ON RUBIN'S VARIANT OF THE p-ADIC BIRCH AND SWINNERTON-DYER CONJECTURE

A. AGBOOLA

Abstract. We study Rubin's variant of the p-adic Birch and Swinnerton-Dyer conjecture for CM elliptic curves concerning certain special values of the Katz two-variable p-adic L-function that lie outside the range of p-adic interpolation.

1. Introduction

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

Set $\mathcal{K}_\infty := K(E_{\pi^\infty})$, $\mathcal{K}^*_\infty := K(E_{\pi^{*\infty}})$, and $\mathfrak{K}_\infty := \mathcal{K}_\infty \mathcal{K}^*_\infty$. Write K_∞ (resp. K^*_∞) for the unique $\mathbf{Z}_p$ extension of K unramified outside $\mathfrak{p}$ (resp. $\mathfrak{p}^*$). Let $\mathcal{O}$ denote the completion of the ring of integers of the maximal unramified extension of $\mathbf{Q}_p$. For any extension L/K we set $\Lambda(L) := \Lambda(\mathrm{Gal}(L/K)) := \mathbf{Z}_p[[\mathrm{Gal}(L/K)]]$, and $\Lambda(L)_{\mathcal{O}} := \mathcal{O}[[\mathrm{Gal}(L/K)]]$. We write $X(L)$ (resp. $X^*(L)$) for the Pontryagin dual of the $\mathfrak{p}$-primary Selmer group $\mathrm{Sel}(L, E_{\pi^\infty})$ (resp. the $\mathfrak{p}^*$-primary Selmer group $\mathrm{Sel}(L, E_{\pi^{*\infty}})$) of E/L.

Let

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

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 [14, p. 325]. We write T (resp. T^*) for the $\mathfrak{p}$-adic (resp. $\mathfrak{p}^*$-adic) Tate module of E.

The two-variable Iwasawa main conjecture (proved by Rubin [16]) implies that $X(\mathfrak{K}_\infty)$ is a torsion $\Lambda(\mathfrak{K}_\infty)$-module whose characteristic ideal in $\Lambda(\mathfrak{K}_\infty)_{\mathcal{O}}$ is generated by a twist of

---

Date: Final version. January 22, 2007.

2000 *Mathematics Subject Classification.* 11G05, 11R23, 11G16.

Key words and phrases. Rubin, p-adic L-function, Birch and Swinnerton-Dyer conjecture, elliptic curve, Mazur-Tate-Teitelbaum.

Partially supported by NSF grant DMS-0401319.

Katz's two-variable p-adic L-function $\mathcal{L}_{\mathfrak{p}}$ by the character ψ. The function $\mathcal{L}_{\mathfrak{p}}$ satisfies a p-adic interpolation formula that may be described as follows (see [14, Theorem 7.1] for the version given here, and also [6, Theorem II.4.14]). 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 need not concern us here.

Define

$$L_{\mathfrak{p}}(s) := \mathcal{L}_{\mathfrak{p}}(\psi < \psi >^{s-1}), \quad L^*_{\mathfrak{p}}(s) := \mathcal{L}_{\mathfrak{p}}(\psi^* < \psi^* >^{s-1})$$

for $s \in \mathbf{Z}_p$. The character ψ lies within the range of interpolation of $\mathcal{L}_{\mathfrak{p}}$, and the $\mathfrak{p}$-adic Birch and Swinnerton-Dyer conjecture for E (see [1, pages 133–134], [12, Theorem V.8]) predicts that $\mathrm{ord}_{s=1} L_{\mathfrak{p}}(s)$ is equal to the rank r of $E(\mathbf{Q})$, and that

$$\lim_{s \to 1} \frac{L_{\mathfrak{p}}(s)}{(s-1)^r} \sim [\log_p(\psi(\gamma_1))]^r \cdot \left(1 - \frac{\psi(\mathfrak{p})}{p}\right) \cdot \left(1 - \frac{\psi(\mathfrak{p}^*)}{p}\right) \cdot |Ш(K)(\mathfrak{p})| \cdot R_{K,\mathfrak{p}},$$

where γ_1 is a topological generator of $\mathrm{Gal}(\mathcal{K}_\infty/K)$, $Ш(K)(\mathfrak{p})$ is the $\mathfrak{p}$-primary component of the Tate-Shafarevich group $Ш(K)$ of E/K, $R_{K,\mathfrak{p}}$ is the regulator associated to the algebraic $\mathfrak{p}$-adic height pairing

$$\{\ ,\ \}_{K,\mathfrak{p}} : \mathrm{Sel}(K, T^*) \times \mathrm{Sel}(K, T) \to O_{K,\mathfrak{p}}$$

on E/K (see [10]), and the symbol '$\sim$' denotes equality up to multiplication by a p-adic unit.

On the other hand, the character ψ^* lies outside the range of interpolation of $\mathcal{L}_{\mathfrak{p}}$ and the function $L^*_{\mathfrak{p}}(s)$ has not been studied nearly as much as $L_{\mathfrak{p}}(s)$. The only results concerning $L^*_{\mathfrak{p}}(s)$ of which the author is aware are due to Rubin (see [14], [15]). When $r \geq 1$, Rubin formulated a variant of the $\mathfrak{p}$-adic Birch and Swinnerton-Dyer conjecture for $L^*_{\mathfrak{p}}(s)$ which predicts that that $\mathrm{ord}_{s=1} L^*_{\mathfrak{p}}(s)$ is equal to $r-1$, and which gives a formula for $\lim_{s \to 1}[L^*_{\mathfrak{p}}(s)/(s-1)^{r-1}]$. Under suitable hypotheses, Rubin showed that his conjecture is equivalent to the usual $\mathfrak{p}$-adic Birch and Swinnerton-Dyer conjecture, and he proved both conjectures when $r = 1$. In the case $r = 1$, he then used these results to give a striking p-adic construction of a global point of infinite order in $E(\mathbf{Q})$ directly from the special value of a p-adic L-function.

When $r = 0$, however, the above analysis breaks down, and the situation is less clear. The functional equation satisfied by $\mathcal{L}_{\mathfrak{p}}$ (see [6, II §6]) shows that $\mathrm{ord}_{s=1} L_{\mathfrak{p}}(s)$ and $\mathrm{ord}_{s=1} L^*_{\mathfrak{p}}(s)$ have opposite parity, and so when $r = 0$, one expects that $\mathrm{ord}_{s=1} L^*_{\mathfrak{p}}(s)$ is odd. This may perhaps be viewed as being an analogue of a similar exceptional zero phenomenon observed in the work of Mazur, Tate and Teitelbaum concerning p-adic Birch and Swinnerton-Dyer conjectures for elliptic curves *without* complex multiplication (see [9], [8]). As Rubin points out (see [15, Remark on p. 74]), it is reasonable to guess that $\mathrm{ord}_{s=1} L_{\mathfrak{p}}^*(s) = 1$. If this is so, then one would like to determine the value of $\lim_{s \to 1}[L_{\mathfrak{p}}^*(s)/(s-1)]$.

In this paper we study an Iwasawa module naturally associated to $L_{\mathfrak{p}}^*(s)$ via the two-variable main conjecture and, among other things, we prove that the above guess is indeed correct. The Iwasawa module in question is the Pontryagin dual $X_{\mathfrak{p}^*}(K_\infty^*, W^*)$ of a certain *restricted Selmer group* $\Sigma_{\mathfrak{p}^*}(K_\infty^*, W^*)$. This restricted Selmer group is defined by *reversing* the Selmer conditions above $\mathfrak{p}$ and $\mathfrak{p}^*$ that are used to define the usual Selmer group $\mathrm{Sel}(K_\infty^*, W^*)$. The two-variable main conjecture implies that a characteristic power series $H_K \in \Lambda(K_\infty^*)$ of $X_{\mathfrak{p}^*}(K_\infty^*, W^*)$ may be viewed as being an algebraic p-adic L-function corresponding to $L_{\mathfrak{p}}^*(s)$. We study $L_{\mathfrak{p}}^*(s)$ by analysing the behaviour of H_K.

A special case of our results may be described as follows. We define a compact restricted Selmer group $\check{\Sigma}_{\mathfrak{p}^*}(K, T^*) \subseteq H^1(K, T^*)$. The $O_{K,\mathfrak{p}^*}$-module $\check{\Sigma}_{\mathfrak{p}^*}(K, T^*)$ is free of rank $|r-1|$, and if $r \geq 1$, then it lies in the usual Selmer group $\mathrm{Sel}(K, T^*)$ associated to T^*. The $O_{K,\mathfrak{p}^*}$-rank of $\check{\Sigma}_{\mathfrak{p}^*}(K, T^*)$ governs the order of vanishing of $L_{\mathfrak{p}}^*(s)$ at $s = 1$ in the same way that the $O_{K,\mathfrak{p}}$-rank of $\mathrm{Sel}(K, T)$ determines $\mathrm{ord}_{s=1} L_{\mathfrak{p}}(s)$. We also define a similar group $\check{\Sigma}_{\mathfrak{p}}(K, T) \subseteq H^1(K, T)$, and we explain how to construct a p-adic height pairing

$$[\,,\,]_{K,\mathfrak{p}^*} : \check{\Sigma}_{\mathfrak{p}}(K, T) \times \check{\Sigma}_{\mathfrak{p}^*}(K, T^*) \to O_{K,\mathfrak{p}^*}.$$

If $r \geq 1$, then in fact $\check{\Sigma}_{\mathfrak{p}}(K, T) \subseteq \mathrm{Sel}(K, T)$, $\check{\Sigma}_{\mathfrak{p}^*}(K, T^*) \subseteq \mathrm{Sel}(K, T^*)$, and, if the $\mathfrak{p}^*$-adic Birch and Swinnerton-Dyer conjecture is true, then the p-adic height pairing $[\,,\,]_{K,\mathfrak{p}^*}$ is non-degenerate. We conjecture that $[\,,\,]_{K,\mathfrak{p}^*}$ is also non-degenerate when $r = 0$ (see Remark 6.6).

