Z}_p^{\times}$ extension cut out by χ. If $m_{\mathfrak{q}}(\chi) \neq 0$, then Proposition 6.1 implies that there is a height one Lubin-Tate formal group $\mathbf{F}(K_{\mathfrak{q}}^{(\chi_{\mathfrak{q}})})$ defined over $K_{\mathfrak{q}}$ such that $K_{\mathfrak{q}}^{(\chi_{\mathfrak{q}})}/K_{\mathfrak{q}}$ is the division tower associated to $\mathbf{F}(K_{\mathfrak{q}}^{(\chi_{\mathfrak{q}})})$. Over $K_{\mathfrak{q}}^{\mathrm{nr}}$, the formal groups $\mathbf{F}(K_{\mathfrak{q}}^{(\chi_{\mathfrak{q}})})$ and $\hat{\mathbf{G}}_m$ are isomorphic, and so (b) implies that

$$\chi_{\mathfrak{q}} \mid_{\mathrm{Gal}(\overline{K}_{\mathfrak{q}}/K_{\mathfrak{q}}^{\mathrm{nr}})} = \kappa_{\mathbf{F}(\mathcal{K}_{\mathfrak{q}}^{(\chi_{\mathfrak{q}})})}^{m_{\mathfrak{q}}(\chi)} \mid_{\mathrm{Gal}(\overline{K}_{\mathfrak{q}}/K_{\mathfrak{q}}^{\mathrm{nr}})} .$$

We therefore deduce that

$$\chi_{\mathfrak{q}} = \kappa_{\mathbf{F}(K_{\mathfrak{q}}^{(\chi_{\mathfrak{q}})})}^{m_{\mathfrak{q}}(\chi)}.$$

If $m_{\mathfrak{q}}(\chi) = 0$, then $K_{\mathfrak{q}}^{(\chi_{\mathfrak{q}})}/K_{\mathfrak{q}}$ is the unique unramified $\mathbf{Z}_p^{\times}$-extension of $K_{\mathfrak{q}}$. $\square$

Suppose now that ϕ^* is LLT at $\mathfrak{q}$ of type $m_{\mathfrak{q}}(\phi^*)$. If $m_{\mathfrak{q}}(\phi^*) \neq 0$, then we may identify T^* with $T_{\mathbf{F}(\mathcal{K}_{\mathfrak{q},\infty}^*)}^{\otimes m_{\mathfrak{q}}(\phi^*)}$ via the map $w^* \mapsto \nu^{\otimes m_{\mathfrak{q}}(\phi^*)}$. This is a $\mathrm{Gal}(\overline{K}_{\mathfrak{q}}/K_{\mathfrak{q}})$-isomorphism. (We remind the reader that this isomorphism depends upon a choice of isomorphism between the formal group $\mathbf{F}(\mathcal{K}_{\mathfrak{q},\infty}^*)$ and the multiplicative formal group $\hat{\mathbf{G}}_m$ over $\mathcal{O}$ (see (6.1)).) The element $\mathrm{loc}_{\mathfrak{q}}(P_u(\phi))$ (see (5.1)) is then identified with the element $Q_{\mathrm{loc}_{\mathfrak{q}}(u)}(\chi_{\mathrm{cyc}}\kappa_{\mathbf{F}(\mathcal{K}_{\mathfrak{q},\infty}^*)}^{-m_{\mathfrak{q}}(\phi^*)})$ (see (6.7)).

If $m_{\mathfrak{q}}(\phi^*) = 0$, then $\phi_{\mathfrak{q}}^*$ is unramified, and $\phi_{\mathfrak{q}} = \phi_{\mathfrak{q}}^{*-1}\cdot\chi_{\mathrm{cyc}}$ cuts out the totally ramified $\mathbf{Z}_p^{\times}$-extension $\mathcal{K}_{\mathfrak{q},\infty}$ of $K_{\mathfrak{q}}$. In this case, the element $\mathrm{loc}_{\mathfrak{q}}(P_u(\phi))$ is identified with the element $Q_{\mathrm{loc}_{\mathfrak{q}}(u)}(\phi_{\mathfrak{q}})$ of (6.10).

We introduce the following notation to enable us to state our results in a uniform fashion.

Definition 6.8. Suppose that ϕ^* is LLT at $\mathfrak{q}$ of type $m_{\mathfrak{q}}(\phi^*)$; so we have that

$$\phi_{\mathfrak{q}}^* = \kappa_{\mathbf{F}(\mathcal{K}_{\mathfrak{q},\infty}^*)}^{m_{\mathfrak{q}}(\phi^*)}.$$

(a) If $x \in H^1(K_{\mathfrak{q}}, T)$, we define

$$\mathfrak{Log}_V(x) = \begin{cases} \mathrm{Log}_V(x) & \text{if } m_{\mathfrak{q}}(\phi^*) \leq 0; \\ \mathrm{Exp}_V^*(x) & \text{if } m_{\mathfrak{q}}(\phi^*) \geq 1. \end{cases} \tag{6.15}$$

(b) Define

$$\mathfrak{Eul}_{\mathfrak{q}}(\phi^{*-1}) = \begin{cases} \mathrm{Eul}_{\mathfrak{q}}(\phi^{*-1}, -m_{\mathfrak{q}}(\phi^*)) & \text{if } m_{\mathfrak{q}}(\phi^*) \leq -1; \\ \left(1 - \phi^*_{\mathfrak{q}}(\mathrm{Fr}_{\mathfrak{q}})\right)^{-1} \cdot \left(1 - \frac{\phi^*_{\mathfrak{q}}(\mathrm{Fr}_{\mathfrak{q}})^{-1}}{p}\right)^{-1} & \text{if } m_{\mathfrak{q}}(\phi^*) = 0. \\ \mathrm{Eul}_{\mathfrak{q}}(\phi^{*-1}, -m_{\mathfrak{q}}(\phi^*)^{-1} & \text{if } m_{\mathfrak{q}}(\phi^*) \geq 1. \end{cases} \tag{6.16}$$

(c) Define

$$\Omega(\phi^*_{\mathfrak{q}}) = \begin{cases} (-1)^{m_{\mathfrak{q}}(\phi^*)} \cdot (-m_{\mathfrak{q}}(\phi^*) - 1)! \cdot \Omega^{m_{\mathfrak{q}}(\phi^*)}_{\eta_{\mathbf{F}(\mathcal{K}^*_{\mathfrak{q},\infty})}} & \text{if } m_{\mathfrak{q}}(\phi^*) \leq -1; \\ \Omega_{\eta_{\mathbf{F}(\mathcal{K}_{\mathfrak{q},\infty})}} & \text{if } m_{\mathfrak{q}}(\phi^*) = 0. \\ (m_{\mathfrak{q}}(\phi^*) - 1)! \cdot \Omega^{m_{\mathfrak{q}}(\phi^*)}_{\eta_{\mathbf{F}(\mathcal{K}^*_{\mathfrak{q},\infty})}} & \text{if } m_{\mathfrak{q}}(\phi^*) \geq 1. \end{cases} \tag{6.17}$$

□

The following result is now a direct consequence of Theorems 6.4 and 6.6.

Theorem 6.9. *Suppose that ϕ^* is LLT at $\mathfrak{q}$ of type $m_{\mathfrak{q}}(\phi^*)$. Then, using the notation established in Definition 6.8, we have that*

$$\mathfrak{Log}_V(\mathrm{loc}_{\mathfrak{q}}(P_u(\phi))) = \mathfrak{Eul}_{\mathfrak{q}}(\phi^{*-1}) \cdot \Omega(\phi^{*-1}_{\mathfrak{q}}) \cdot \int_{\mathcal{G}_{K_{\mathfrak{q}}}} \phi^*_{\mathfrak{q}}(x) \cdot d\mu_{\mathrm{loc}_{\mathfrak{q}}(u)}.$$

□

7. The p-adic height pairing

Let F/K be a finite extension. In this section we shall use the methods of [18] and [20] to construct a p-adic height pairing

$$[-,-]^{(\phi)}_{F,\mathfrak{q}} : \Sigma_{\mathfrak{q}^*}(F, T^*) \times \Sigma_{\mathfrak{q}}(F, T) \to \mathbf{Z}_p,$$

and we shall describe some of its properties.

Let us first recall the statement of the weak $\mathfrak{q}$-adic Leopoldt hypothesis for F.

Definition 7.1. Let M/K be any finite extension, and consider the diagonal injection

$$i_M : O_M^\times \to \prod_{v|\mathfrak{q}} O_{M,v}^\times.$$

Let $\overline{i_M(O_M^\times)}$ denote the $\mathfrak{q}$-adic closure of $i_M(O_M^\times)$ in $\prod_{v|\mathfrak{q}} O_{M,v}^\times$, and set

$$\delta(M) := \mathrm{rk}_{\mathbf{Z}}(O_M^\times) - \mathrm{rk}_{\mathbf{Z}_p}(\overline{i_M(O_M^\times)}).$$

The *weak* $\mathfrak{q}$*-adic Leopoldt hypothesis for* F asserts that the numbers $\delta(L')$ are bounded as L' runs through all finite extensions of F contained in $\mathcal{F}_\infty^*$. The *strong* $\mathfrak{q}$*-adic Leopoldt hypothesis for* F asserts that the numbers $\delta(L')$ are all equal to zero.

We remark that the strong Leopoldt hypothesis is known to hold for all abelian extensions of K (see [6]). $\square$

Next, we recall that $\mathcal{B}^{(\mathfrak{q})}(\mathcal{F}_\infty)$ denotes the maximal abelian pro-p extension of $\mathcal{F}_\infty$ which is unramified away from $\mathfrak{q}$ and totally split at all places lying above $\mathfrak{q}^*$, and that $\mathcal{Y}^{(\mathfrak{q})}(\mathcal{F}_\infty) := \mathrm{Gal}(\mathcal{B}^{(\mathfrak{q})}(\mathcal{F}_\infty)/\mathcal{F}_\infty)$. The construction of the pairing $[-,-]_{F,\mathfrak{q}}^{(\phi)}$ rests upon the following key result.

Theorem 7.2. *If the weak* $\mathfrak{q}$*-adic Leopoldt hypothesis holds for* F*, then there is a natural isomorphism*

$$\Psi_{F,\mathfrak{q}^*}^{(\phi^*)} : \Sigma_{\mathfrak{q}^*}(F, T^*) \xrightarrow{\sim} \mathrm{Hom}(T, \mathcal{Y}^{(\mathfrak{q})}(\mathcal{F}_\infty))^{\mathrm{Gal}(\mathcal{F}_\infty/F)}.$$

As the proof of this theorem is very similar to that of [18, Théorème 3.2], we shall just describe the main outlines, and we refer the reader to [18] for more details.

Recall from Proposition 5.6 that we have an isomorphism

$$H^1(\mathcal{F}_n, W_{p^n}^*) \xrightarrow{\sim} \mathrm{Hom}(W_{p^n}, \mathcal{F}_n^\times/\mathcal{F}_n^{\times p^n}); \quad f \mapsto \tilde{f},$$

and that there are similar local isomorphisms at each finite place of F. Suppose that $h \in \Sigma_{\mathfrak{q}^*}(\mathcal{F}_n, W_{p^n}^*)$. Then it follows from the local conditions defining $\Sigma_{\mathfrak{q}^*}(\mathcal{F}_n, W_{p^n}^*)$ that, for each finite place v of F, we have:

(a) $\tilde{h}(u) \in \mathcal{F}_{n,v}^{\times p^n}$ for all $v \mid \mathfrak{q}$;

(b) $p^n \mid v_{\mathcal{F}_n}(\tilde{h}(u))$ for all $v \nmid \mathfrak{q}^*$.

(There are no local conditions imposed at places lying above $\mathfrak{q}^*$.)

Now let $G_n := \mathrm{Gal}(\mathcal{F}_n/F)$, and write J_n for the group of finite ideles of $\mathcal{F}_n$. Let $V_{n,\mathfrak{q}}$ denote the subgroup of J_n consisting of those elements of J_n whose components are equal to 1 at all places dividing $\mathfrak{q}$, and are units at all places not dividing $\mathfrak{q}^*$. We set

$$C_{n,\mathfrak{q}} := J_n/(V_{n,\mathfrak{q}} \cdot \mathcal{F}_n), \quad \Omega_{n,\mathfrak{q}} := \prod_{v \mid \mathfrak{q}} \mu_{p^n}(\mathcal{F}_{n,v}),$$

and we note that the order of $\Omega_{n,\mathfrak{q}}$ remains bounded as n varies.