Define

$$Ш_{\mathrm{rel}(\mathfrak{p})}(K) := \mathrm{Ker}\left[H^1(K, E) \to \prod_{v \nmid \mathfrak{p}} H^1(K_v, E)\right],$$

and write $Ш_{\mathrm{rel}(\mathfrak{p})}(K)(\mathfrak{p}^*)$ for its $\mathfrak{p}^*$-primary subgroup. Let $Ш_{\mathrm{rel}(\mathfrak{p})}(K)(\mathfrak{p}^*)_{/\,\mathrm{div}}$ denote the quotient of $Ш_{\mathrm{rel}(\mathfrak{p})}(K)(\mathfrak{p}^*)$ by its maximal divisible subgroup. It may be shown that $Ш_{\mathrm{rel}(\mathfrak{p})}(K)(\mathfrak{p}^*)$ has $O_{K,\mathfrak{p}^*}$-corank one, and that $Ш_{\mathrm{rel}(\mathfrak{p})}(K)(\mathfrak{p}^*)_{/\,\mathrm{div}}$ is finite.

Theorem A. *Suppose that* $[\ ,\ ]_{K,\mathfrak{p}^*}$ *is non-degenerate, and let* γ *be a topological generator of* $\mathrm{Gal}(\mathcal{K}^*_\infty/K)$*. Then, if* $r = 0$*, we have* $\mathrm{ord}_{s=1} L^*_{\mathfrak{p}}(s) = 1$*, and*

$$\lim_{s\to 1} \frac{L^*_{\mathfrak{p}}(s)}{s-1} \sim \log_p(\psi^*(\gamma)) \cdot (1 - \psi(\mathfrak{p}^*)) \cdot \frac{|\text{Ш}_{\mathrm{rel}(\mathfrak{p})}(K)(\mathfrak{p}^*)_{/\,\mathrm{div}}|}{[H^1(K_{\mathfrak{p}^*}, T) : \mathrm{loc}_{\mathfrak{p}^*}(\Sigma_{\mathfrak{p}}(K,T)]} \cdot \mathcal{R}_{K,\mathfrak{p}^*},$$

where $\mathcal{R}_{K,\mathfrak{p}^*}$ *is a* p*-adic regulator associated to* $[\ ,\ ]_{K,\mathfrak{p}^*}$*.*

We also obtain an exact (but much less explicit) formula for $\lim_{s\to 1} L^*_{\mathfrak{p}}(s)/(s-1)$ by applying the methods of [14] in our present setting (see Theorem 9.5 below).

Suppose now that $r \geq 1$, and assume that $\text{Ш}(K)(p)$ is finite. Then $E(K) \otimes_{O_K} O_{K,\mathfrak{p}^*}$ is a free $O_{K,\mathfrak{p}^*}$-module of rank r, and the kernel of the localisation map

$$E(K) \otimes_{O_K} O_{K,\mathfrak{p}^*} \to E(K_{\mathfrak{p}^*}) \otimes_{O_K} O_{K,\mathfrak{p}^*}$$

has $O_{K,\mathfrak{p}^*}$-rank $r-1$. Let $y_1, \dots, y_{r-1}$ be an $O_{K,\mathfrak{p}^*}$-basis of this kernel, and extend it to an $O_{K,\mathfrak{p}^*}$-basis $y_1, \dots, y_{r-1}, y_{\mathfrak{p}^*}$ of $E(K) \otimes_{O_K} O_{K,\mathfrak{p}^*}$. We write $x_1, \dots, x_{r-1}, y_{\mathfrak{p}}$ for a similarly constructed $O_{K,\mathfrak{p}}$-basis of $E(K) \otimes_{O_K} O_{K,\mathfrak{p}}$. The following result is a direct consequence of Rubin's precise formula for $\lim_{s\to 1}[L^*_{\mathfrak{p}}(s)/(s-1)^{r-1}]$ (see [14, Corollary 11.3]). We give a new proof of this result which is different from that contained in [14]. In particular, our proof gives an alternative way of viewing the somewhat unusual regulator $R^*_{\mathfrak{p}}$ defined in [14, §11].

Theorem B. *Suppose that* $r \geq 1$ *and that* $[\ ,\ ]_{K,\mathfrak{p}^*}$ *is non-degenerate. Then* $\mathrm{ord}_{s=1} L^*_{\mathfrak{p}}(s) = r - 1$*, and*

$$\lim_{s\to 1} \frac{L^*_{\mathfrak{p}}(s)}{(s-1)^{r-1}} \sim [\log_p(\psi^*(\gamma))]^{r-1} \cdot p^{-2} \cdot |\text{Ш}(K)(\mathfrak{p}^*)| \cdot \log_{E,\mathfrak{p}^*}(y_{\mathfrak{p}^*}) \cdot \log_{E,\mathfrak{p}}(y_{\mathfrak{p}}) \cdot \mathcal{R}_{K,\mathfrak{p}^*}, \tag{1.2}$$

where $\log_{E,\mathfrak{p}^*}$ *(resp.* $\log_{E,\mathfrak{p}}$*) denotes the* $\mathfrak{p}^*$*-adic (resp.* $\mathfrak{p}$*-adic) logarithm associated to* E*.*

An outline of the contents of this paper is as follows. In Section 2 we recall some basic facts about twists of Iwasawa modules and derivatives of characteristic power series, and we apply these results to describe the relationship between $L^*_{\mathfrak{p}}(s)$ and a characteristic power series $H_K \in \Lambda(K^*_\infty)$ of $X_{\mathfrak{p}^*}(K^*_\infty, W^*)$. In Section 3 we define various Selmer groups, and we establish some of their properties. We describe how to construct an algebraic p-adic height pairing on restricted Selmer groups in Section 4. In Section 5 we calculate (under certain hypotheses) the leading term of a characteristic power series $H_F \in \Lambda(F^*_\infty)$ of $X_{\mathfrak{p}^*}(F^*_\infty, W^*)$, where F/K is any finite extension, and $F^*_\infty := FK^*_\infty$. In Section 6 we study restricted Selmer groups over K, and we show that, under certain standard assumptions, $\mathrm{ord}_{s=1} L_{\mathfrak{p}}^*(s) = |r-1|$. We then give the proof of Theorem A in Section 7, and that of Theorem B in Section 8. Finally, in Section 9, we explain how the methods of [14] may be used to give a formula for the exact value of $\lim_{s\to 1} L_p^*(s)/(s-1)$ when $r=0$.

Acknowledgements. I am very grateful indeed to Karl Rubin for extremely helpful conversations and correspondence. Parts of this paper were written while I was visiting the Université de Bordeaux I and the Centre de Recherches Mathématiques at the Université de Montreal. I thank these institutions for their hospitality and support.

Notation and conventions. For each integer $n \geq 1$, we write

$$\mathcal{K}_n := K(E_{\pi^n}), \quad \mathcal{K}_n^* := K(E_{\pi^{*n}}).$$

For each place v of K, we write k_v for the residue field of v, and $\tilde{E}_v/k_v$ for the reduction of the elliptic curve E modulo v. We set $W := E_{\pi^\infty}$ and $W^* := E_{\pi^{*\infty}}$.

Throughout this paper, F denotes a finite extension of K, and we set

$$\begin{aligned}
&\mathcal{F}_n := F\mathcal{K}_n, \quad \mathcal{F}_\infty := F\mathcal{K}_\infty, \quad F_\infty := FK_\infty, \\
&\mathcal{F}_n^* := F\mathcal{K}_n^*, \quad \mathcal{F}_\infty^* := F\mathcal{K}_\infty^*, \quad F_\infty^* := FK_\infty^*, \\
&\mathfrak{F}_\infty := F\mathfrak{K}_\infty.
\end{aligned}$$

For any extension L/K we write $\mathcal{M}(L)$ (resp. $\mathcal{M}^*(L)$) for the maximal abelian pro-p extension of L which is unramified away from $\mathfrak{p}$ (resp. $\mathfrak{p}^*$), and we set

$$\mathcal{X}(L) := \mathrm{Gal}(\mathcal{M}(L)/L), \quad \mathcal{X}^*(L) := \mathrm{Gal}(\mathcal{M}^*(L)/L).$$

We let $\mathcal{B}(L)$ (resp. $\mathcal{B}^*(L)$) denote the maximal abelian pro-p extension of L which is unramified away from $\mathfrak{p}$ (resp. $\mathfrak{p}^*$) and totally split at all places of L lying above $\mathfrak{p}^*$ (resp. $\mathfrak{p}$), and we write

$$\mathcal{Y}(L) := \mathrm{Gal}(\mathcal{B}(L)/L), \quad \mathcal{Y}^*(L) := \mathrm{Gal}(\mathcal{B}^*(L)/L).$$

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 $O_{K,\mathfrak{q}}$-module, with $\mathfrak{q} \in \{\mathfrak{p}, \mathfrak{p}^*\}$, then we write $T_{\mathfrak{q}}(M)$ for the $\mathfrak{q}$-adic Tate module of M.