Proposition 7.3. *There is an exact sequence*

$$\mathrm{Hom}(W_{p^n}, \Omega_{n,\mathfrak{q}})^{G_n} \to \mathrm{Hom}(W_{p^n}, C_{n,\mathfrak{q}})^{G_n} \xrightarrow{\eta_n} \Sigma_{\mathfrak{q}^*}(F, W_{p^n}^*) \to 0. \tag{7.1}$$

Proof. The proof of this Proposition is identical, *mutatis mutandis*, to that of [18, Proposition 3.13]. $\square$

Now let η_n' be the map obtained from η_n via passage to the quotient by the kernel of η_n, and write $C_{n,\mathfrak{q}}(p)$ for the p-primary part of $C_{n,\mathfrak{q}}$. Then it may be shown exactly as on [18, pp. 387–389] that passing to inverse limits over the maps $\eta_n'^{-1}$ yields an isomorphism

$$\Xi_{F,\mathfrak{q}} : \varprojlim \check{\Sigma}_{\mathfrak{q}^*}(F, W_{p^n}^*) = \Sigma_{\mathfrak{q}^*}(F, T^*) \xrightarrow{\sim} \mathrm{Hom}(T, \varprojlim C_{n,\mathfrak{q}}(p))^{\mathrm{Gal}(\mathcal{F}_\infty/F)}.$$

(Here the inverse limit $\varprojlim C_{n,\mathfrak{q}}(p)$ is taken with respect to the norm maps $\mathcal{F}_n^\times \to \mathcal{F}_{n-1}^\times$.)

The proof of Theorem 7.2 is completed by the following result.

Proposition 7.4. *If the weak $\mathfrak{q}$-adic Leopoldt hypothesis holds for F, then there is an isomorphism*

$$\mathrm{Hom}(T, \varprojlim C_{n,\mathfrak{q}}(p))^{\mathrm{Gal}(\mathcal{F}_\infty/F)} \simeq \mathrm{Hom}(T, \mathcal{Y}^{(\mathfrak{q})}(\mathcal{F}_\infty))^{\mathrm{Gal}(\mathcal{F}_\infty/F)}.$$

Proof. This may be shown in the same way as [18, Lemme 3.18]. $\square$

We can now describe how the isomorphism $\Psi^{(\phi^*)}_{F,\mathfrak{q}^*}$ may be used to construct a p-adic height pairing

$$[-,-]^{(\phi)}_{F,\mathfrak{q}} : \Sigma_{\mathfrak{q}^*}(F,T^*) \times \Sigma_{\mathfrak{q}}(F,T) \to \mathbf{Z}_p.$$

Recall (see Theorem 4.6(b) that the restriction map

$$\Sigma_{\mathfrak{q}}(F,W) \to \Sigma_{\mathfrak{q}}(\mathcal{F}_\infty, W) \tag{7.2}$$

is injective, and that there is a natural isomorphism (see Theorem 4.5)

$$\Sigma_{\mathfrak{q}}(\mathcal{F}_\infty, W) \xrightarrow{\sim} \mathrm{Hom}(\mathcal{X}^{(\mathfrak{q})}(\mathcal{F}_\infty), W). \tag{7.3}$$

The local conditions defining the restricted Selmer group $\Sigma_{\mathfrak{q}}(F,W)$ imply that (7.2) and (7.3) induce an injection

$$\Sigma_{\mathfrak{q}}(F,W) \to \mathrm{Hom}(\mathcal{Y}^{(\mathfrak{q})}(\mathcal{F}_\infty), W), \tag{7.4}$$

and taking Pontryagin duals yields a surjection

$$\mathrm{Hom}(T, \mathcal{Y}^{(\mathfrak{q})}(\mathcal{F}_\infty)) \to X_{\mathfrak{q}}(F,W). \tag{7.5}$$

Composing this with the natural surjection

$$X_{\mathfrak{q}}(F,W) \to [\Sigma_{\mathfrak{q}}(F,W)_{\mathrm{div}}]^\wedge$$

and taking $\mathrm{Gal}(\mathcal{F}_\infty/F)$-invariants yields a homomorphism

$$\beta^{(\phi)}_{F,\mathfrak{q}} : \mathrm{Hom}(T, \mathcal{Y}^{(\mathfrak{q})}(\mathcal{F}_\infty))^{\mathrm{Gal}(\mathcal{F}_\infty/F)} \to [\Sigma_{\mathfrak{q}}(F,W)_{\mathrm{div}}]^\wedge.$$

Next, we observe that we have a canonical isomorphism

$$\begin{aligned}[\Sigma_{\mathfrak{q}}(F,W)_{\mathrm{div}}]^\wedge &\simeq \mathrm{Hom}(T_p(\Sigma_{\mathfrak{q}}(F,W)_{\mathrm{div}}), \mathbf{Z}_p)\\ &= \mathrm{Hom}(T_p(\Sigma_{\mathfrak{q}}(F,W)), \mathbf{Z}_p),\end{aligned}$$

where the last equality holds because

$$T_p(\Sigma_{\mathfrak{q}}(F,W)_{\mathrm{div}}) = T_p(\Sigma_{\mathfrak{q}}(F,W)).$$

Also, for each $n \geq 1$, we have a surjective map

$$\Sigma_{\mathfrak{q}}(F, W_{p^n}) \to \Sigma_{\mathfrak{q}}(F, W)_{p^n}$$

with finite kernel. Via passage to inverse limits, these yield a map

$$\check{\Sigma}_{\mathfrak{q}}(F, T) \to T_p(\Sigma_{\mathfrak{q}}(F, W))$$

which also has finite kernel.

It follows from the above discussion that we may view $\beta^{(\phi)}_{F,\mathfrak{q}}$ as a homomorphism

$$\beta^{(\phi)}_{F,\mathfrak{q}} : \mathrm{Hom}(T, \mathcal{Y}^{(\mathfrak{q})}(\mathcal{F}_\infty))^{\mathrm{Gal}(\mathcal{F}_\infty/F)} \to \mathrm{Hom}(\check{\Sigma}_{\mathfrak{q}}(F, T), \mathbf{Z}_p).$$

We thus obtain a map

$$\beta^{(\phi)}_{F,\mathfrak{q}} \circ \Psi^{(\phi^*)}_{F,\mathfrak{q}^*} : \check{\Sigma}_{\mathfrak{q}^*}(F, T^*) \to \mathrm{Hom}(\check{\Sigma}_{\mathfrak{q}}(F, T), \mathbf{Z}_p),$$

and this yields the desired pairing

$$[-,-]^{(\phi)}_{F,\mathfrak{q}} : \check{\Sigma}_{\mathfrak{q}^*}(F, T^*) \times \check{\Sigma}_{\mathfrak{q}}(F, T) \to \mathbf{Z}_p.$$

Definition 7.5. If $x_1, \ldots, x_m$ and $x^*_1, \ldots, x^*_m$ are $\mathbf{Z}_p$-bases modulo torsion of $\Sigma_{\mathfrak{q}}(F, T)$ and $\Sigma_{\mathfrak{q}^*}(F, T^*)$ respectively, then we define the regulator $\mathcal{R}^{(\phi)}_{F,\mathfrak{q}}$ associated to $[-,-]^{(\phi)}_{F,\mathfrak{q}}$ by

$$\mathcal{R}^{(\phi)}_{F,\mathfrak{q}} := \det([x^*_i, x_j]^{(\phi)}_{F,\mathfrak{q}}).$$

We conjecture that $\mathcal{R}^{(\phi)}_{F,\mathfrak{q}}$ is always non-zero. $\square$

We now turn to the local decomposition of $[-,-]^{(\phi)}_{F,\mathfrak{q}}$. Suppose that

$$y = [y_n] \in \check{\Sigma}_{\mathfrak{q}}(F, T), \qquad y^* = [y^*_n] \in \check{\Sigma}_{\mathfrak{q}^*}(F, T^*).$$

For each positive integer n, we define $q_{n,\mathfrak{q}^*}$ to be the map

$$q_{n,\mathfrak{q}^*} : \check{\Sigma}_{\mathfrak{q}^*}(F, T^*) \xrightarrow{\Psi^{(\phi^*)}_{F,\mathfrak{q}^*}} \mathrm{Hom}(T, \mathcal{Y}^{(\mathfrak{q})}(\mathcal{F}_\infty))^{\mathrm{Gal}(\mathcal{F}_\infty/F)} \to \mathrm{Hom}(W_{p^n}, C_{n,\mathfrak{q}})^{\mathrm{Gal}(\mathcal{F}_\infty/F)},$$

where the second arrow is the natural quotient map afforded by the isomorphism described in Proposition 7.4.

For each $\varsigma \in W_{p^n}$, let $n(\varsigma)$ denote the exact power of p that kills ς. Let $S_{n,\varsigma}(y_n^*)$ denote any representative of $\eta_n^{-1}(y_n^*)(\varsigma)$ in J_n. For each finite place v of K, define $\{y^*, y\}_{n,v}^{(\varsigma)}$ to be the unique element of $\mathbf{Z}_p/p^n\mathbf{Z}_p$ such that

$$\{y^*, y\}_{n,v}^{(\varsigma)} \cdot \varsigma = y_n([S_{n,\varsigma}(y_n^*)_v, F_v^{\mathrm{ab}}/\mathcal{F}_{n,v}]),$$

where $[S_{n,\varsigma}(y_n^*)_v, F_v^{\mathrm{ab}}/\mathcal{F}_{n,v}] \in \mathrm{Gal}(F_v^{\mathrm{ab}}/\mathcal{F}_{n,v})$ is the obvious local Artin symbol.

Proposition 7.6. *(cf.* [18, Lemma 3.19]*)*

(a) For any $\varsigma \in W_{p^n}$, we have

$$[y^*, y]_{F,\mathfrak{q}}^{(\phi)} \cdot \varsigma = y_n([q_{n,\mathfrak{q}^*}(y)(\varsigma), F^{\mathrm{ab}}/\mathcal{F}_n]), \tag{7.6}$$

where $[q_{n,\mathfrak{q}^*}(y)(\varsigma), F^{\mathrm{ab}}/\mathcal{F}_n] \in \mathrm{Gal}(F^{\mathrm{ab}}/\mathcal{F}_n)$ is the obvious global Artin symbol.

(b) We have

$$[y^*, y]_{F,\mathfrak{q}}^{(\phi)} \equiv \sum_v \{y^*, y\}_{n,v}^{(\varsigma)} \pmod{p^{n(\varsigma)}\mathbf{Z}_p}, \tag{7.7}$$

where the sum is over all finite places v of $\mathcal{F}_n$.

Proof. (a) This follows immediately from the following commutative diagram:

$$\begin{array}{ccccc}
\check{\Sigma}_{\mathfrak{q}^*}(F, T^*) & \xrightarrow{\Psi_{F,\mathfrak{q}^*}^{(\phi^*)}} & \mathrm{Hom}(T, \mathcal{Y}^{(\mathfrak{q})}(\mathcal{F}_\infty))^{\mathrm{Gal}(\mathcal{F}_\infty/F)} & \xrightarrow{\beta_{F,\mathfrak{q}}^{(\phi)}} & \mathrm{Hom}(\check{\Sigma}_{\mathfrak{q}}(K, T), \mathbf{Z}_p) \\
\downarrow & & \downarrow & & \downarrow \\
\Sigma_{\mathfrak{q}^*}(K, W_{p^n}^*) & \xrightarrow{\eta_n'^{-1}} & \dfrac{\mathrm{Hom}(W_{p^n}, C_{n,\mathfrak{q}})^{\mathrm{Gal}(\mathcal{F}_\infty/F)}}{\mathrm{Ker}(\eta_n)} & \longrightarrow & \mathrm{Hom}(\Sigma_{\mathfrak{q}}(F, W_{p^n}), \mathbf{Z}_p/p^n\mathbf{Z}_p)
\end{array}$$

In this diagram, the second arrow on the bottom row is induced by the map

$$f \mapsto (c \mapsto \{\varsigma \mapsto c([f(\varsigma), F^{\mathrm{ab}}/\mathcal{F}_n])\}), \qquad f \in \mathrm{Hom}(W_{p^n}, C_{n,\mathfrak{q}})^{\mathrm{Gal}(\mathcal{F}_\infty/F)}$$

and is well-defined because $[z, F^{\mathrm{ab}}/\mathcal{F}_n] = 0$ for all $z \in \Omega_{n,\mathfrak{q}}$. Note also that here we have canonically identified $\mathbf{Z}_p/p^n\mathbf{Z}_p$ with $\mathrm{Hom}(W_{p^n}, W_{p^n})$ via the map

$$\beta \mapsto \{\varsigma \mapsto \beta \cdot \varsigma\}.$$

(b) This follows from the local decomposition of the global Artin symbol afforded via class field theory, viz. if $\alpha \in J_n$, then

$$[\alpha, F^{\mathrm{ab}}/\mathcal{F}_n] = \prod_v [\alpha_v, F_v^{\mathrm{ab}}/\mathcal{F}_{n,v}],$$

where the product is over all finite places v of $\mathcal{F}_n$. □

Let us now explain how Proposition 7.6 may be applied to elements in restructed Selmer groups that are constructed via twisted units in Section 5. Suppose that $u = [u_n] \in \varprojlim H^1(\mathcal{F}_n, \mathbf{Z}_p(1))$. Suppose also that, for each place v of F with $v \mid \mathfrak{q}$, we have that $u = \vartheta_F^{(\phi)} \cdot \beta_v$ for some $\beta_v = [\beta_{v,n}] \in \varprojlim H^1(\mathcal{F}_{n,v}, \mathbf{Z}_p(1))$. Then Proposition 5.10 implies that $P_u(\phi^*) \in \Sigma_{\mathfrak{q}^*}(F, T^*)$. Suppose now that y is any element of $\Sigma_{\mathfrak{q}}(F, T)$. The following result, which expresses $[P_u(\phi^*), y]_{F,\mathfrak{q}}^{(\phi)}$ in terms of Kummer pairings and cup products, is an immediate consequence of Proposition 7.6 and Corollary 5.13.

Proposition 7.7. *We have that*

$$\begin{aligned}[P_u(\phi^*), y]_{F,\mathfrak{q}}^{(\phi)} &= \sum_{v \mid \mathfrak{q}} (\beta_v, \mathrm{loc}_v(y))_{F_v}^{(\phi)} \\ &= \sum_{v \mid \mathfrak{q}} P_{\beta_v}(\phi^*) \cup \mathrm{loc}_v(y).\end{aligned}$$

□

8. A leading term formula

We retain the notation of the previous sections. Recall that F_∞/F denotes the unque $\mathbf{Z}_p$-extension contained in $\mathcal{F}_\infty/F$. Set $\Gamma_F := \mathrm{Gal}(F_\infty)/F$, and fix a topological generator γ_F of Γ_F. We identify $\Lambda(F_\infty)$ with the power series ring $\mathbf{Z}_p[[X]]$ via the map $\gamma_F \mapsto X + 1$, and we let $H_{\mathfrak{q},\phi}^{(F)} \in \Lambda(F_\infty)$ be a characteristic power series of $X_{\mathfrak{q}}(F_\infty, W)$. In this section, we shall calculate the p-adic valuation of the leading coefficient of $H_{\mathfrak{q},\phi}^{(F)}$, assuming that the weak

$\mathfrak{q}$-adic Leopoldt hypothesis holds for F, and that the p-adic regulator $\mathcal{R}^{(\phi)}_{F,\mathfrak{q}}$ is non-zero.

The following result is a straightforward consequence of work of Ralph Greenberg on the structure of certain Galois groups.

Proposition 8.1. *Suppose that F satisfies the weak $\mathfrak{q}$-adic Leopoldt hypothesis. Then the $\Lambda(F_\infty)$-module $X_{\mathfrak{q}}(F_\infty, W)$ contains no non-trivial finite submodules.*

Proof. It is not difficult to show that a slight modification of the arguments given in [11, §4] may be used to prove that if F satisfies the weak $\mathfrak{q}$-adic Leopoldt hypothesis, then the $\Lambda(F_\infty)$-module $\mathcal{X}^{\mathfrak{q}}(F_\infty)$ has no non-trivial, finite submodules. For brevity, we omit the details. The result now follows from Theorems 4.6 and 4.5. □

Suppose now that the weak $\mathfrak{q}$-adic Leopoldt hypothesis holds for F, and that $\mathcal{R}^{(\phi)}_{F,\mathfrak{q}} \neq 0$, i.e. that the p-adic height pairing

$$[-,-]^{\phi}_{F,\mathfrak{q}} : \Sigma_{\mathfrak{q}^*}(F, T^*) \times \Sigma_{\mathfrak{q}}(F, T) \to \mathbf{Z}_p$$

is non-degenerate. Set

$$n^{(F)}_{\mathfrak{q}}(\phi) := \mathrm{rk}_{\mathbf{Z}_p}(\Sigma_{\mathfrak{q}}(F, T)).$$

Theorem 8.2. *With the above hypotheses and notation, we have that*

$$\mathrm{ord}_{X=0}\, H^{(F)}_{\mathfrak{q},\phi} = n^{(F)}_{\mathfrak{q}}(\phi),$$

and

$$\left.\frac{H^{(F)}_{\mathfrak{q},\phi}}{X^{n^{(F)}_{\mathfrak{q}}(\phi)}}\right|_{X=0} \sim |\Sigma_{\mathfrak{q}}(F, W)_{/\,\mathrm{div}}| \cdot |\check{\Sigma}_{\mathfrak{q}}(F, T)_{\mathrm{tors}}| \cdot \mathcal{R}^{(\phi)}_{F,\mathfrak{q}}.$$

Proof. We first observe that there is a surjective homomorphism

$$X_{\mathfrak{q}}(F_\infty, W) \to [\Sigma_{\mathfrak{q}}(F, W)_{\mathrm{div}}]^{\wedge};$$

this implies that $H^{(F)}_{\mathfrak{q},\phi}$ is divisible by $X^{n^{(F)}_{\mathfrak{q}}(\phi)}$. Let Z_∞ denote the kernel of this map. Then the Snake Lemma yields the exact sequence

$$0 \to (Z_\infty)^{\Gamma_F} \to X_{\mathfrak{q}}(F_\infty, W)^{\Gamma_F} \xrightarrow{\xi_F} [\Sigma_{\mathfrak{q}}(F, W)_{\mathrm{div}}]^{\wedge} \to$$
$$\to (Z_\infty)_{\Gamma_F} \to X_{\mathfrak{q}}(F_\infty, W)_{\Gamma_F} \to [\Sigma_{\mathfrak{q}}(F, W)_{\mathrm{div}}]^{\wedge} \to 0.$$

We now observe that the kernel of the last map

$$X_{\mathfrak{q}}(F_\infty, W)_{\Gamma_F} \to [\Sigma_{\mathfrak{q}}(F, W)_{\mathrm{div}}]^{\wedge}$$

is dual to the cokernel of the map

$$\Sigma_{\mathfrak{q}}(F, W)_{\mathrm{div}} \to \Sigma_{\mathfrak{q}}(F_\infty, W)^{\Gamma_F}.$$

Since $\Sigma_{\mathfrak{q}}(F, W) \simeq \Sigma_{\mathfrak{q}}(F_\infty, W)^{\Gamma_F}$ (via Theorem 4.6(b)), it follows that this cokernel is isomorphic to $\Sigma_{\mathfrak{q}}(F, W)_{/\,\mathrm{div}}$, which is finite.

We therefore deduce that the multiplicity of X in $H^{(F)}_{\mathfrak{q},\phi}$ is equal to $n^{(F)}_{\mathfrak{q}}(\phi)$ if and only if $(Z_\infty)_{\Gamma_F}$ is finite, which in turn is the case if and only if the cokernel of ξ_F is finite. Recall that (see Theorem 4.5)

$$X_{\mathfrak{q}}(F_\infty, W)^{\Gamma_F} \simeq \mathrm{Hom}(T, \mathcal{X}^{\mathfrak{q}}(\mathcal{F}_\infty))^{\mathrm{Gal}(\mathcal{F}_\infty/F)},$$

and note that the homomorphism ξ_F may be written as the following composition of maps

$$\mathrm{Hom}(T, \mathcal{X}^{(\mathfrak{q})}(F_\infty))^{\mathrm{Gal}(\mathcal{F}_\infty/F)} \to \mathrm{Hom}(T, \mathcal{Y}^{(\mathfrak{q})}(F_\infty))^{\mathrm{Gal}(\mathcal{F}_\infty/F)} \to \Sigma_{\mathfrak{q}}(F, W)^{\wedge} \to$$
$$\to [\Sigma_{\mathfrak{q}}(F, W)_{/\,\mathrm{div}}]^{\wedge}$$

(see (7.4), (7.5)). It follows that the cokernel of ξ_F is finite if and only if the p-adic height pairing $[-,-]^{(\phi)}_{F,\mathfrak{q}^*}$ is non-degenerate.

We now see that if $[-,-]^{(\phi)}_{F,\mathfrak{q}^*}$ is non-degenerate, then $(Z_\infty)_{\Gamma_F}$ is finite. This implies that $(Z_\infty)^{\Gamma_F}$ is also finite, whence it follows via Proposition 8.1 that $(Z_\infty)^{\Gamma_F} = 0$. Hence we have

$$\left.\frac{H^{(F)}_{\mathfrak{q},\phi}}{X^{n^{(F)}_{\mathfrak{q}}(\phi)}}\right|_{X=0} \sim |(Z_\infty)_{\Gamma_F}| \sim |\Sigma_{\mathfrak{q}}(F, W)_{/\,\mathrm{div}}| \cdot |\operatorname{Coker}(\xi_F)|.$$

Now

$$\begin{aligned}
|\operatorname{Coker}(\xi_F)| &= [(\Sigma_{\mathfrak{q}}(F,W)_{\mathrm{div}})^{\wedge} : \xi_F(X_{\mathfrak{q}}(F_\infty,W)^{\Gamma_F})] \\
&= [T_p(\Sigma_{\mathfrak{q}}(F,W)) : \Psi_F(\check{\Sigma}_{\mathfrak{q}}(F,T))] \\
&= \mathcal{R}^{(\phi^*)}_{F,\mathfrak{q}^*} \cdot \left| \left[\operatorname{Ker}(\check{\Sigma}_{\mathfrak{q}}(F,T) \to T_p(\Sigma_{\mathfrak{q}}(F,W)))\right] \right| \\
&= \mathcal{R}^{(\phi^*)}_{F,\mathfrak{q}^*} \cdot |\check{\Sigma}_{\mathfrak{q}}(F,T)_{\mathrm{tors}}|.
\end{aligned}$$

Hence

$$\left.\frac{H^{(F)}_{\mathfrak{q},\phi}}{X^{n^{(F)}_{\mathfrak{q}}(\phi)}}\right|_{X=0} \sim |\Sigma_{\mathfrak{q}}(F,W)_{/\mathrm{div}}| \cdot |\check{\Sigma}_{\mathfrak{q}}(F,T)_{\mathrm{tors}}| \cdot \mathcal{R}^{(\phi^*)}_{F,\mathfrak{q}^*},$$

as claimed. □

Corollary 8.3. *We have that*

$$\operatorname{ord}_{s=1} L_{\mathfrak{q}}(\phi,s) \geq n^{(K)}_{\mathfrak{q}}(\phi),$$

with equality if and only if $\mathcal{R}^{(\phi^*)}_{K,\mathfrak{q}^*} \neq 0$*. If* $\mathcal{R}^{(\phi^*)}_{K,\mathfrak{q}^*} \neq 0$*, then*

$$\mathcal{L}^{(n_{\mathfrak{q}}(\phi))}_{\mathfrak{q}}(\phi) \sim |\Sigma_{\mathfrak{q}}(K,W)_{/\mathrm{div}}| \cdot |\check{\Sigma}_{\mathfrak{q}}(K,T)_{\mathrm{tors}}| \cdot \mathcal{R}^{(\phi^*)}_{K,\mathfrak{q}^*},$$

Proof. This is a direct consequence of Theorem 8.2 and its proof (see also Remark 4.8). □

9. Restricted Selmer groups over K

In this section we shall use Poitou-Tate duality to study the relationships between the ranks of different Selmer groups over K. Throughout this section, we take $F = K$, and so (in accord with our earlier notation), we write

$$n_{\mathfrak{q}}(\phi) = n^{(K)}_{\mathfrak{q}}(\phi) := \operatorname{rk}_{\mathbf{Z}_p}(\Sigma_{\mathfrak{q}}(K,T)). \tag{9.1}$$

We set

$$n_{\mathrm{str}}(\phi) := \operatorname{rk}_{\mathbf{Z}_p}(\mathrm{Sel}_{\mathrm{str}}(K,T)), \quad n_{\mathrm{rel}}(\phi) := \operatorname{rk}_{\mathbf{Z}_p}(\mathrm{Sel}_{\mathrm{rel}}(K,T)),$$

and we let $r_{\mathfrak{q}}(\phi)$ denote the $\mathbf{Z}_p$-rank of the image of the localisation map

$$\mathrm{loc}_{\mathfrak{q}} : \Sigma_{\mathfrak{q}}(K,T) \to H^1(K_{\mathfrak{q}},T).$$

Lemma 9.1. *We have that* $\mathrm{rk}_{\mathbf{Z}_p}(H^1(K_{\mathfrak{q}},T) = 1$. *Hence* $r_{\mathfrak{q}}(\phi)$ *is equal to* 0 *or* 1.