We set $D_{\mathfrak{p}} := K_{\mathfrak{p}}/O_{K,\mathfrak{p}}$ and $D_{\mathfrak{p}^*} := K_{\mathfrak{p}^*}/O_{K,\mathfrak{p}^*}$.

2. Twists and derivatives

In this section we shall recall some basic facts concerning twists of Iwasawa modules and derivatives of characteristic power series. We then apply these results to a twist of the Katz two-variable p-adic L-function $\mathcal{L}_{\mathfrak{p}}$ by the character ψ^*.

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 we have 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 $g \in \mathcal{G}_F$. If M is a finitely generated $\Lambda(\mathcal{G}_F)$-module with characteristic power series f_M, 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 $\Pi_{\mathcal{G}_F/\mathcal{H}}(\mathrm{Tw}_\rho(f_M))$ 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

$$[\mathrm{Tw}_\rho(f_M)](\rho_1) = [\Pi_{\mathcal{G}_F/\mathcal{H}}(\mathrm{Tw}_\rho(f_M))](\rho_1), \tag{2.1}$$

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 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 $\Pi_{\mathcal{G}/\mathcal{H}}(\mathrm{Tw}_\rho(f_M))$ at such characters.

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

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

where $|\Delta|$ is prime to p, and $G \simeq \mathbf{Z}_p$. Let γ be a fixed topological generator of $\mathcal{G}_F/\mathcal{H}$, and let $\Pi_G : \Lambda(\mathcal{G}_F/\mathcal{H}) \to \Lambda(G)$ be the natural quotient map. We identify $\Lambda(G)$ with $\mathbf{Z}_p[[t]]$ in the usual way via the map $\Pi_G(\gamma) \mapsto 1+t$.

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 largest integer such that $f_N \in I^n_{\mathcal{G}_F/\mathcal{H}}$ and $f_N \notin I^{n+1}_{\mathcal{G}_F/\mathcal{H}}$. It is not hard to check that $\Pi_G(f_N)(t)$ is a characteristic power series of the $\Lambda(G)$-module N^Δ, and that

$$((\gamma-1)^{-n} f_N)(\mathbf{1}) = \left.\frac{\Pi_G(f_N)}{t^n}\right|_{t=0}, \tag{2.2}$$

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 $\vartheta_\nu := \nu(\gamma)^{-1}\gamma - 1$. Then if $m \geq 0$ is any integer, it follows from the definitions that we have

$$(\vartheta_\nu^{-m} f_N)(\nu) = [(\gamma - 1)^{-m}\,\mathrm{Tw}_\nu(f_N)](\mathbf{1}), \tag{2.3}$$

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

We now recall how (2.3) is related to derivatives of certain p-adic analytic functions as described in [14, §7]. Write $<\nu>: \mathcal{G}_F/\mathcal{H} \to \mathbf{Z}_p^\times$ for the composition of ν with the natural projection $\mathbf{Z}_p^\times \to 1 + p\mathbf{Z}_p$, and suppose that $\chi : \mathcal{G}_F/\mathcal{H} \to \mathbf{Z}_p^\times$ is any character of order prime to p. The map from $\mathbf{Z}_p$ to $\mathbf{C}_p$ given by $s \mapsto f_N(\nu\chi <\nu>^{s-1})$ defines an analytic function on $\mathbf{Z}_p$. Define

$$\mathrm{ord}_{\nu\chi}(f_N) := \mathrm{ord}_{s=1}\, f_N(\nu\chi <\nu>^{s-1}),$$

and set

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

We write

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

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

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

and

$$\mathbf{D}^{(m)}(\vartheta_\nu^m f_N)(\nu\chi) = \{\log_p(\nu(\gamma))\}^m f_N(\nu\chi) = [\{\log_p(\nu(\gamma))\}^m\,\mathrm{Tw}_\nu(f_N)](\chi). \tag{2.4}$$

We can now see from (2.2), (2.3) and (2.4) that if $n_\nu := \mathrm{ord}_\nu(f_N)$, then we may write $f_N = \vartheta_\nu^{n_\nu} F_\nu$ with $F_\nu \in \Lambda(\mathcal{G}_F/\mathcal{H})$, and we have

$$\begin{aligned}
f_N^{(n_\nu)}(\nu) &= \lim_{s\to 1} \frac{f_N(\nu <\nu>^{s-1})}{(s-1)^{n_\nu}} \\
&= \mathbf{D}^{(n_\nu)}(\vartheta_\nu^{n_\nu} F_\nu)(\nu) \\
&= [\{\log_p(\nu(\gamma))\}^{n_\nu}\,\mathrm{Tw}_\nu(F_\nu)](\mathbf{1}) \\
&= \{\log_p(\nu(\gamma))\}^{n_\nu} \cdot \Pi_G(\mathrm{Tw}_\nu(F_\nu))(0) \\
&= \{\log_p(\nu(\gamma))\}^{n_\nu} \cdot \frac{\Pi_G(\mathrm{Tw}_\nu(f_N))}{t^{n_\nu}}\bigg|_{t=0}.
\end{aligned} \tag{2.5}$$

We shall now apply the above discussion to the case in which $F = K$, $M = \mathcal{X}(\mathfrak{K}_\infty)$, $\rho = \nu = \psi^*$, $\mathcal{H} = \mathrm{Gal}(\mathfrak{K}_\infty/\mathcal{K}_\infty^*)$, $G = \mathrm{Gal}(K_\infty^*/K)$ and $\chi = \mathbf{1}$.

Recall that the two-variable main conjecture asserts that $\mathcal{X}(\mathfrak{K}_\infty)$ is a torsion $\Lambda(\mathfrak{K}_\infty)$-module, and that the Katz two-variable p-adic L-function $\mathcal{L}_\mathfrak{p}$ is a characteristic power series of $\mathcal{X}(\mathfrak{K}_\infty)$ in $\Lambda(\mathfrak{K}_\infty)_{\mathcal{O}}$. We therefore see that $\mathrm{Tw}_{\psi^*}(\mathcal{L}_{\mathfrak{p}}) \in \Lambda(\mathfrak{K}_\infty)_{\mathcal{O}}$ is a characteristic power series of $\mathcal{X}(\mathfrak{K}_\infty)(\psi^{*-1})$. Let $I_{K^*_\infty}$ denote the kernel of the natural map $\Lambda(\mathfrak{K}_\infty) \to \Lambda(K^*_\infty)$. Fix any characteristic power series $H_K \in \Lambda(K^*_\infty)$ of the $\Lambda(K^*_\infty)$-module

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

Then we deduce from (2.1), (2.2) and (2.5) that

$$\mathrm{ord}_{s=1} L^*_{\mathfrak{p}}(s) = \mathrm{ord}_{t=0} H_K, \tag{2.6}$$

and if we set $n_{\psi^*} := \mathrm{ord}_{s=1} L^*_{\mathfrak{p}}(s)$, then

$$\mathcal{L}_{\mathfrak{p}}^{(n_{\psi^*})}(\psi^*) = \lim_{s \to 1} \frac{L^*_{\mathfrak{p}}(s)}{(s-1)^{n_{\psi^*}}} \sim \{\log_p(\psi^*(\gamma))\}^{n_{\psi^*}} \cdot \left.\frac{H_K}{t^{n_{\psi^*}}}\right|_{t=0}, \tag{2.7}$$

where '$\sim$' denotes equality up to multiplication by a p-adic unit (in fact, in this case, we have equality up to multiplication by an element of $\mathcal{O}^\times$).

3. Selmer Groups

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

For any place v of F, we define $H^1_f(F_v, W)$ to be the image of $E(F_v) \otimes D_{\mathfrak{p}}$ under the Kummer map

$$E(F_v) \otimes D_{\mathfrak{p}} \to H^1(F_v, W),$$

and we define $H^1_f(F_v, W^*)$ in a similar manner. Note that $H^1_f(F_v, W) = 0$ if $v \nmid \mathfrak{p}$. We also set

$$H^1_f(F_v, E_{\pi^n}) := \mathrm{Im}[E(F_v)/\pi^n E(F_v) \to H^1(F_v, E_{\pi^n})],$$
$$H^1_f(F_v, E_{\pi^{*n}}) := \mathrm{Im}[E(F_v)/\pi^{*n} E(F_v) \to H^1(F_v, E_{\pi^{*n}})].$$

Suppose that $M \in \{W, W^*, E_{\pi^n}, E_{\pi^{*n}}\}$ 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

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

(The terminology 'restricted Selmer group' is meant to reflect a choice of a combination of relaxed and strict Selmer conditions at places above p.)