Proof. The first assertion follows from [13, Proposition 1, p.109], while the second assertion is an immediate consequence of the first. □

Lemma 9.2. *We have that*

$$n_{\mathfrak{q}}(\phi) = n_{\mathrm{str}}(\phi) + r_{\mathfrak{q}}(\phi). \tag{9.2}$$

and

$$n_{\mathfrak{q}}(\phi) = n_{\mathrm{rel}}(\phi) + r_{\mathfrak{q}^*}(\phi) \tag{9.3}$$

Proof. The first equality follows at once from the exact sequence

$$0 \to \mathrm{Sel}_{\mathrm{str}}(K,T) \to \Sigma_{\mathfrak{q}}(K,T) \xrightarrow{\mathrm{loc}_{\mathfrak{q}}} H^1(K_{\mathfrak{q}},T),$$

while the second follows from

$$0 \to \Sigma_{\mathfrak{q}}(\phi) \to \mathrm{Sel}_{\mathrm{rel}}(K,T) \xrightarrow{\mathrm{loc}_{\mathfrak{q}^*}} H^1(K_{\mathfrak{q}^*},T).$$

□

Lemma 9.3. *We have that*

$$n_{\mathrm{rel}}(\phi) = n_{\mathfrak{q}}(\phi) - r_{\mathfrak{q}^*}(\phi) + 1.$$

Proof. We first observe that the Poitou-Tate exact sequence yields

$$0 \to \Sigma_{\mathfrak{q}}(K,T) \to \mathrm{Sel}_{\mathrm{rel}}(K,T) \xrightarrow{\alpha} H^1(K_{\mathfrak{q}^*},T) \to \Sigma_{\mathfrak{q}^*}(K,W^*)^{\wedge}. \tag{9.4}$$

The cokernel of α is equal to the Pontryagin dual of the image of the localisation map

$$\mathrm{loc}_{\mathfrak{q}^*} : \Sigma_{\mathfrak{q}^*}(K,W^*) \to H^1(K_{\mathfrak{q}^*},W^*),$$

and so has $\mathbf{Z}_p$ rank $r_{\mathfrak{q}^*}(\phi^*)$. Hence

$$\mathrm{rk}_{\mathbf{Z}_p}(\mathrm{Im}(\alpha)) = 1 - r_{\mathfrak{q}^*}(\phi^*),$$

and so

$$n_{\mathrm{rel}}(\phi) = n_{\mathfrak{q}}(\phi) - r_{\mathfrak{q}^*}(\phi^*) + 1,$$

as claimed. □

Proposition 9.4. *We have that*

$$|r_{\mathfrak{q}}(\phi) - r_{\mathfrak{q}^*}(\phi)| = |n_{\mathfrak{q}}(\phi) - n_{\mathfrak{q}^*}(\phi)| = 1.$$

Proof. The equality $|r_{\mathfrak{q}}(\phi) - r_{\mathfrak{q}^*}(\phi)| = 1$ follows from (9.3) and Lemma 9.3 (with $\mathfrak{q}$ replaced by $\mathfrak{q}^*$). The equality $|n_{\mathfrak{q}}(\phi) - n_{\mathfrak{q}^*}(\phi)| = 1$ is then a direct consequence of (9.2) for $n_{\mathfrak{q}}(\phi)$ and $n_{\mathfrak{q}^*}(\phi)$. □

Proposition 9.5. *If the p-adic height pairing $[-,-]_{K,\mathfrak{q}}^{(\phi)}$ is non-degenerate, then we have*

$$r_{\mathfrak{q}}(\phi) = r_{\mathfrak{q}^*}(\phi^*).$$

Proof. The pairing $[-,-]_{K,\mathfrak{q}}^{(\phi)}$ yields a pairing

$$[-,-]_{K,\mathrm{str}}^{(\phi)} : \mathrm{Sel}_{\mathrm{str}}(K,T^*) \times \mathrm{Sel}_{\mathrm{str}}(K,T) \to \mathbf{Z}_p$$

via restriction. We claim that if $[-,-]_{K,\mathfrak{q}}^{(\phi)}$ is non-degenerate, then so is $[-,-]_{K,\mathrm{str}}^{(\phi)}$. To see why this is so, suppose that $x \in \mathrm{Sel}_{\mathrm{str}}(K,T^*)$ satisfies $[x,y]_{K,\mathrm{str}}^{(\phi)}$ for all $y \in \mathrm{Sel}_{\mathrm{str}}(K,T)$. As $[-,-]_{K,\mathfrak{q}}^{(\phi)}$ is non-degenerate by hypothesis, it follows that $\mathrm{Sel}_{\mathrm{str}}(K,T)$ is strictly contained in $\Sigma_{\mathfrak{q}}(K,T)$, and that $r_{\mathfrak{q}}(\phi) = 1$. It is not hard to check that for any $z \in \Sigma_{\mathfrak{q}}(K,T)$ satisfying $\mathrm{loc}_{\mathfrak{q}}(z) \neq 0$, we have that $[\alpha,z]_{K,\mathfrak{q}}^{(\phi)} = 0$ for all $\alpha \in \mathrm{Sel}_{\mathrm{str}}(K,T^*)$. This implies that $[x,y]_{K,\mathfrak{q}}^{(\phi)} = 0$ for all $y \in \Sigma_{\mathfrak{q}}(K,T)$, which contradicts $[-,-]_{K,\mathfrak{q}}^{(\phi)}$ being non-degenerate.

It therefore follows that if $[-,-]_{K,\mathfrak{q}}^{(\phi)}$ is non-degenerate, then $n_{\mathfrak{q}}(\phi) = n_{\mathfrak{q}^*}(\phi^*)$ and $n_{\mathrm{str}}(\phi) = n_{\mathrm{str}}(\phi^*)$. We deduce from Lemma 9.2 that $r_{\mathfrak{q}}(\phi) = r_{\mathfrak{q}^*}(\phi^*)$, as asserted. □

To continue our analysis, let us suppose that $\mathfrak{q}$ is chosen so that $r_{\mathfrak{q}}(\phi) = 1$ (the other possible cases will follow via symmetry). Then we have that $r_{\mathfrak{q}}(\phi^*) = r_{\mathfrak{q}^*}(\phi) = 0$, $n_{\mathfrak{q}}(\phi) = n_{\mathrm{rel}}(\phi)$, $n_{\mathfrak{q}^*}(\phi) = n_{\mathrm{rel}}(\phi) + 1$, and

$$\Sigma_{\mathfrak{q}}(K, W)_{\mathrm{div}} = \mathrm{Sel}_{\mathrm{rel}}(K, W)_{\mathrm{div}}, \quad \Sigma_{\mathfrak{q}^*}(K, W)_{\mathrm{div}} = \mathrm{Sel}_{\mathrm{str}}(K, W)_{\mathrm{div}}.$$

Proposition 9.6. *Suppose that $r_{\mathfrak{q}}(\phi) = 1$.*

(a) We have that

$$\frac{|\,\mathrm{Sel}_{\mathrm{rel}}(K, W)/_{\mathrm{div}}|}{|\Sigma_{\mathfrak{q}}(K, W)/_{\mathrm{div}}|} = [H^1(K_{\mathfrak{q}^*}, T^*) : \mathrm{loc}_{\mathfrak{q}^*}(\Sigma_{\mathfrak{q}^*}(K, T^*))]. \tag{9.5}$$

(b) We have that

$$\frac{|\,\mathrm{Sel}_{\mathrm{rel}}(K, W)/_{\mathrm{div}}|}{|\Sigma_{\mathfrak{q}^*}(K, W)/_{\mathrm{div}}|} = \frac{[H^1(K_{\mathfrak{q}}, T) : \mathrm{loc}_{\mathfrak{q}}(\mathrm{Sel}_{\mathrm{rel}}(K, T))]}{|H^1(K_{\mathfrak{q}}, T)_{\mathrm{tors}}||\,\mathrm{loc}_{\mathfrak{q}}(\mathrm{Sel}_{\mathrm{rel}}(K, W))/_{\mathrm{div}}|}. \tag{9.6}$$

Proof. (a) Since $r_{\mathfrak{q}}(\phi) = 1$, we have (as remarked above) that $\Sigma_{\mathfrak{q}}(K, W)_{\mathrm{div}} = \mathrm{Sel}_{\mathrm{rel}}(K, W)_{\mathrm{div}}$, and the Poitou-Tate exact sequence implies that there is an exact sequence

$$0 \to \Sigma_{\mathfrak{q}}(K, W) \to \mathrm{Sel}_{\mathrm{rel}}(K, W) \xrightarrow{\mathrm{loc}_{\mathfrak{q}^*}} H^1(K_{\mathfrak{q}^*}, W) \xrightarrow{\alpha} \Sigma_{\mathfrak{q}^*}(K, T^*)^{\wedge}.$$

The kernel of α is equal to the Pontryagin dual of the cokernel of the map

$$\Sigma_{\mathfrak{q}^*}(K, T^*) \to H^1(K_{\mathfrak{q}^*}, W)^{\wedge} \simeq H^1(K_{\mathfrak{q}^*}, T^*),$$

and so (9.5) follows.

(b) There is an exact sequence

$$0 \to \Sigma_{\mathfrak{q}^*}(K, W) \to \mathrm{Sel}_{\mathrm{rel}}(K, W) \xrightarrow{\mathrm{loc}_{\mathfrak{q}}} \mathrm{loc}_{\mathfrak{q}}(\mathrm{Sel}_{\mathrm{rel}}(K, W)) \to 0. \tag{9.7}$$

If M is any cofinitely generated, torsion $\mathbf{Z}_p$-module, then we have

$$\mathrm{Ext}^1(\mathbf{Q}_p/\mathbf{Z}_p, M) \simeq M/_{\mathrm{div}}, \quad \mathrm{Ext}^1(\mathbf{Q}_p/\mathbf{Z}_p, M_{\mathrm{div}}) = \mathrm{Ext}^2(\mathbf{Q}_p/\mathbf{Z}_p, M) = 0.$$

Since $r_{\mathfrak{q}}(\phi) = 1$, and $H^1(K_{\mathfrak{q}}, W)$ is of $\mathbf{Z}_p$-corank one, we have that

$$\begin{aligned}\mathrm{Hom}(\mathbf{Q}_p/\mathbf{Z}_p, \mathrm{loc}_{\mathfrak{q}}(\mathrm{Sel}_{\mathrm{rel}}(K,W))) &= \mathrm{Hom}(\mathbf{Q}_p/\mathbf{Z}_p, \mathrm{loc}_{\mathfrak{q}}(\mathrm{Sel}_{\mathrm{rel}}(K,W))_{\mathrm{div}}) \\ &= \mathrm{Hom}(\mathbf{Q}_p/\mathbf{Z}_p, H^1(K_{\mathfrak{q}}, W)_{\mathrm{div}}) \\ &= H^1(K_{\mathfrak{q}}, T)/H^1(K_{\mathfrak{q}}, T)_{\mathrm{tors}}.\end{aligned}$$

Hence, applying the functor $\mathrm{Hom}(\mathbf{Q}_p/\mathbf{Z}_p, -)$ to the exact sequence (9.7) yields

$$\begin{aligned}&0 \to \Sigma_{\mathfrak{q}^*}(K,T) \to \mathrm{Sel}_{\mathrm{rel}}(K,T) \to H^1(K_{\mathfrak{q}}, T)/H^1(K_{\mathfrak{q}}, T)_{\mathrm{tors}} \to \\ &\to \Sigma_{\mathfrak{q}^*}(K,W)/_{\mathrm{div}} \to \mathrm{Sel}_{\mathrm{rel}}(K,W)/_{\mathrm{div}} \to \mathrm{loc}_{\mathfrak{q}}(\mathrm{Sel}_{\mathrm{rel}}(K,W))/_{\mathrm{div}} \to 0,\end{aligned}$$

and this immediately implies (9.6). □

Recall that $H_{\mathfrak{q},\phi}^{(K)} \in \Lambda(K_\infty)$ denotes a characteristic power series of $X_{\mathfrak{q}}(K_\infty, W)$. Let us set

$$H_{\mathfrak{q},\phi}^{(K)}(0)^* := \left.\frac{H_{\mathfrak{q},\phi}^{(K)}}{X^{n_{\mathfrak{q}}(\phi)}}\right|_{X=0}.$$

Theorem 9.7. *Suppose that $r_{\mathfrak{q}}(\phi) = 1$, and that the p-adic height pairings $[-,-]_{K,\mathfrak{q}}^{(\phi)}$ and $[-,-]_{K,\mathfrak{q}^*}^{(\phi)}$ are non-degenerate. Then we have*

$$\begin{aligned}&|\,\mathrm{Sel}_{\mathrm{rel}}(K,W)/_{\mathrm{div}}| \sim \\ &\frac{H_{\mathfrak{q},\phi}^{(K)}(0)^*}{|\Sigma_{\mathfrak{q}}(K,T)_{\mathrm{tors}}|\mathcal{R}_{K,\mathfrak{q}}^{(\phi)}} \cdot [H^1(K_{\mathfrak{q}^*}, T^*) : \mathrm{loc}_{\mathfrak{q}^*}(\Sigma_{\mathfrak{q}^*}(K,T^*))] \sim \\ &\frac{H_{\mathfrak{q}^*,\phi}^{(K)}(0)^*}{|\Sigma_{\mathfrak{q}^*}(K,T)_{\mathrm{tors}}|\mathcal{R}_{K,\mathfrak{q}^*}^{(\phi)}} \cdot \frac{[H^1(K_{\mathfrak{q}}, T) : \mathrm{loc}_{\mathfrak{q}}(\mathrm{Sel}_{\mathrm{rel}}(K,T))]}{|H^1(K_{\mathfrak{q}}, T)_{\mathrm{tors}}||\,\mathrm{loc}_{\mathfrak{q}}(\mathrm{Sel}_{\mathrm{rel}}(K,W))/_{\mathrm{div}}|}.\end{aligned}$$

Proof. This follows directly from Theorem 8.2 and Proposition 9.6. □

10. Elliptic units and the two-variable p-adic L-function

In this section we shall first briefly recall some basic facts concerning elliptic units and the construction of the Katz two-variable p-adic L-function (see

[10]). We then explain how elliptic units may be used to construct canonical elements in restricted Selmer groups and we describe how certain special values of the p-adic L-function may be expressed in terms of these canonical elements.

Throughout this section N_∞ will denote a $\mathbf{Z}_p^\times$-extension of K.

10.1. **Elliptic units.** Recall that $\mathfrak{f}$ denotes the conductor of the elliptic curve E/K. Let $\mathfrak{a}$ be any ideal of O_K with $(\mathfrak{a}, 6\mathfrak{f}p) = 1$, and write $I(\mathfrak{a})$ for the set of ideals of O_K that are coprime to $\mathfrak{a}$. If $\mathfrak{m} \in I(\mathfrak{a})$, we write $w_\mathfrak{m}$ for the number of roots of unity in K congruent to 1 modulo $\mathfrak{m}$.

Suppose that $L \subset \mathbf{C}$ is any lattice with complex multiplication by O_K. Then we may define an elliptic function $\Theta(z; L, \mathfrak{a})$ by

$$\Theta(z; L, \mathfrak{a}) := \frac{\Delta(L)}{\Delta(\mathfrak{a}^{-1}L)} \prod_u \frac{\Delta(L)}{(\mathcal{P}(z, L) - \mathcal{P}(u, L)^6)};$$

here the product is over all non-zero $u \in \mathfrak{a}^{-1}L/L$, Δ denotes the modular discriminant, and $\mathcal{P}$ is the Weierstrass $\mathcal{P}$-function. If $\mathfrak{m} \in I(\mathfrak{a})$ is not a prime power, then then $\Theta(1; \mathfrak{m}, \mathfrak{a})$ is a unit in the ray class field $K(\mathfrak{m})$. For any prime $\mathfrak{l} \in I(\mathfrak{a})$, we have the following distribution relation:

$$\mathbf{N}_{K(\mathfrak{m}\mathfrak{l})/K(\mathfrak{m})} \Theta(1; \mathfrak{m}\mathfrak{l}, \mathfrak{a})^{w_\mathfrak{m}/w_{\mathfrak{m}\mathfrak{l}}} = \begin{cases} \Theta(1; \mathfrak{m}, \mathfrak{a}) & \text{if } \mathfrak{l} \mid \mathfrak{m}; \\ \Theta(1; \mathfrak{m}, \mathfrak{a})^{1-\sigma_\mathfrak{l}^{-1}} & \text{otherwise.} \end{cases}$$

It follows from the distribution relation that $\{\Theta(1; \mathfrak{f}p^k, \mathfrak{a})\}_{k>0}$ is a norm-compatible sequence in $K(\mathfrak{f}p^\infty)/K$, and that if $\mathfrak{a}$ and $\mathfrak{b}$ are any two ideals in O_K that are coprime to $6\mathfrak{f}p$ then

$$\Theta(1; \mathfrak{f}p^k, \mathfrak{a})^{\sigma_\mathfrak{b} - \mathbf{N}(\mathfrak{b})} = \Theta(1; \mathfrak{f}p^k, \mathfrak{b})^{\sigma_\mathfrak{a} - \mathbf{N}(\mathfrak{a})}. \tag{10.1}$$

For any finite extension F/K with $K \subseteq F \subseteq K(\mathfrak{f}p^\infty)$, we choose any $m > 0$ such that $F \subseteq K(\mathfrak{f}p^m)$, and we set

$$\theta(F; \mathfrak{a}) := \mathbf{N}_{K(\mathfrak{f}p^m)/F}(\Theta(1; \mathfrak{f}p^m, \mathfrak{a}));$$

this is independent of the choice of m. We set

$$\theta(\mathcal{K}_\infty;\mathfrak{a}) := [\theta(\mathcal{K}_n;\mathfrak{a})] \in \mathcal{E}(\mathcal{K}_\infty)$$

The following result is very similar to [23, Proposition 3.2].

Proposition 10.1. *Suppose that the $\mathbf{Z}_p^\times$-extension N_∞/K is linearly disjoint from the cyclotomic extension $K(\mu_{p^\infty})/K$. Then there exists*

$$\theta(N_\infty) = [\theta(N_n)] \in \mathcal{E}(N_\infty)$$

such that

$$\theta(N_\infty;\mathfrak{a}) = \theta(N_\infty)^{\sigma_\mathfrak{a} - \mathbf{N}(\mathfrak{a})} \tag{10.2}$$

for all ideals $\mathfrak{a}$ in O_K with $(\mathfrak{a}, 6\mathfrak{f}p) = 1$.

Proof. Since $\mu_p \not\subseteq N_\infty$, the Chebotarev density theorem implies that for each n, we may find an ideal $\mathfrak{b}_n$ that is coprime to $6\mathfrak{f}p$ and is such that $\sigma_{\mathfrak{b}_n}$ fixes N_n and acts non-trivially on μ_p. This implies that

$$\sigma_{\mathfrak{b}_n} - \mathbf{N}(\mathfrak{b}_n) = 1 - \mathbf{N}(\mathfrak{b}_n)$$

is a unit in $\mathbf{Z}_p[\mathrm{Gal}(N_n/K)]$. It therefore follows from (10.1) that

$$\theta(N_n;\mathfrak{a}) \in (\sigma_\mathfrak{a} - \mathbf{N}(\mathfrak{a})) \cdot H^1(N_n, \mathbf{Z}_p(1)),$$

(where here we have abused notation slightly and identified $\theta(N_n;\mathfrak{a})$ with its image in $H^1(N_n, \mathbf{Z}_p(1))$). We set

$$\theta(N_n) := \theta(N_n;\mathfrak{a})^{(\sigma_\mathfrak{a} - \mathbf{N}(\mathfrak{a}))^{-1}};$$

this is well-defined, since by assumption $H^1(N_n, \mathbf{Z}_p(1))$ is $\mathbf{Z}_p$-torsion-free, and $\theta(N_n)$ is also independent of $\mathfrak{a}$. The elements $\theta(N_n)$ are norm-coherent, and $\theta(N_\infty) := [\theta(N_n)]$ satisfies (10.2), as required. $\square$

10.2. **p-adic L-functions.** If k, j are integers, recall that a Grossencharacter of type (k, j) is defined to be a $\overline{K}$-valued function ϵ which is defined on integral ideals of O_K coprime to a fixed ideal $\mathfrak{m}$ such that if $\mathfrak{a} = \alpha O_K$ with $\alpha \equiv 1 \pmod{\mathfrak{m}}$, then $\epsilon(\mathfrak{a}) = \alpha^k \overline{\alpha}^j$. For any ideal $\mathfrak{m}$ of O_K, we write $L_{\infty,\mathfrak{m}}(\epsilon, s)$ for the $\mathbf{C}$-valued completed Hecke L-function attached to ϵ with the Euler factors dividing $\mathfrak{m}$ removed. If ϵ is a Grossencharacter of conductor dividing $\mathfrak{m}$, then it has an associated p-adic Galois character

$$\epsilon_{\mathfrak{q}} : \mathrm{Gal}(K(\mathfrak{m}p^\infty)) \to \mathbf{C}_p^\times; \quad \sigma_{\mathfrak{a}} \to i_{\mathfrak{q}}(\epsilon(\mathfrak{a})),$$

where $\mathfrak{q} \in \{\mathfrak{p}, \mathfrak{p}^*\}$ and $i_{\mathfrak{q}} : \overline{K} \hookrightarrow \overline{K}_{\mathfrak{q}}$ is the natural embedding afforded by $\mathfrak{q}$.

A result of Katz (see [10, Theorem II.4.14]) asserts that there exists a p-adic measure $\mu_{\mathfrak{q}} \in \Lambda(K(\mathfrak{f}p^\infty))_{\mathcal{O}}$ such that if ϵ is any Grossencharacter of type (k, j) with $0 \leq -j < k$ and of conductor dividing $\mathfrak{f}p^\infty$, then there is an interpolation formula:

$$\alpha_{\mathfrak{q}}(\epsilon) \int \epsilon_{\mathfrak{q}} d\mu_{\mathfrak{q}} = \left(1 - \frac{\epsilon(\mathfrak{q})}{p}\right) \cdot L_{\infty,\mathfrak{f}\mathfrak{q}^*}(\epsilon^{-1}, 0).$$

Here $\alpha_{\mathfrak{q}}(\epsilon)$ is an explicit, non-zero constant (whose precise description we shall not need), the integral is over $\mathrm{Gal}(K(\mathfrak{f}p^\infty)/K)$, and we view the right-hand side of the equality as lying in $\mathbf{C}_p$ via the embedding $i_{\mathfrak{q}}$.