We also define

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

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

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

Theorem 3.1. *Let L be any field such that $\mathcal{F}_\infty^* \subseteq L \subseteq \mathfrak{F}_\infty$. Then there is an isomorphism*

$$X_{\mathfrak{p}^*}(L, W^*) \simeq \mathcal{X}(L)(\psi^{*-1}) \tag{3.1}$$

of $\Lambda(L)$-modules.

Proof. This is simply the analogue for restricted Selmer groups of a well-known theorem of Coates concerning true Selmer groups (see [4, Theorem 12]). We first observe that, since $\mathcal{F}_\infty^* \subseteq L$, we have isomorphisms of $\Lambda(L)$-modules

$$\mathcal{X}(L)(\psi^{*-1}) \simeq \mathrm{Hom}(T^*, \mathcal{X}(L)), \qquad \mathcal{X}(L)(\psi^{*-1})^\wedge \simeq \mathrm{Hom}(\mathcal{X}(L), W^*).$$

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

$$\Sigma_{\mathfrak{p}^*}(L, W^*) \xrightarrow{\sim} \mathrm{Hom}(\mathcal{X}(L), W^*). \tag{3.2}$$

This may be proved in exactly the same way as [4, Theorem 12]. □

The following result is a 'control theorem' for restricted Selmer groups.

Proposition 3.2. *(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*

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

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

$$e_F = (\gamma - \psi^{*-1}(\gamma))^{-1} \prod_{v|\mathfrak{p}^*} (\gamma_v - \psi^{*-1}(\gamma_v)),$$

where γ is a topological generator of $\mathrm{Gal}(\mathcal{F}^*_\infty/F)$, and, for each place v of $\mathcal{F}^*_\infty$ lying above $\mathfrak{p}^*$, 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 $X_{\mathfrak{p}^*}(\mathcal{F}^*_\infty, W^*)$, then $e_F^{-1}\Pi_{\mathcal{F}^*_\infty}(f) \in \Lambda(\mathcal{F}^*_\infty)$ is a characteristic power series of $X_{\mathfrak{p}^*}(\mathcal{F}^*_\infty, W^*)$.

(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

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

is an isomorphism.

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

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

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:

$$\begin{array}{ccccccc}
0 \longrightarrow & \Sigma_{\mathfrak{p}^*}(\mathcal{F}^*_\infty, W^*) & \longrightarrow & H^1(\mathcal{N}/\mathcal{F}^*_\infty, W^*) & \xrightarrow{\mathrm{loc}_{\mathfrak{p}^*}} & \prod_{v|\mathfrak{p}^*} H^1(\mathcal{N}_v/\mathcal{F}^*_{\infty,v}, W^*) \\
& \alpha\downarrow & & \downarrow & & \downarrow \\
0 \longrightarrow & \Sigma_{\mathfrak{p}^*}(\mathfrak{F}_\infty, W^*)[I_{\mathcal{F}^*_\infty}] & \longrightarrow & H^1(\mathcal{N}/\mathfrak{F}_\infty, W^*)[I_{\mathcal{F}^*_\infty}] & \xrightarrow{\mathrm{loc}_{\mathfrak{p}^*}} & \prod_{v|\mathfrak{p}^*} H^1(\mathcal{N}_v/\mathfrak{F}_{\infty,v}, W^*)
\end{array}$$

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

$$\begin{aligned}
0 \to \mathrm{Ker}(\alpha) \to H^1(\mathfrak{F}_\infty/\mathcal{F}^*_\infty, W^*) &\xrightarrow{g_1} \prod_{v|\mathfrak{p}^*} H^1(\mathfrak{F}_{\infty,v}/\mathcal{F}^*_{\infty,v}, W^*) \to \\
\to \mathrm{Coker}(\alpha) \to H^2(\mathfrak{F}_\infty/\mathcal{F}^*_\infty, W^*) &\xrightarrow{g_2} \prod_{v|\mathfrak{p}^*} H^2(\mathfrak{F}_{\infty,v}/\mathcal{F}^*_{\infty,v}, W^*) \to 0. \qquad (3.3)
\end{aligned}$$

Now,

$$\begin{aligned} &H^1(\mathfrak{F}_\infty/\mathcal{F}_\infty^*, W^*) \simeq \mathrm{Hom}(\mathrm{Gal}(\mathfrak{F}_\infty/\mathcal{F}_\infty^*), W^*), \\ &\prod_{v|\mathfrak{p}^*} H^1(\mathfrak{F}_{\infty,v}/\mathcal{F}_{\infty,v}^*, W^*) \simeq \prod_{v|\mathfrak{p}^*} \mathrm{Hom}(\mathrm{Gal}(\mathfrak{F}_{\infty,v}/\mathcal{F}_{\infty,v}^*), W^*), \end{aligned} \tag{3.4}$$

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

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

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 (3.3) that $\mathrm{Ker}(\alpha)$ is finite, and that there is an exact sequence

$$0 \to \mathrm{Ker}(\alpha) \to H^1(\mathfrak{F}_\infty/\mathcal{F}_\infty^*, W^*) \xrightarrow{g_1} \prod_{v|\mathfrak{p}^*} H^1(\mathfrak{F}_{\infty,v}/\mathcal{F}_{\infty,v}^*, W^*) \to \mathrm{Coker}(\alpha) \to 0. \tag{3.5}$$

It follows from (3.4) that

$$\begin{aligned} &\mathrm{Char}_{\Lambda(\mathcal{F}_\infty^*)} \left(H^1(\mathfrak{F}_\infty/\mathcal{F}_\infty^*, W^*)\right)^\wedge = \gamma - \psi^{*-1}(\gamma); \\ &\mathrm{Char}_{\Lambda(\mathcal{F}_\infty^*)} \left(\prod_{v|\mathfrak{p}^*} H^1(\mathfrak{F}_{\infty,v}/\mathcal{F}_{\infty,v}^*, W^*)\right)^\wedge = \prod_{v|\mathfrak{p}^*}(\gamma_v - \psi^{*-1}(\gamma_v)). \end{aligned}$$

Hence we deduce from (3.5) that

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

as asserted.

(b) In this case we consider the commutative diagram

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

We have that

$$\begin{aligned} \mathrm{Ker}(\beta_2) &= H^1(\mathcal{F}_\infty^*/L, W^*) = 0, \\ \mathrm{Ker}(\beta_3) &= \prod_{v|\mathfrak{p}^*} H^1(\mathcal{F}_{\infty,v}^*/L_v, W^*) = 0, \\ \mathrm{Coker}(\beta_2) &= H^2(\mathcal{F}_\infty^*/L, W^*) = 0, \end{aligned}$$

(see [12, p. 40], for example), and so the Snake Lemma implies that β_1 is an isomorphism, as claimed. □

Corollary 3.3. *For any field L with $F \subseteq L \subseteq \mathcal{F}_\infty^*$, we have an isomorphism*

$$X_{\mathfrak{p}^*}(L, T^*) \simeq \mathcal{X}(\mathcal{F}_\infty)(\psi^{*-1})/I_L(\mathcal{X}(\mathcal{F}_\infty)(\psi^{*-1}) \tag{3.6}$$

of $\Lambda(L)$-modules.

Proof. This follows directly from Proposition 3.2 and Theorem 3.1. □

Remark 3.4. If we take $F = K$ in Proposition 3.2, then it is easy to check that $e_K \in \Lambda(\mathcal{K}_\infty^*)^\times$. We therefore see from Proposition 3.2(a) and Corollary 3.3 that the element $H_K \in \Lambda(K_\infty^*)$ fixed in Section 2 is a characteristic power series of $X_{\mathfrak{p}^*}(K_\infty^*, W^*)$. □

Definition 3.5. For any finite extension F/K and any prime $\mathfrak{q}$ of K we define

$$Ш(F)_{\mathrm{rel}(\mathfrak{q})} := \mathrm{Ker}\left[H^1(F, E) \to \prod_{v \nmid \mathfrak{q}} H^1(F_v, E) \right],$$

and we set

$$E_{1,\mathfrak{q}}(F) := \mathrm{Ker}\left[E(F) \otimes_{O_K} O_{K,\mathfrak{q}} \to \prod_{v \mid \mathfrak{q}} E(F_v) \right].$$

□

Lemma 3.6. *Let F/K be any finite extension, and let $\mathfrak{q} \in \{\mathfrak{p}, \mathfrak{p}^*\}$. Then $\check{\Sigma}_{\mathfrak{q}}(F, T_{\mathfrak{q}})$ is a free $O_{K,\mathfrak{q}}$-module.*

Proof. It follows from the definitions that $\check{\Sigma}_{\mathfrak{q}}(F, T_{\mathfrak{q}})_{\mathrm{tors}} \subseteq \check{\mathrm{Sel}}(F, T_{\mathfrak{q}})$. The desired result now follows from the fact that the restriction of the localisation map

$$\check{\mathrm{Sel}}(F, T_{\mathfrak{q}}) \to \prod_{v \mid \mathfrak{q}} E(F_v) \otimes_{O_K} O_{K,\mathfrak{q}}$$

to $\check{\mathrm{Sel}}(F, T_{\mathfrak{q}})_{\mathrm{tors}}$ is injective. □

4. The p-adic height pairing on restricted Selmer groups

In this section we shall explain how the methods described by Perrin-Riou in [10] and [12] may be used to construct a p-adic height pairing

$$[\ ,\ ]_{F,\mathfrak{p}^*} : \Sigma_{\mathfrak{p}}(F, T) \times \Sigma_{\mathfrak{p}^*}(F, T^*) \to O_{K,\mathfrak{p}^*}.$$

We begin by describing the $\mathfrak{p}$-adic Leopoldt hypotheses with which we shall work.