Definition 10.2. We define the Katz two-variable p-adic L-function $\mathcal{L}_{\mathfrak{q}}$ by the interpolation formula

$$\mathcal{L}_{\mathfrak{q}}(\epsilon) = \int_{\mathrm{Gal}(K(\mathfrak{f}p^\infty)/K)} \epsilon_{\mathfrak{q}} d\mu_{\mathfrak{q}}$$

for all Grossencharacters ϵ of conductor dividing $\mathfrak{f}p^\infty$, and we view $\mathcal{L}_{\mathfrak{q}}$ as lying in $\Lambda(K(\mathfrak{f}p^\infty))_{\mathcal{O}}$. Hence, if ϵ is of type (k, j) with $0 \leq -j < k$, then

$$\alpha_{\mathfrak{q}}(\epsilon)^{-1} \mathcal{L}_{\mathfrak{q}}(\epsilon) = \left(1 - \frac{\epsilon(\mathfrak{q})}{p}\right) \cdot L_{\infty,\mathfrak{f}\mathfrak{q}^*}(\epsilon^{-1}, 0).$$

If $\epsilon_{\mathfrak{q}}$ factors through $\mathrm{Gal}(F/K)$ for some subextension F/K of $K(\mathfrak{f}p^{\infty})/K$, then

$$\int_{\mathrm{Gal}(K(\mathfrak{f}p^{\infty})/K)} \epsilon_{\mathfrak{q}} d\mu_{\mathfrak{q}} = \int_{\mathrm{Gal}(F/K)} \epsilon_{\mathfrak{q}} d\mu_{\mathfrak{q}},$$

and so we have that

$$\mathcal{L}_{\mathfrak{q}}(\epsilon) = (\mathcal{L}_{\mathfrak{q}}|_F)(\epsilon), \tag{10.3}$$

where $\mathcal{L}_{\mathfrak{q}}|_F$ denotes the image of $\mathcal{L}_{\mathfrak{q}}$ under the natural projection map

$$\Lambda(K(\mathfrak{f}p^{\infty}))_{\mathcal{O}} \to \Lambda(F)_{\mathcal{O}}.$$

□

Theorem 10.3. *Let $N_\infty \subseteq K(\mathfrak{f}p^{\infty})$ be a $\mathbf{Z}_p^{\times}$-extension of K. Assume that N_∞/K is linearly disjoint from the cyclotomic extension $K(\mu_{p^\infty})/K$. Let $\Theta(N_n)_{\mathfrak{q}} = \mathrm{loc}_{\mathfrak{q}}(\Theta(N_n))$, and write*

$$\Theta(N_\infty)_{\mathfrak{q}} = \mathrm{loc}_{\mathfrak{q}}(\Theta(N_\infty)) = [\Theta(N_n)_{\mathfrak{q}}]$$

for the image of $\Theta(N_\infty)$ in $U_{\mathfrak{q}}(N_\infty)$ (see Proposition 10.1).

(a) Suppose that N_∞/K is totally ramified at $\mathfrak{q}$, and write

$$\mathrm{Col}_{N_{\infty,\mathfrak{q}}/K_{\mathfrak{q}}} : U_{\mathfrak{q}}(N_\infty) \to \Lambda(N_\infty)_{\mathcal{O}}$$

for the Coleman map associated to $N_{\infty,\mathfrak{q}}/K_{\mathfrak{q}}$. Then we have that

$$\mathrm{Col}_{N_{\infty,\mathfrak{q}}/K_{\mathfrak{q}}}(\Theta(N_\infty)_{\mathfrak{q}}) = \mathcal{L}_{\mathfrak{q}}|_{N_\infty}.$$

(b) If N_∞/K is unramified at $\mathfrak{q}$, and

$$\mathrm{Col}^{\mathrm{nr}}_{N_{\infty,\mathfrak{q}}/K_{\mathfrak{q}}} : U_{\mathfrak{q}}(N_\infty) \to \Lambda(N_\infty)_{\mathcal{O}}$$

denotes the unramified Coleman map associated to $N_{\infty,\mathfrak{q}}/K_{\mathfrak{q}}$, then we have that

$$\mathrm{Col}^{\mathrm{nr}}_{N_{\infty,\mathfrak{q}}/K_{\mathfrak{q}}}(\Theta(N_\infty)_{\mathfrak{q}}) = \mathcal{L}_{\mathfrak{q}}|_{N_\infty}.$$

(c) Let $\chi : \mathrm{Gal}(K(\mathfrak{f}p^{\infty})/K) \to \mathbf{Z}_p^{\times}$ be any character which factors through $\mathrm{Gal}(N_\infty/K)$, and suppose that $\Theta(N_\infty)_{\mathfrak{q}} \in (\vartheta_K^{(\chi)})^d \cdot U_{\mathfrak{q}}(N_\infty)$ for some integer

$d \geq 1$. Then, because $U_{\mathfrak{q}}(N_\infty)$ is $\vartheta_K^{(\chi)}$-torsion free (see [10, Chapter III, Proposition 1.3]*), we may write*

$$\Theta(N_\infty)_{\mathfrak{q}} = (\vartheta_K^{(\chi)})^d \cdot \overline{\Theta}_{\mathfrak{q}}(N_\infty)^{(d)} \tag{10.4}$$

for a unique $\overline{\Theta}_{\mathfrak{q}}(N_\infty)^{(d)} \in U_{\mathfrak{q}}(N_\infty)$. Define

$$\mu_{\mathfrak{q}}^{(d)} := \mathrm{Col}_{N_{\infty,\mathfrak{q}}/K_{\mathfrak{q}}}(\overline{\Theta}_{\mathfrak{q}}(N_\infty)^{(d)}).$$

Then we have that

$$\mathcal{L}_{\mathfrak{q}}^{(d)}(\chi) = \int_{\mathrm{Gal}(N_\infty/K)} \chi_{\mathfrak{q}} d\mu_{\mathfrak{q}}^{(d)}.$$

In particular, $\mathrm{ord}_{s=1} L_{\mathfrak{q}}(\chi, s)$ *is the highest power of $\vartheta_K^{(\chi)}$ that divides $U_{\mathfrak{q}}(N_\infty)$.*

Proof. (a) Let

$$\mathcal{N}_{K(\mathfrak{f}p^\infty)_{\mathfrak{q}}/N_{\infty,\mathfrak{q}}} : U_{\mathfrak{q}}(K(\mathfrak{f}p^\infty)) \to U_{\mathfrak{q}}(N_\infty); \quad [u_n] \mapsto [\overline{u}_n]$$

be defined by

$$\overline{u}_n = N_{K(\mathfrak{f}p^k)_{\mathfrak{q}}/N_{n,\mathfrak{q}}}(u_k)$$

for any $K(\mathfrak{f}p^k)$ containing N_n. (This does not depend upon the choice of k.) Let

$$\mathrm{Col}_{K(\mathfrak{f}p^\infty)_{\mathfrak{q}}/K_{\mathfrak{q}}} : U_{\mathfrak{q}}(N(\mathfrak{f}p^\infty)) \to \Lambda(N(\mathfrak{f}p^\infty))_{\mathcal{O}}$$

be the Coleman map associated to $N(\mathfrak{f}p^\infty)_{\mathfrak{q}}/K_{\mathfrak{q}}$. Then there is a commutative diagram

$$\begin{array}{ccc} U_{\mathfrak{q}}(K(\mathfrak{f}p^\infty)) & \xrightarrow{\mathrm{Col}_{K(\mathfrak{f}p^\infty)_{\mathfrak{q}}/K_{\mathfrak{q}}}} & \Lambda(N(\mathfrak{f}p^\infty)_{\mathcal{O}} \\ {\scriptstyle \mathcal{N}_{K(\mathfrak{f}p^\infty)_{\mathfrak{q}}/N_{\infty,\mathfrak{q}}}}\downarrow & & \downarrow \\ U_{\mathfrak{q}}(N_\infty) & \xrightarrow{\mathrm{Col}_{N_{\infty,\mathfrak{q}}/K_{\mathfrak{q}}}} & \Lambda(N_\infty)_{\mathcal{O}}, \end{array} \tag{10.5}$$

where the right-hand vertical arrow is the natural quotient map.

For each ideal $\mathfrak{a}$ in O_K that is coprime to $6p\mathfrak{f}$, let

$$\theta(K(\mathfrak{f}p^\infty;\mathfrak{a}))_{\mathfrak{q}} = \mathrm{loc}_{\mathfrak{q}}(\theta_{\mathfrak{q}}(K(\mathfrak{f}p^\infty;\mathfrak{a}))) \in U_{\mathfrak{q}}(K(\mathfrak{f}p^\infty)).$$

It is shown in [10, Proposition III.1.4] that

$$\mathrm{Col}_{K(\mathfrak{f}p^\infty)_\mathfrak{q}/K_\mathfrak{q}}(\theta(K(\mathfrak{f}p^\infty;\mathfrak{a}))_\mathfrak{q}) = (\sigma_\mathfrak{a} - \mathbf{N}(\mathfrak{a}))\cdot\mu_\mathfrak{q},$$

and this implies that

$$(\mathrm{Col}_{K(\mathfrak{f}p^\infty)_\mathfrak{q}/K_\mathfrak{q}}(\theta(K(\mathfrak{f}p^\infty;\mathfrak{a}))_\mathfrak{q}))|_{N_\infty} = (\sigma_\mathfrak{a} - \mathbf{N}(\mathfrak{a}))\cdot(\mathcal{L}_\mathfrak{q})|_{N_\infty}. \tag{10.6}$$

We also see from (10.5) and Proposition 10.1 that

$$\begin{aligned}(\mathrm{Col}_{K(\mathfrak{f}p^\infty)_\mathfrak{q}/K_\mathfrak{q}}(\theta(K(\mathfrak{f}p^\infty;\mathfrak{a}))_\mathfrak{q}))|_{N_\infty} &= \mathrm{Col}_{N_{\infty,\mathfrak{q}}/K_\mathfrak{q}}(\theta(N_\infty;\mathfrak{a})_\mathfrak{q}) \\ &= (\sigma_\mathfrak{a} - \mathbf{N}(\mathfrak{a}))\cdot\mathrm{Col}_{N_{\infty,\mathfrak{q}}/K_\mathfrak{q}}(\theta(N_\infty)_\mathfrak{q})\end{aligned} \tag{10.7}$$

The desired result now follows from (10.6) and (10.7).

(b) The proof of (b) is almost identical to that of (a).

(c)This follows directly from parts (a) and (b) together with the definition of $\mathcal{L}_\mathfrak{q}^{(d)}(\chi)$ (see (3.5)). □

11. Canonical elements in restricted Selmer groups

We shall now apply the results of Section 10 to construct canonical elements in restricted Selmer groups from twisted elliptic units. These elements are closely related to certain special values of the two-variable p-adic L-function $\mathcal{L}_\mathfrak{q}$ via Theorem 10.3.

Throughout this section we assume that ϕ and ϕ^* are $\mathbf{Z}_p^\times$-valued characters of $\mathrm{Gal}(K(\mathfrak{f}p^\infty)/K)$ *of infinite order, such that the extensions $\mathcal{K}_\infty/K$ and $\mathcal{K}_\infty^*/K$ are linearly disjoint from $K(\mu_{p^\infty})/K$.*

Definition 11.1. (a) Let $d(\phi^*)$ denote the largest non-negative integer such that

$$\Theta(\mathcal{K}_\infty^*) \in (\vartheta_K^{(\phi^*)})^{d(\phi^*)}\cdot\mathcal{E}(\mathcal{K}_\infty^*).$$

A theorem of Yager (see [10, Chapter III, Proposition 4.5]) implies that $\mathcal{E}(\mathcal{K}_\infty^*)$ is $\vartheta_K^{(\phi^*)}$-torsion free, and so we may write

$$\Theta(\mathcal{K}_\infty^*) = (\vartheta_K^{(\phi^*)})^{d(\phi^*)} \cdot \Theta(\mathcal{K}_\infty^*)^{(d(\phi^*))}$$

for a unique $\Theta(\mathcal{K}_\infty^*)^{(d(\phi^*))} \in \mathcal{E}(\mathcal{K}_\infty^*)$. We define $y(\mathcal{K}_\infty^*;\phi) = [y(\mathcal{K}_n^*;\phi)] \in \varprojlim(\mathcal{K}_n^*, T)$ by

$$y(\mathcal{K}_\infty^*;\phi) := \mathrm{Tw}_{\phi^{*-1}}(\Theta(\mathcal{K}_\infty^*)^{(d(\phi^*)}) \tag{11.1}$$

and $y(\phi) \in H^1(K,T)$ by

$$y(\phi) := y(\mathcal{K}_0^*;\phi) = y(K;\phi). \tag{11.2}$$

We write

$$y(\mathcal{K}_\infty^*;\phi)_\mathfrak{q} := \mathrm{loc}_\mathfrak{q}(y(\mathcal{K}_\infty^*;\phi)) \in \varprojlim H^1(\mathcal{K}_{n,\mathfrak{q}}^*, T),$$

and

$$y(\phi)_\mathfrak{q} := \mathrm{loc}_\mathfrak{q}(y(\phi)) \in H^1(K_\mathfrak{q}, T).$$