Definition 4.1. Let M/K be any finite extension, and consider the diagonal injection

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

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

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

The *weak* $\mathfrak{p}$*-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* $\mathfrak{p}$*-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 [2]). □

Recall that $\mathcal{B}(\mathcal{F}_\infty^*)$ denotes the maximal abelian pro-p extension of $\mathcal{F}_\infty^*$ which is unramified away from $\mathfrak{p}$ and totally split at all places above $\mathfrak{p}^*$, and that $\mathcal{Y}(\mathcal{F}_\infty^*) = \mathrm{Gal}(\mathcal{B}(\mathcal{F}_\infty^*)/\mathcal{F}_\infty^*)$. The main ingredient in the construction of $[\,,\,]_{F,\mathfrak{p}^*}$ is the following result.

Theorem 4.2. *If the weak* $\mathfrak{p}$*-adic Leopoldt hypothesis holds for* F *then there is a natural isomorphism*

$$\Psi_F : \check{\Sigma}_{\mathfrak{p}}(F,T) \xrightarrow{\sim} \mathrm{Hom}(T^*, \mathcal{Y}(\mathcal{F}_\infty^*))^{\mathrm{Gal}(\mathcal{F}_\infty^*/F)}.$$

The proof of this theorem is very similar to that of [10, Théorème 3.2]. We shall therefore just describe the main outlines of the proof, and we refer the reader to [10] for some of the details which we omit.

In order to describe the proof of Theorem 4.2, we require a number of intermediary results.

Lemma 4.3. *There is an isomorphism of* $\mathrm{Gal}(\mathcal{F}_n^*/F)$*-modules*

$$H^1(\mathcal{F}_n^*, E_{\pi^n}) \xrightarrow{\sim} \mathrm{Hom}(E_{\pi^{*n}}, \mathcal{F}_n^{*\times}/\mathcal{F}_n^{*\times p^n}); \quad f \mapsto \tilde{f}. \tag{4.1}$$

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

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

Proof. See [10, Lemme 3.8]. The isomorphism (4.1) is defined as follows. Let $f \in H^1(\mathcal{F}_n^*, E_{\pi^n})$, and write

$$w_n : E_{\pi^n} \times E_{\pi^{*n}} \longrightarrow \mu_{p^n}$$

for the Weil pairing. We identify $\mathcal{F}_n^{*\times}/\mathcal{F}_n^{*\times p^n}$ with $H^1(\mathcal{F}_n^*, \mu_{p^n})$ via Kummer theory. If $u \in E_{\pi^{*n}}$, then $\tilde{f}(u) \in H^1(\mathcal{F}_n^*, \mu_{p^n})$ is defined to be the element represented by the cocycle

$$\sigma \mapsto w_n(f(\sigma), u)$$

for all $\sigma \in \mathrm{Gal}(\overline{F}/\mathcal{F}_n^*)$. □

Lemma 4.4. *For each place v of $\mathcal{F}_n^*$ with $v \nmid \mathfrak{p}^*$, there is an isomorphism*

$$E(\mathcal{F}_{n,v}^*)/\pi^n E(\mathcal{F}_{n,v}^*) \xrightarrow{\sim} \mathrm{Hom}(E_{\pi^{*n}}, O_{\mathcal{F}_{n,v}^*}^\times / O_{\mathcal{F}_{n,v}^*}^{\times p^n}).$$

Proof. See [10, Lemme 3.11]. □

Corollary 4.5. *Suppose that $h \in H^1(\mathcal{F}_n^*, E_{\pi^n})$. Then $h \in \Sigma_{\mathfrak{p}}(\mathcal{F}_n^*, E_{\pi^n})$ if and only if, for each $u \in E_{\pi^n}$, the following local conditions are satisfied:*
(a) $\tilde{h}(u) \in \mathcal{F}_{n,v}^{*\times p^n}$ for all $v \mid \mathfrak{p}$;
(b) $p^n \mid v_{\mathcal{F}_n^*}(\tilde{h}(u))$ for all $v \nmid \mathfrak{p}^*$.
(Note that we impose no local conditions at places lying above $\mathfrak{p}^*$.)

Proof. This follows directly from Lemmas 4.3 and 4.4. □

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

$$C_n := J_n/V_n\mathcal{F}_n^{*\times}, \qquad \Omega_n := \prod_{v \mid \mathfrak{p}} \mu_{p^n}(\mathcal{F}_{n,v}^*),$$

and we note that the order of Ω_n is bounded as n varies.

Proposition 4.6. *There is an exact sequence*

$$\mathrm{Hom}(E_{\pi^{*n}}, \Omega_n)^{G_n} \to \mathrm{Hom}(E_{\pi^{*n}}, C_n)^{G_n} \xrightarrow{\eta_n} \Sigma_{\mathfrak{p}}(F, E_{\pi^n}) \to 0.$$

Proof. The proof of this Proposition is identical, *mutatis mutandis*, to that of [10, Proposition 3.13]. □

Now let η_n' be the map obtained from η_n via passage to the quotient by the kernel of η_n, and write $C_n(p)$ for the p-primary part of C_n. Then it may be shown exactly as on [10, pp. 387–389] that passing to inverse limits over the maps $\eta_n'^{-1}$ yields an isomorphism

$$\Xi_F : \varprojlim \check{\Sigma}_{\mathfrak{p}}(F, E_{\pi^n}) = \Sigma_{\mathfrak{p}}(F, T) \xrightarrow{\sim} \mathrm{Hom}(T^*, \varprojlim C_n(p))^{\mathrm{Gal}(\mathcal{F}_\infty^*/F)}.$$

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

The proof of Theorem 4.2 is completed by the following result.

Proposition 4.7. *If the weak $\mathfrak{p}$-adic Leopoldt hypothesis holds for F, then there is an isomorphism*

$$\mathrm{Hom}(T^*, \varprojlim C_n(p))^{\mathrm{Gal}(\mathcal{F}_\infty^*/F)} \simeq \mathrm{Hom}(T^*, \mathcal{Y}(\mathcal{F}_\infty^*))^{\mathrm{Gal}(\mathcal{F}_\infty^*/F)}.$$

Proof. This may be shown in the same way as [10, Lemme 3.18]. □

We now explain how the isomorphism Ψ_F may be used to construct a p-adic height pairing

$$[\,,\,]_{F,\mathfrak{p}^*} : \check{\Sigma}_{\mathfrak{p}}(F,T) \times \check{\Sigma}_{\mathfrak{p}^*}(F,T^*) \to O_{K,\mathfrak{p}^*}.$$

We first recall (see Proposition 3.2(b)) that the restriction map

$$\Sigma_{\mathfrak{p}^*}(F,W^*) \to \Sigma_{\mathfrak{p}^*}(\mathcal{F}^*_\infty, W^*) \tag{4.2}$$

is injective, and that there is a natural isomorphism (see Theorem 3.1)

$$\Sigma_{\mathfrak{p}^*}(\mathcal{F}^*_\infty, W^*) \xrightarrow{\sim} \mathrm{Hom}(\mathcal{X}(\mathcal{F}^*_\infty), W^*). \tag{4.3}$$

It follows from the local conditions defining the restricted Selmer group $\Sigma_{\mathfrak{p}^*}(F,W^*)$ that (4.2) and (4.3) induce an injection

$$\Sigma_{\mathfrak{p}^*}(F,W^*) \to \mathrm{Hom}(\mathcal{Y}(\mathcal{F}^*_\infty), W^*), \tag{4.4}$$

and taking Pontryagin duals yields a surjection

$$\mathrm{Hom}(T^*, \mathcal{Y}(\mathcal{F}^*_\infty)) \to X_{\mathfrak{p}^*}(F,W^*). \tag{4.5}$$

Composing this with the natural surjection

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

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

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

Next, we observe that we have a canonical isomorphism

$$\begin{aligned}[\Sigma_{\mathfrak{p}^*}(F,W^*)_{\mathrm{div}}]^\wedge &\simeq \mathrm{Hom}_{O_{K,\mathfrak{p}^*}}(T_{\mathfrak{p}^*}(\Sigma_{\mathfrak{p}^*}(F,W^*)_{\mathrm{div}}), O_{K,\mathfrak{p}^*})\\ &= \mathrm{Hom}_{O_{K,\mathfrak{p}^*}}(T_{\mathfrak{p}^*}(\Sigma_{\mathfrak{p}^*}(F,W^*)), O_{K,\mathfrak{p}^*}),\end{aligned}$$

where the last equality holds because

$$T_{\mathfrak{p}^*}(\Sigma_{\mathfrak{p}^*}(F,W^*)_{\mathrm{div}} = T_{\mathfrak{p}^*}(\Sigma_{\mathfrak{p}^*}(F,W^*)).$$

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

$$\Sigma_{\mathfrak{p}^*}(F, E_{\pi^{*n}}) \to \Sigma_{\mathfrak{p}^*}(F,W^*)_{\pi^{*n}}$$

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

$$\check{\Sigma}_{\mathfrak{p}^*}(F,T^*) \to T_{\mathfrak{p}^*}(\Sigma_{\mathfrak{p}^*}(F,W^*))$$

which is an isomorphism because $\check{\Sigma}_{\mathfrak{p}^*}(F,T^*)$ is $O_{K,\mathfrak{p}^*}$-free (see Lemma 3.6).

It follows from the above discussion that we may view β_F as a homomorphism

$$\beta_F : \mathrm{Hom}(T^*, \mathcal{Y}(\mathcal{F}^*_\infty))^{\mathrm{Gal}(\mathcal{F}^*_\infty/F)} \to \mathrm{Hom}_{O_{K,\mathfrak{p}^*}}(\check{\Sigma}_{\mathfrak{p}^*}(F,T^*), O_{K,\mathfrak{p}^*}).$$

We thus obtain a map

$$\beta_F \circ \Psi_F : \check{\Sigma}_{\mathfrak{p}}(F,T) \to \mathrm{Hom}_{O_{K,\mathfrak{p}^*}}(\check{\Sigma}_{\mathfrak{p}^*}(F,T^*), O_{K,\mathfrak{p}^*}),$$

and this yields the desired pairing

$$[\,,\,]_{F,\mathfrak{p}^*} : \check{\Sigma}_{\mathfrak{p}}(F,T) \times \check{\Sigma}_{\mathfrak{p}^*}(F,T^*) \to O_{K,\mathfrak{p}^*}.$$

It is natural to conjecture that this pairing is always non-degenerate (see Remark 6.6).

If $x_1, \ldots, x_m$ is an $O_{K,\mathfrak{p}}$-basis of $\check{\Sigma}_{\mathfrak{p}}(F,T)$ (resp. if $y_1, \ldots, y_m$ is an $O_{K,\mathfrak{p}^*}$-basis of $\check{\Sigma}_{\mathfrak{p}^*}(F,T^*)$), then we define the regulator $\mathcal{R}_{F,\mathfrak{p}^*}$ associated to $[\,,\,]_{F,\mathfrak{p}^*}$ by

$$\mathcal{R}_{F,\mathfrak{p}^*} := \det([x_i, y_j]_{F,\mathfrak{p}^*}). \tag{4.6}$$

5. The leading term

We retain the notation of the previous section. Write $\Gamma_F := \mathrm{Gal}(F^*_\infty/F)$, fix a topological generator γ_F of Γ_F, and identify $\Lambda(F^*_\infty)$ with the power series ring $\mathbf{Z}_p[[t]]$ via the map $\gamma_F \mapsto t+1$. Let $H_F \in \Lambda(F^*_\infty)$ be a characteristic power series of $X_{\mathfrak{p}^*}(F^*_\infty, W^*)$. In this section we shall calculate the leading coefficient of H_F, assuming that the strong Leopoldt hypothesis holds for F and that $[\,,\,]_{F,\mathfrak{p}^*}$ is non-degenerate.

Proposition 5.1. *Suppose that F satisfies the strong $\mathfrak{p}$-adic Leopoldt hypothesis. Then the $\Lambda(F^*_\infty)$-module $X_{\mathfrak{p}^*}(F^*_\infty, W^*)$ has no finite, non-trivial submodules.*

Proof. It is straightforward to show that a slight modification of the arguments given in [7, §4] establishes the fact that if F satisfies the strong $\mathfrak{p}$-adic Leopoldt hypothesis, then the $\Lambda(F^*_\infty)$-module $X(F^*_\infty)$ has no finite, non-trivial submodules. For brevity, we omit the details. The desired result now follows from Proposition 3.2 and Theorem 3.1. □

Theorem 5.2. *Let $H_F \in \Lambda(F^*_\infty)$ be a characteristic power series of $X_{\mathfrak{p}^*}(F^*_\infty, W^*)$. Assume that the strong $\mathfrak{p}$-adic Leopoldt hypothesis holds for F, and that $[\,,\,]_{F,\mathfrak{p}^*}$ is non-degenerate. Set $m := \mathrm{rk}_{O_{K,\mathfrak{p}^*}}(\check{\Sigma}_{\mathfrak{p}^*}(F,T^*))$. Then $\mathrm{ord}_{t=0} H_F = m$, and*

$$\left.\frac{H_F}{t^m}\right|_{t=0} \sim |\Sigma_{\mathfrak{p}^*}(F,W^*)_{/\,\mathrm{div}}| \cdot \mathcal{R}_{F,\mathfrak{p}^*}. \tag{5.1}$$

Proof. We begin by noting that there is a surjective homomorphism

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

This implies that H_F is divisible by t^m. If we write Z_∞ for the kernel of this map, then the Snake Lemma yields the following exact sequence:

$$\begin{aligned} 0 \to (Z_\infty)^{\Gamma_F} \to X_{\mathfrak{p}^*}(F^*_\infty, W^*)^{\Gamma_F} &\xrightarrow{\xi_F} [\Sigma_{\mathfrak{p}^*}(F, W^*)_{\mathrm{div}}]^\wedge \to \\ \to (Z_\infty)_{\Gamma_F} \to X_{\mathfrak{p}^*}(F^*_\infty, W^*)_{\Gamma_F} &\to [\Sigma_{\mathfrak{p}^*}(F, W^*)_{\mathrm{div}}]^\wedge \to 0. \end{aligned}$$

The kernel of the last map

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

is dual to the cokernel of the map

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

Since $\Sigma_{\mathfrak{p}^*}(F, W^*) \simeq \Sigma_{\mathfrak{p}^*}(F^*_\infty, W^*)^{\Gamma_F}$ (via Proposition 3.2(b)), it follows that this cokernel is isomorphic to $\Sigma_{\mathfrak{p}^*}(F, W^*)_{/\,\mathrm{div}}$, which is finite.

We therefore deduce that the multiplicity of t in H_F is equal to m 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 (see Theorem 3.1)

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

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

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

(see (4.4), (4.5)). Hence the cokernel of ξ_F is finite if and only if the p-adic height pairing $[\,,\,]_{F,\mathfrak{p}^*}$ is non-degenerate.

We now see that if $[\,,\,]_{F,\mathfrak{p}^*}$ 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 5.1 that $(Z_\infty)^{\Gamma_F} = 0$. Hence we have

$$\left.\frac{H_F}{t^m}\right|_{t=0} \sim |(Z_\infty)_{\Gamma_F}| \sim |\Sigma_{\mathfrak{p}^*}(F, W^*)_{/\,\mathrm{div}}| \cdot |\operatorname{Coker}(\xi_F)|.$$

Now

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

Hence

$$\left.\frac{H_F}{t^m}\right|_{t=0} \sim |\Sigma_{\mathfrak{p}^*}(F, W^*)_{/\,\mathrm{div}}| \cdot \mathcal{R}_{F,\mathfrak{p}^*},$$

as claimed. □

6. Restricted Selmer groups over K

In this section we shall analyse various properties of restricted Selmer groups over K. The main tool for doing this is the Poitou-Tate exact sequence (see e.g. [5, Theorem 1.5] or [11, Proposition 4.1.1]).

We write S_F for the set of places of F lying above p, and G_{F,S_F} for the Galois group over F of the maximal abelian extension of F that is unramified away from all places in S_F.

Proposition 6.1. *There are isomorphisms*

$$\check{\mathrm{Sel}}_{\mathrm{str}}(F, T^*) \simeq H^2(G_{F,S_F}, W)^\wedge, \qquad \check{\mathrm{Sel}}_{\mathrm{str}}(F, T) \simeq H^2(G_{F,S_F}, W^*)^\wedge.$$

Proof. The middle of the Poitou-Tate exact sequence yields

$$0 \to \mathrm{Sel}_{\mathrm{str}}(F, E_{\pi^{*n}})^\wedge \to H^2(G_{F,S_F}, E_{\pi^n}) \to \bigoplus_{v \in S_F} H^2(F_v, E_{\pi^n}).$$

Dualising, and using the fact that, via Tate local duality, we have $H^2(F_v, E_{\pi^n})^\wedge \simeq H^0(F_v, E_{\pi^{*n}})$ for each place v of F gives

$$\bigoplus_{v \in S_F} H^0(F_v, E_{\pi^{*n}}) \to H^2(G_{F,S_F}, E_{\pi^n})^\wedge \to \mathrm{Sel}_{\mathrm{str}}(F, E_{\pi^{*n}}) \to 0.$$

By passing to limits we obtain

$$\bigoplus_{v \in S_F} H^0(F_v, T^*) \to H^2(G_{F,S_F}, W)^\wedge \to \check{\mathrm{Sel}}_{\mathrm{str}}(F, T^*) \to 0,$$

and this establishes the first isomorphism, since the first term of this last sequence is equal to zero.

The second isomorphism may be proved in a similar manner. □

Recall that $r = \mathrm{rk}_{O_K}(E(K))$.