(b) Recall the definition of $\overline{\Theta}_\mathfrak{q}(\mathcal{K}_\infty^*)^{(d)} \in U_\mathfrak{q}(\mathcal{K}_\infty^*)$ given in (10.4). If $\overline{\Theta}_\mathfrak{q}(\mathcal{K}_\infty^*)^{(d)}$ is defined, then we define $\overline{y}_\mathfrak{q}(\mathcal{K}_\infty^*;\phi)^{(d)} \in \varprojlim H^1(\mathcal{K}_n^*/K_\mathfrak{q}, T)$ by

$$\overline{y}_\mathfrak{q}(\mathcal{K}_\infty^*;\phi)^{(d)} = [\overline{y}_\mathfrak{q}(\mathcal{K}_n^*;\phi)^{(d)}] := \mathrm{Tw}_{\phi^{*-1}}(\overline{\Theta}_\mathfrak{q}(\mathcal{K}_\infty^*)^{(d)}) \tag{11.3}$$

and $\overline{y}_\mathfrak{q}(\phi)^{(d)} \in H^1(K_\mathfrak{q}, T)$ by

$$\overline{y}_\mathfrak{q}(\phi)^{(d)} := \overline{y}_\mathfrak{q}(\mathcal{K}_0^*;\phi)^{(d)} = \overline{y}_\mathfrak{q}(K;\phi)^{(d)}. \tag{11.4}$$

□

Remark 11.2. It follows from the definition of $d(\phi)$ that we have

$$\Theta(\mathcal{K}_\infty)_\mathfrak{q} \in (\vartheta_K^{(\phi)})^{d(\phi)} \cdot \mathcal{E}(\mathcal{K}_\infty) \subseteq (\vartheta_K^{(\phi)})^{d(\phi)} \cdot U_\mathfrak{q}(\mathcal{K}_\infty)$$

for each $\mathfrak{q} \in \{\mathfrak{p}, \mathfrak{p}^*\}$. Hence, if $d(\phi) \geq 1$, then Theorem 10.3(c) implies that

$$\mathcal{L}_\mathfrak{p}(\phi) = \mathcal{L}_{\mathfrak{p}^*}(\phi) = 0.$$

Since $\mathrm{rank}_{\Lambda(\mathcal{K}_\infty)}(U_\mathfrak{q}(\mathcal{K}_\infty) = 1$, it follows that

$$\mathrm{rank}_{\Lambda(\mathcal{K}_\infty)}[\mathrm{Hom}(U_\mathfrak{q}(\mathcal{K}_\infty)/\mathcal{E}(\mathcal{K}_\infty), W)^{\mathrm{Gal}(\mathcal{K}_\infty/K)}] \leq 1,$$

and so

$$\vartheta_K^{(\phi)} \cdot U_{\mathfrak{q}}(\mathcal{K}_\infty) \subseteq \mathcal{E}(\mathcal{K}_\infty).$$

We therefore see that

$$d(\phi) \leq \operatorname{ord}_{s=1} L_{\mathfrak{q}}(\phi, s) \leq d(\phi) + 1. \tag{11.5}$$

If $\mathcal{R}_{K,\mathfrak{q}^*}^{(\phi^*)} \neq 0$, then Theorem 8.2 implies that

$$\operatorname{ord}_{s=1} L_{\mathfrak{q}}(\phi, s) = \operatorname{ord}_{s=1} L_{\mathfrak{q}^*}(\phi^*, s),$$

and so

$$|d(\phi) - d(\phi^*)| \leq 1.$$

It seems reasonable to expect that $d(\phi) > 1$ does not occur very often. $\square$

We now turn to the relationship between the canonical elements $y(\phi)$ and special values of $\mathcal{L}_{\mathfrak{q}}$ when ϕ^* is LLT at $\mathfrak{q}$.

Theorem 11.3. *Suppose that ϕ^* is LLT at $\mathfrak{q}$, and recall the notation of Definition 6.8.*

(a) We have

$$\mathfrak{Log}_V(y(\phi)_{\mathfrak{q}}) = \mathfrak{Eul}_{\mathfrak{q}}(\phi^{*-1}) \cdot \Omega(\phi_{\mathfrak{q}}^{*-1}) \cdot \mathcal{L}_{\mathfrak{q}}^{(d(\phi^*))}(\phi^*)$$

(b) If $m \geq 1$ and $\overline{y}_{\mathfrak{q}}(\phi)^{(m)}$ is defined, then we have

$$\mathfrak{Log}_V(\overline{y}_{\mathfrak{q}}(\phi)^{(m)}) = \mathfrak{Eul}_{\mathfrak{q}}(\phi^{*-1}) \cdot \Omega(\phi_{\mathfrak{q}}^{*-1}) \cdot \mathcal{L}_{\mathfrak{q}}^{(m)}(\phi^*).$$

Proof. This follows directly from Theorems 6.9 and 10.3 $\square$

Corollary 11.4. *(a) Suppose that ϕ^* is LLT at $\mathfrak{q}^*$. Then we have that $y(\phi) \in \Sigma_{\mathfrak{q}}(K, T)$ if and only if $\mathcal{L}_{\mathfrak{q}^*}^{(d(\phi^*))}(\phi^*) = 0$.*

(b) If $y(\phi) \in \Sigma_{\mathfrak{q}}(K, T)$, and ϕ^* is LLT at $\mathfrak{q}$, then $y(\phi)$ is of infinite order if and only if $\mathcal{L}_{\mathfrak{q}}^{(d(\phi^*))}(\phi^*) \neq 0$.

Proof. We first note that $y(\phi) \in \Sigma_{\mathfrak{q}}(K,T)$ if and only if $y(\phi)_{\mathfrak{q}^*} = 0$. Theorem 11.3(a) implies that $y(\phi)_{\mathfrak{q}} = 0$ if and only if $\mathcal{L}_{\mathfrak{q}^*}^{(d(\phi^*))}(\phi^*) = 0$, and this establishes (a).

If $y(\phi) \in \Sigma_{\mathfrak{q}}(K,T)$, then $y(\phi)$ is of infinite order if and only if $y(\phi)_{\mathfrak{q}}$ is also of infinite order. Part (b) now also follows from Theorem 11.3(a). $\square$

Theorem 11.5. *Suppose that*

$$y(\phi) \in \Sigma_{\mathfrak{q}}(K,T), \quad y(\phi^*) \in \Sigma_{\mathfrak{q}^*}(K,T^*),$$

and that both ϕ and ϕ^* are LLT at $\mathfrak{q}$. Then we have that

$$\begin{aligned}[y(\phi^*), y(\phi)]_{K,\mathfrak{q}}^{(\phi)} &= \mathfrak{Eul}_{\mathfrak{q}}(\phi^{*-1}) \cdot \mathfrak{Eul}_{\mathfrak{q}}(\phi^{-1}) \cdot \Omega(\phi_{\mathfrak{q}}^{*-1}) \cdot \Omega(\phi_{\mathfrak{q}}^{-1}) \\ &\times \mathcal{L}_{\mathfrak{q}}^{(d(\phi)+1)}(\phi) \cdot \mathcal{L}_{\mathfrak{q}}^{(d(\phi^*))}(\phi^*).\end{aligned}$$

Proof. Since ϕ is LLT at $\mathfrak{q}$ and $y(\phi^*) \in \Sigma_{\mathfrak{q}^*}(K,T^*)$, Corollary 11.4(a) implies that $\mathcal{L}_{\mathfrak{q}}^{(d(\phi))}(\phi) = 0$. This in turn implies that

$$\mathrm{loc}_{\mathfrak{q}}(\Theta(\mathcal{K}_\infty)^{(d(\phi))}) \in \vartheta_\phi \cdot U_{\mathfrak{q}}(\mathcal{K}_\infty)$$

and it follows from the definitions that in fact

$$\mathrm{loc}_{\mathfrak{q}}(\Theta(\mathcal{K}_\infty)^{(d(\phi))}) = \vartheta_\phi \cdot \Theta_{\mathfrak{q}}^{(d(\phi)+1)}(\mathcal{K}_\infty).$$

Applying Proposition 7.7 together with (6.9), we obtain

$$\begin{aligned}[y(\phi^*), y(\phi)]_{K,\mathfrak{q}}^{(\phi)} &= \overline{y}_{\mathfrak{q}}(\phi^*)^{(d(\phi)+1)} \cup y(\phi)_{\mathfrak{q}} \\ &= \mathfrak{Log}_{V^*}(\overline{y}_{\mathfrak{q}}(\phi^*)^{(d(\phi)+1)}) \cdot \mathfrak{Log}_V(y(\phi)_{\mathfrak{q}}).\end{aligned}$$

The desired result now follows from Theorem 11.3. $\square$

Our next result relates the value of $\mathcal{L}_{\mathfrak{q}}^{(d(\phi)+1)}(\phi)$ to that of $\mathcal{L}_{\mathfrak{q}}^{(d(\phi^*))}(\phi^*)$ when both ϕ and ϕ^* are LLT at $\mathfrak{q}$. We remark that at least one of the characters ϕ or ϕ^* always lies outside the range of interpolation of $\mathcal{L}_{\mathfrak{q}}$.

Theorem 11.6. *Suppose that*

$$y(\phi) \in \Sigma_{\mathfrak{q}}(K,T), \quad y(\phi^*) \in \Sigma_{\mathfrak{q}^*}(K,T^*),$$

and that both ϕ and ϕ^* are LLT at $\mathfrak{q}$. Suppose also that $[y(\phi^*), y(\phi)]_{K,\mathfrak{q}}^{(\phi)} \neq 0$. Then we have

$$\mathcal{L}_{\mathfrak{q}}^{(d(\phi)+1)}(\phi) = \frac{\mathfrak{Eul}_{\mathfrak{q}}(\phi^{*-1}) \cdot \Omega(\phi_{\mathfrak{q}}^{*-1}) \cdot [y(\phi^*), y(\phi)]_{K,\mathfrak{q}}^{(\phi)}}{\mathfrak{Eul}_{\mathfrak{q}}(\phi^{-1}) \cdot \Omega(\phi_{\mathfrak{q}}^{-1}) \cdot \mathfrak{Log}_V(y(\phi)_{\mathfrak{q}})^2} \cdot \mathcal{L}_{\mathfrak{q}}^{(d(\phi^*))}(\phi^*).$$

Proof. If $[y(\phi^*), y(\phi)]_{K,\mathfrak{q}}^{(\phi)} \neq 0$, then $y(\phi)$ is of infinite order, and so Corollary 11.4(a) implies that $\mathcal{L}_{\mathfrak{q}}^{(d(\phi^*))}(\phi^*) \neq 0$. Theorem 11.3(a) implies that

$$\mathcal{L}_{\mathfrak{q}}^{(d(\phi^*))}(\phi^*) = \frac{\mathfrak{Log}_V(y(\phi)_{\mathfrak{q}})^2}{\mathfrak{Eul}_{\mathfrak{q}}(\phi^{*-1})^2 \cdot \Omega(\phi_{\mathfrak{q}}^{*-1})^2 \cdot \mathcal{L}_{\mathfrak{q}}^{(d(\phi^*))}(\phi^*)},$$

and substituting this into the expression for $[y(\phi^*), y(\phi)]_{K,\mathfrak{q}}^{(\phi)}$ afforded by Theorem 11.5 establishes the desired result. □

12. Complex conjugate characters

In this section we shall apply our earlier results to formulate a common generalisation of the main theorems of [23] and [2] to CM modular forms of higher weight.

We begin with the following definition.

Definition 12.1. We say that ϕ and ϕ^* are *complex conjugate* if they are interchanged by the involution on characters of $\mathrm{Gal}(\overline{K}/K)$ induced by the action of complex conjugation.

Remark 12.2. Suppose that $\mathfrak{q} \in \{\mathfrak{p}, \mathfrak{p}^*\}$. It follows from e.g. [10, III.1.4] that the measures $\mu_{\mathfrak{q}}$ and $\mu_{\mathfrak{q}^*}$ are interchanged by the action of complex conjugation on $\Lambda(K(\mathfrak{f}p^\infty))$. Hence, if ϕ and ϕ^* are complex conjugate, then we have the equality

$$\mathcal{L}_{\mathfrak{q}}(\phi) = \mathcal{L}_{\mathfrak{q}^*}(\phi^*),$$

after identifying $K_{\mathfrak{q}}$ and $K_{\mathfrak{q}^*}$ with $\mathbf{Q}_p$. Also, if ϕ is LLT at $\mathfrak{q}$, then ϕ^* is LLT at $\mathfrak{q}^*$. □

Theorem 12.3. *Suppose that ϕ and ϕ^* are complex conjugate. Suppose also that $\mathcal{L}_{\mathfrak{q}}(\phi) \neq 0$, and that both ϕ and ϕ^* are LLT at $\mathfrak{q}$. Then:*

(a) $d(\phi) = d(\phi^*) = 0$.

(b) We have that $n_{\mathfrak{q}^*}(\phi) = n_{\mathfrak{q}}(\phi^*) = 1$, and so $\mathcal{L}_{\mathfrak{q}^*}(\phi) = \mathcal{L}_{\mathfrak{q}}(\phi^*) = 0$.