Proposition 6.2. *Suppose that $r \geq 1$. Then*

$$\begin{aligned}\mathrm{rk}_{O_{K,\mathfrak{p}^*}}(\check{\mathrm{Sel}}_{\mathrm{str}}(K, T^*)) &= \mathrm{rk}_{O_{K,\mathfrak{p}^*}}(\check{\mathrm{Sel}}_{\mathrm{str}(\mathfrak{p}^*)}(K, T^*)) \\ &= \mathrm{rk}_{O_{K,\mathfrak{p}^*}}(\check{\mathrm{Sel}}(K, T^*)) - 1.\end{aligned}$$

Proof. Since $r \geq 1$, the image of the localisation map

$$\mathrm{Sel}(K, T^*) \to E(K_{\mathfrak{p}^*}) \otimes O_{K,\mathfrak{p}^*}$$

is infinite. The result now follows from the fact that

$$\mathrm{rk}_{O_{K,\mathfrak{p}^*}}[E(K_{\mathfrak{p}^*}) \otimes O_{K,\mathfrak{p}^*}] = \mathrm{rk}_{O_{K,\mathfrak{p}^*}} \left[\prod_{v|p} E(K_v) \otimes O_{K,\mathfrak{p}^*} \right] = 1.$$

□

Lemma 6.3. *(a) The cohomology group $H^1_f(K_{\mathfrak{p}^*}, T)$ is finite, and*

$$|H^1_f(K_{\mathfrak{p}^*}, T)| \sim |\tilde{E}_{\mathfrak{p}^*}(k_{\mathfrak{p}^*})| \sim 1 - \psi(\mathfrak{p}^*)$$

in $\mathbf{Z}_p$.

(b) We have

$$H^1_f(K_{\mathfrak{p}^*}, T) = H^1(K_{\mathfrak{p}^*}, T)_{\mathrm{tors}},$$

and $H^1(K_{\mathfrak{p}^*}, T)/H^1_f(K_{\mathfrak{p}^*}, T)$ is $O_{K,\mathfrak{p}^*}$-free of rank one.

Proof. Part (a) follows directly from [4, Lemma 1].

To prove part (b), we observe that, via Tate local duality, the dual of $H^1(K_{\mathfrak{p}^*}, T)/H^1_f(K_{\mathfrak{p}^*}, T)$ is equal to $E(K_{\mathfrak{p}^*}) \otimes D_{\mathfrak{p}^*}$, and this last group is divisible of $O_{K,\mathfrak{p}^*}$-corank one. □

Proposition 6.4. *(a) Suppose that $r \geq 1$. Then*

$$\mathrm{rk}_{O_{K,\mathfrak{p}^*}}(\check{\mathrm{Sel}}_{\mathrm{rel}}(K, T^*)) = \mathrm{rk}_{O_{K,\mathfrak{p}^*}}(\check{\mathrm{Sel}}(K, T^*)),$$

and

$$[\check{\mathrm{Sel}}_{\mathrm{rel}}(K, T^*) : \check{\mathrm{Sel}}(K, T^*)] \sim |\tilde{E}_{\mathfrak{p}^*}(k_{\mathfrak{p}^*})|.$$

(b) Suppose that $r = 0$. Then

$$\mathrm{rk}_{O_{K,\mathfrak{p}^*}}(\check{\mathrm{Sel}}_{\mathrm{rel}}(K, T^*)) = 1.$$

Proof. The Poitou-Tate exact sequence yields

$$0 \to \check{\mathrm{Sel}}(K, T^*) \to \check{\mathrm{Sel}}_{\mathrm{rel}}(K, T^*) \xrightarrow{\alpha} \bigoplus_{v|p} \frac{H^1(K_v, T^*)}{H^1_f(K_v, T^*)} \to \mathrm{Sel}(K, W)^{\wedge}. \tag{6.1}$$

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

$$\mathrm{Sel}(K, W) \to \bigoplus_{v|p} H^1_f(K_v, W),$$

and so has $O_{K,\mathfrak{p}^*}$-rank one if $r \geq 1$ and rank zero if $r = 0$. As

$$\mathrm{rk}_{O_{K,\mathfrak{p}^*}}[\oplus_{v|p}(H^1(K_v, T^*)/H^1_f(K_v, T^*))] = 1,$$

we therefore deduce that $\mathrm{rk}_{O_{K,\mathfrak{p}^*}}(\check{\mathrm{Sel}}_{\mathrm{rel}}(K, T^*))$ is equal to $\mathrm{rk}_{O_{K,\mathfrak{p}^*}}(\check{\mathrm{Sel}}(K, T^*))$ if $r \geq 1$, and is equal to one if $r = 0$. In particular, we have that $\check{\mathrm{Sel}}_{\mathrm{rel}}(K, T^*)/\check{\mathrm{Sel}}(K, T^*)$ is finite if $r \geq 1$.

Now suppose that $r \geq 1$. As $H^1(K_{\mathfrak{p}}, T^*)/H^1_f(K_{\mathfrak{p}}, T^*)$ is $O_{K,\mathfrak{p}^*}$-free of rank one (Lemma 6.3(b)) and $\check{\mathrm{Sel}}_{\mathrm{rel}}(K, T^*)/\check{\mathrm{Sel}}(K, T^*)$ is finite, (6.1) implies that there is an exact sequence

$$0 \to \frac{\check{\mathrm{Sel}}_{\mathrm{rel}}(K, T^*)}{\check{\mathrm{Sel}}(K, T^*)} \to \frac{H^1(K_{\mathfrak{p}^*}, T^*)}{H^1_f(K_{\mathfrak{p}^*}, T^*)} \xrightarrow{\alpha'} \mathrm{Sel}(K, W)^{\wedge}.$$

Since $E(K_{\mathfrak{p}^*}) \otimes D_{\mathfrak{p}} = 0$, it follows that α' is the zero map. The dual of $H^1(K_{\mathfrak{p}^*}, T^*)/H^1_f(K_{\mathfrak{p}^*}, T^*)$ is isomorphic to $H^1_f(K_{\mathfrak{p}^*}, T)$, and Lemma 6.3(a) implies that

$$|H^1_f(K_{\mathfrak{p}^*}, T)| \sim |\tilde{E}_{\mathfrak{p}^*}(k_{\mathfrak{p}^*})|.$$

Hence $[\check{\mathrm{Sel}}_{\mathrm{rel}}(K, T^*) : \check{\mathrm{Sel}}(K, T^*)] \sim |\tilde{E}_{\mathfrak{p}^*}(k_{\mathfrak{p}^*})|$, as claimed. □

Proposition 6.5. *Suppose that* $r \geq 1$. *Then*

$$\check{\Sigma}_{\mathfrak{p}^*}(K, T^*) = \check{\mathrm{Sel}}_{\mathrm{str}(\mathfrak{p}^*)}(K, T^*).$$

In particular, we have

$$\mathrm{rk}_{O_{K,\mathfrak{p}^*}}(\check{\Sigma}_{\mathfrak{p}^*}(K, T^*)) = \mathrm{rk}_{O_{K,\mathfrak{p}^*}}(\check{\mathrm{Sel}}(K, T^*)) - 1.$$

Proof. From Proposition 6.4(a), we have

$$\mathrm{rk}_{O_{K,\mathfrak{p}^*}}(\check{\mathrm{Sel}}_{\mathrm{rel}}(K, T^*)) = \mathrm{rk}_{O_{K,\mathfrak{p}^*}}(\check{\mathrm{Sel}}(K, T^*)).$$

This implies that

$$\begin{aligned} \mathrm{rk}_{O_{K,\mathfrak{p}^*}}(\Sigma_{\mathfrak{p}^*}(K, T^*)) &= \mathrm{rk}_{O_{K,\mathfrak{p}^*}}(\check{\mathrm{Sel}}_{\mathrm{str}(\mathfrak{p}^*)}(K, T^*)) \\ &= \mathrm{rk}_{O_{K,\mathfrak{p}^*}}(\check{\mathrm{Sel}}(K, T^*)) - 1. \end{aligned} \tag{6.2}$$

It follows from the definitions of $\check{\Sigma}_{\mathfrak{p}^*}(K, T^*)$ and $\check{\mathrm{Sel}}_{\mathrm{str}(\mathfrak{p}^*)}(K, T^*)$ that we have the following exact sequence

$$0 \to \check{\mathrm{Sel}}_{\mathrm{str}(\mathfrak{p}^*)}(K, T^*) \to \check{\Sigma}_{\mathfrak{p}^*}(K, T^*) \xrightarrow{\beta} \frac{H^1(K_{\mathfrak{p}^*}, T^*)}{H^1_f(K_{\mathfrak{p}}, T^*)} \to \mathrm{Coker}(\beta) \to 0,$$

where β is induced by the obvious localisation map. From (6.2), we see that $\check{\Sigma}_{\mathfrak{p}^*}(K, T^*)/\check{\mathrm{Sel}}_{\mathrm{str}(\mathfrak{p}^*)}(K, T^*)$ is finite. Hence, as $H^1(K_{\mathfrak{p}}, T^*)/H^1_f(K_{\mathfrak{p}}, T^*)$ is $O_{K,\mathfrak{p}^*}$-free of rank one (see Lemma 6.3(b)), it follows that β is the zero map. This implies that

$$\check{\Sigma}_{\mathfrak{p}^*}(K, T^*) = \check{\mathrm{Sel}}_{\mathrm{str}(\mathfrak{p}^*)}(K, T^*)$$

as claimed.