(c) $y(\phi)$ and $y(\phi^*)$ are of infinite order, with

$$y(\phi) \in \Sigma_{\mathfrak{q}^*}(K,T), \quad y(\phi^*) \in \Sigma_{\mathfrak{q}}(K,T^*).$$

(d) $\mathcal{L}_{\mathfrak{q}}(\phi^*) = 0$ and $\mathcal{L}_{\mathfrak{q}}^{(1)}(\phi^*) \neq 0$.

(e) $\mathcal{R}_{K,\mathfrak{q}^*}^{(\phi)} \neq 0$.

(f) Let

$$x(\phi) \in \Sigma_{\mathfrak{q}^*}(K,T), \quad x(\phi^*) \in \Sigma_{\mathfrak{q}}(K,T^*)$$

be any elements of infinite order. Then we have the following equality in $\mathbf{Q}_p$:

$$\begin{aligned}&\mathfrak{Eul}_{\mathfrak{q}}(\phi^{-1}) \cdot \Omega(\phi_{\mathfrak{q}}^{-1}) \cdot [x(\phi^*), x(\phi)]_{K,\mathfrak{q}^*}^{(\phi)} \cdot \mathcal{L}_{\mathfrak{q}}(\phi)\\ &= \mathfrak{Eul}_{\mathfrak{q}^*}(\phi^{-1}) \cdot \Omega(\phi_{\mathfrak{q}^*}^{-1}) \cdot \mathfrak{Log}_V(x(\phi)_{\mathfrak{q}^*}) \cdot \mathfrak{Log}_{V^*}(x(\phi^*)_{\mathfrak{q}}) \cdot \mathcal{L}_{\mathfrak{q}^*}^{(1)}(\phi).\end{aligned}$$

Proof. (a) This follows immediately from the fact that $\mathcal{L}_{\mathfrak{q}}(\phi) = \mathcal{L}_{\mathfrak{q}^*}(\phi^*) \neq 0$ (cf. Remark 12.2).

(b) Since $\mathcal{L}_{\mathfrak{q}}(\phi) = \mathcal{L}_{\mathfrak{q}^*}(\phi^*) \neq 0$, Theorem 8.2 implies that $n_{\mathfrak{q}}(\phi) = n_{\mathfrak{q}^*}(\phi^*) = 0$. Now it follows from Proposition 9.4 that $n_{\mathfrak{q}^*}(\phi) = n_{\mathfrak{q}}(\phi^*) = 1$. Finally, Theorem 8.2 implies that $\mathcal{L}_{\mathfrak{q}^*}(\phi) = \mathcal{L}_{\mathfrak{q}}(\phi^*) = 0$, as claimed.

(c)It follows from (a), (b), and Theorem 11.3 that $\mathfrak{Log}_V(y(\phi)_{\mathfrak{q}}) = 0$ (whence $y(\phi) \in \Sigma_{\mathfrak{q}^*}(K,T)$) and that $\mathfrak{Log}_V(y(\phi)_{\mathfrak{q}^*}) \neq 0$ (whence $y(\phi)$ is of infinite order). The argument concerning $y(\phi^*)$ is similar.

(d) As $d(\phi^*) = 0$, and $\mathcal{L}_{\mathfrak{q}}(\phi^*) = 0$, this follows from Remark 11.2.

(e) Part (d) implies that $\mathcal{L}_{\mathfrak{q}}(\phi)\mathcal{L}_{\mathfrak{q}}^{(1)}(\phi^*) \neq 0$. Hence Theorem 11.5 implies that $[y(\phi^*), y(\phi)]_{k,\mathfrak{q}^*}^{(\phi)} \neq 0$, and so we see that $\mathcal{R}_{K,\mathfrak{q}^*}^{(\phi)} \neq 0$ because $n_{\mathfrak{q}^*}(\phi) = n_{\mathfrak{q}}(\phi^*) = 1$.

(f) Since $n_{\mathfrak{q}^*}(\phi) = n_{\mathfrak{q}}(\phi^*) = 1$, we have that

$$\frac{[y(\phi^*), y(\phi)]_{K,\mathfrak{q}^*}^{(\phi)}}{\mathfrak{Log}_V(y(\phi)_{\mathfrak{q}^*}) \cdot \mathfrak{Log}_{V^*}(y(\phi^*)_{\mathfrak{q}})} = \frac{[x(\phi^*), x(\phi)]_{K,\mathfrak{q}^*}^{(\phi)}}{\mathfrak{Log}_V(x(\phi)_{\mathfrak{q}^*}) \cdot \mathfrak{Log}_{V^*}(x(\phi^*)_{\mathfrak{q}})}.$$

The result now follows from Theorems 11.3 and 11.5. □

Let us now set $\mathfrak{q} = \mathfrak{p}$ and consider the complex conjugate characters

$$\phi_k := \psi^{k+1}\psi^{*-k}, \quad \phi_k^* := \psi^{-k}\psi^{*k+1}, \quad (k \geq 0).$$

The character ϕ_k is naturally associated to the CM modular form of weight $2k+2$ attached to ψ and lies within the range of interpolation of $\mathcal{L}_{\mathfrak{p}}$, with

$$\mathcal{L}_{\mathfrak{p}}(\phi_k) = A_k \cdot L(\psi^{2k+1}, k+1), \tag{12.1}$$

where A_k is an explicit, non-zero constant whose precise description need not concern us. On the other hand, the character ϕ_k^* lies outside the range of interpolation of $\mathcal{L}_{\mathfrak{p}}$, and the behaviour of $\mathcal{L}_{\mathfrak{p}}$ at ϕ_k^* is less well-understood.

Let $W(\phi_k)$ denote the Artin root number of ϕ_k, so $W(\phi_k) = \pm 1$. A theorem of Greenberg and Rohrlich implies that if $W(\phi_k) = 1$ for some $k \geq 0$, then $\mathcal{L}_{\mathfrak{p}}(\phi_{k'}) = 0$ for only finitely many $k' \geq 0$ with $k' \equiv k \pmod{p-1}$ (see [12, Theorem 4] or [21, p.184]). Rohrlich has also shown that if $W(\phi_k) = -1$, then $L^{(1)}(\psi^{2k'+1}, k'+1) = 0$ for only finitely many $k' \geq 0$ with $k' \equiv k \pmod{p-1}$. It seems reasonable to expect that an analogous result holds for $\mathcal{L}_{\mathfrak{p}}$, namely that if $W(\phi_k) = -1$, then $\mathcal{L}_{\mathfrak{p}}^{(1)}(\phi_{k'}) = 0$ for only finitely many $k' \geq 0$ with $k' \equiv k \pmod{p-1}$, and Greenberg (unpublished) has shown that this would follow from a suitable generalisation of the results of [15].

(I) Suppose that $\mathcal{L}_{\mathfrak{p}}(\phi_k) \neq 0$, and that ϕ_k and ϕ_k^* are LLT at $\mathfrak{p}$. Then Theorem 12.3 with $\phi = \phi_k$ and $\mathfrak{q} = \mathfrak{p}$ yields a generalisation of [2, Theorem A] to the case of CM modular forms of heigher weight.

(II) Suppose that ϕ_k and ϕ_k^* are LLT at $\mathfrak{p}$, that $d(\phi) = 0$, and that $\mathcal{L}_{\mathfrak{p}}(\phi_k) = 0$.

Then $\mathcal{L}_{\mathfrak{p}}^{(1)}(\phi_k) \neq 0$, and $d(\phi_k) = d(\phi_k^*) = 0$, so $\mathcal{L}_{\mathfrak{p}}(\phi_k^*) \neq 0$. Theorem 12.3 with $\phi = \phi_k^*$ and $\mathfrak{q} = \mathfrak{p}$ yields a generalisation of [23, Theorem 10.1].

Remark 12.4. It would be interesting to know whether or not $d(\phi_k) = 0$ whenever $\mathcal{L}_{\mathfrak{p}}^{(1)}(\phi_k) \neq 0$ and $\mathcal{R}_{K,\mathfrak{p}}^{(\phi_k)} \neq 0$. To show this, it would suffice (via an argument very similar to that given in [22, Proposition 11.6]) to show that if $x \in \Sigma_{\mathfrak{p}}(K, T)$ is of infinite order, then x cuts out an infinitely ramified extension of $\mathcal{K}_\infty$. If $k = 1$ and x is given by a point of infinite order on an elliptic curve, then this is true. However, it does not seem obvious that a similar assertion holds if $k > 1$ and $x \in \Sigma_{\mathfrak{p}}(K, T)$. $\square$

References

[1] A. Agboola, *On Rubin's variant of the p-adic Birch and Swinnerton-Dyer Conjecture*, Comp. Math. **143** (2007), 1374–1398.

[2] A. Agboola, *On Rubin's variant of the p-adic Birch and Swinnerton-Dyer Conjecture II*, Math. Ann. **349** (2011), no. 4, 807–837.

[3] D. Bernardi, C. Goldstein, N. Stephens, *Notes p-adiques sur les courbes elliptiques*, Crelle **351** (1985), 129–170.

[4] M. Bertolini, H. Darmon, K. Prasanna, *p-adic Rankin L-series and rational points on CM elliptic curves*, Pacific J. Math., **260** (2012), 261–303.

[5] S. Bloch, K. Kato, *L-functions and Tamagawa numbers of motives*, In: The Grothendieck Festschrift, Vol. I, 333–400, Progr. Math. **86**, Birkhauser (1990).

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

[7] J. Coates, *Infinite descent on elliptic curves with complex multiplication*, Shaferevich birthday volume.

[8] J. Coates, R. Sujatha, *Galois cohomology of elliptic curves*, Narosa Publishing House (2000).

[9] P. Colmez, *Théorie d'Iwasawa des répresentations de de Rham d'un corps local*, Ann. of Math. (2) **148** (1998), 485–471.

[10] E. de Shalit, *Iwasawa theory of elliptic curves with complex multiplication*, Academic Press (1987).

[11] R. Greenberg, *On the structure of certain Galois groups*, Invent. Math. **47** (1978), 85–99.

[12] R. Greenberg, *On the Birch and Swinnerton-Dyer conjecture*, Invent. Math. **72** (1983), 241–265.

[13] R. Greenberg, *Iwasawa theory for p-adic representations*, In: Algebraic number theory,97–137, Adv. Stud. Pure Math. **17**, Academic Press (1989).

[14] R. Greenberg, *Trivial zeros of p-adic L-functions*, In: p-adic monodromy and the Birch and Swinnerton-Dyer conjecture (Boston, MA, 1991), 149–174, Contemp. Math., 165, Amer. Math. Soc., Providence, RI, 1994.

[15] B. Howard, *Central derivatives of L-functions in Hida families*, Math. Ann. **339** no. 4 (2007), 803–818.

[16] B. Mazur, J. Tate, J. Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **84** (1986), 1–48.

[17] J. Neukirch, *Algebraic number theory*, Springer (1999).

[18] B. Perrin-Riou, *Déscent infinie et hauteurs p-adiques sur les courbes elliptiques à multiplication complexe*, Invent. Math. **70** (1983), 369–398.

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

[20] B. Perrin-Riou, *Arithmétique des courbes elliptiques et théorie d'Iwasawa*, Memoire de la Société Mathématique de France, **17** (1984).

[21] D. Rohrlich, *On L-functions of elliptic curves and anticyclotomic towers*, Invent. Math. **75** (1984), 383–408.

[22] K. Rubin, *Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication*, Invent. Math. **89** (1987), 527–560.

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

[24] K. Rubin, *p-adic variants of the Birch and Swinnerton-Dyer conjecture for elliptic curves with complex multiplication.* In: p-adic monodromy and the Birch and Swinnerton-Dyer conjecture (Boston, MA, 1991), 71–80, Contemp. Math., 165, Amer. Math. Soc., Providence, RI, 1994.

[25] K. Rubin, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. Math. **109** (1992), 25–68.

[26] K. Rubin, *Euler Systems*, Princeton University Press (2000).

[27] K. Rubin, *Euler systems and modular elliptic curves.* In: Galois representations in arithmetic geometry, A.J. Scholl, R. L. Taylor (Eds.), CUP 1998.

[28] J.-P. Serre, *Local Fields*, Springer Verlag (1979).

[29] S. Zhang, *On explicit reciprocity law over formal groups*, Int. J. Math. Sci. **9–12** (2004), 607–635.

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