The final assertion of the Proposition is a direct consequence of Proposition 6.2. □

Remark 6.6. Suppose that $r \geq 1$. Then it follows from Proposition 6.5, together with the definition of $[\,,\,]_{K,\mathfrak{p}^*}$ that the pairing $[\,,\,]_{K,\mathfrak{p}^*}$ is simply the restriction of Perrin-Riou's algebraic p-adic height pairing $\{\,,\,\}_{K,\mathfrak{p}^*}$ to $\check{\mathrm{Sel}}_{\mathrm{str}(\mathfrak{p}^*)}(K,T^*) \times \check{\mathrm{Sel}}_{\mathrm{str}(\mathfrak{p})}(K,T)$. Hence, if $r \geq 1$ and $\{\,,\,\}_{K,\mathfrak{p}^*}$ is non-degenerate, then so is $[\,,\,]_{K,\mathfrak{p}^*}$. We conjecture that the pairing $[\,,\,]_{K,\mathfrak{p}^*}$ is also non-degenerate when $r = 0$. □

Proposition 6.7. *Suppose that $r = 0$. Then*

$$\mathrm{rk}_{O_{K,\mathfrak{p}^*}}(\check{\Sigma}_{\mathfrak{p}^*}(K,T^*)) = 1.$$

Proof. We have an injection

$$0 \to \check{\Sigma}_{\mathfrak{p}^*}(K,T^*) \to \check{\mathrm{Sel}}_{\mathrm{rel}}(K,T^*),$$

and we know that $\mathrm{rk}_{O_{K,\mathfrak{p}^*}}(\check{\mathrm{Sel}}_{\mathrm{rel}}(K,T^*)) = 1$ (Proposition 6.4(b)). Hence $\mathrm{rk}_{O_{K,\mathfrak{p}^*}}(\check{\Sigma}_{\mathfrak{p}^*}(K,T^*))$ is either zero or one.

Suppose that $\mathrm{rk}_{O_{K,\mathfrak{p}^*}}(\check{\Sigma}_{\mathfrak{p}^*}(K,T^*)) = 0$. Then the proof of Theorem 5.2 shows that the characteristic power series $H_K \in \Lambda(K_\infty^*)$ of $X_{\mathfrak{p}^*}(K,W^*)$ does not vanish at $t = 0$. This implies that $\mathrm{ord}_{s=1} L_{\mathfrak{p}}^*(s) = 0$ (see (2.6)). On the other hand, it follows from the functional equation satisfied by the two-variable p-adic L-function $\mathcal{L}_{\mathfrak{p}}$ (see [6, Chapter II, §6]) that the orders of the zeros at $s = 1$ of $L_{\mathfrak{p}}(s)$ and $L_{\mathfrak{p}^*}(s)$ have opposite parity. Since $r = 0$, the order of Ш(K) is known to be finite (see [13]), and so

$$\mathrm{ord}_{s=1} L_{\mathfrak{p}}(s) = \mathrm{rk}_{O_{K,\mathfrak{p}^*}}(\mathrm{Sel}(K,T^*)) = 0.$$

This implies that $\mathrm{ord}_{s=1} L_{\mathfrak{p}}^*(s) \geq 1$, which is a contradiction.

It therefore follows that $\mathrm{rk}_{O_{K,\mathfrak{p}^*}}(\check{\Sigma}_{\mathfrak{p}^*}(K,T^*)) = 1$ as claimed. □

Corollary 6.8. *Assume that $[\,,\,]_{K,\mathfrak{p}^*}$ is non-degenerate.*

(a) If $r \geq 1$ and Ш$(K)(\mathfrak{p}^*)$ is finite, then

$$\mathrm{ord}_{s=1} L_{\mathfrak{p}}^*(s) = r - 1.$$

(b) If $r = 0$, then

$$\mathrm{ord}_{s=1} L_{\mathfrak{p}}^*(s) = 1.$$

Proof. This follows directly from Propositions 6.5 and 6.7, and (2.6). □

Remark 6.9. Corollary 6.8(b) confirms the expectation expressed in [15, Remark on p.74] (see also [14, §11, Remarks(2)]). It would be interesting to know if there is any way of showing that $\mathrm{rk}_{O_{K,\mathfrak{p}^*}}(\Sigma_{\mathfrak{p}^*}(K,T^*)) = 1$ when $r = 0$ *without* appealing to the functional equation satisfied by $\mathcal{L}_{\mathfrak{p}}$. □

Proposition 6.10. *(a) Suppose that* $r \geq 1$*, and assume that* $\text{Ш}(K)(\mathfrak{p}^*)$ *is finite. Then* $\text{Ш}_{\mathrm{rel}(\mathfrak{p})}(K)(\mathfrak{p}^*)$ *is also finite, and we have*

$$|\text{Ш}_{\mathrm{rel}(\mathfrak{p})}(K)(\mathfrak{p}^*)| = |\text{Ш}(K)(\mathfrak{p})| \cdot [E(K_{\mathfrak{p}}) \otimes O_{K,\mathfrak{p}} : \mathrm{loc}_{\mathfrak{p}}(\mathrm{Sel}(K,T))].$$

(b) Suppose that $r = 0$*. Then* $\text{Ш}_{\mathrm{rel}(\mathfrak{p})}(K)(\mathfrak{p}^*)$ *has* $O_{K,\mathfrak{p}^*}$*-corank one.*

Proof. (a) For each $n \geq 1$, we define B_n via exactness of the sequence

$$0 \to \text{Ш}(K)_{\pi^{*n}} \to H^1(K,E)_{\pi^{*n}} \to \prod_v H^1(K_v,E)_{\pi^{*n}} \to B_n \to 0.$$

Then there exists a map $h_n : H^1(K_{\mathfrak{p}},E)_{\pi^{*n}} \to B_n$, and the sequence

$$0 \to \text{Ш}(K)_{\pi^{*n}} \to \text{Ш}_{\mathrm{rel}(\mathfrak{p})}(K)_{\pi^{*n}} \to H^1(K_{\mathfrak{p}},E)_{\pi^{*n}} \xrightarrow{h_n} B_n \tag{6.3}$$

is exact. Passing to direct limits over n in (6.3) yields the sequence

$$0 \to \text{Ш}(K)(\mathfrak{p}^*) \to \text{Ш}_{\mathrm{rel}(\mathfrak{p})}(K)(\mathfrak{p}^*) \to H^1(K_{\mathfrak{p}},E)(\mathfrak{p}^*) \xrightarrow{\varinjlim h_n} \varinjlim B_n. \tag{6.4}$$

It follows from a theorem of Cassels (see [3, p.198]) that the dual of B_n is isomorphic to $\mathrm{Sel}(K, E_{\pi^n})$. Tate local duality implies that the dual of $H^1(K_{\mathfrak{p}},E)_{\pi^{*n}}$ is isomorphic to $E(K_{\mathfrak{p}})/\pi^n E(K_{\mathfrak{p}})$ and that the kernel of $\varinjlim h_n$ is isomorphic to the dual of the cokernel of the localisation map

$$\mathrm{loc}_{\mathfrak{p}} : \check{\mathrm{Sel}}(K,T) \to E(K_{\mathfrak{p}}) \otimes O_{K,\mathfrak{p}}.$$

If $r \geq 1$, then this cokernel is finite, and we therefore deduce that

$$[\text{Ш}_{\mathrm{rel}(\mathfrak{p})}(K)(\mathfrak{p}^*) : \text{Ш}(K)(\mathfrak{p}^*)] = [E(K_{\mathfrak{p}}) \otimes O_{K,\mathfrak{p}} : \mathrm{loc}_{\mathfrak{p}}(\check{\mathrm{Sel}}(K,T))].$$

Hence, we have

$$|\text{Ш}_{\mathrm{rel}(\mathfrak{p})}(K)(\mathfrak{p}^*)| = |\text{Ш}(K)(\mathfrak{p}^*)| \cdot [E(K_{\mathfrak{p}}) \otimes O_{K,\mathfrak{p}} : \mathrm{loc}_{\mathfrak{p}}(\check{\mathrm{Sel}}(K,T))]$$

as claimed.

(b) If $r = 0$, then $\check{\mathrm{Sel}}(K,T)$ is trivial, because $\text{Ш}(K)$ is known to be finite, and $E(K)(\mathfrak{p}) = 0$. This implies that $\mathrm{Coker}(\mathrm{loc}_{\mathfrak{p}}) = E(K_{\mathfrak{p}}) \otimes O_{K,\mathfrak{p}}$ is $O_{K,\mathfrak{p}}$-free of rank one. It now follows from (6.4) that $\text{Ш}_{\mathrm{rel}(\mathfrak{p})}(K)(\mathfrak{p}^*)$ has $O_{K,\mathfrak{p}^*}$-corank one. □

Proposition 6.11. *Suppose that* $r \geq 1$*, and assume that* $\text{Ш}(K)(\mathfrak{p}^*)$ *is finite. Then*

$$|\Sigma_{\mathfrak{p}^*}(K,W^*)_{/\,\mathrm{div}}| = |\text{Ш}_{\mathrm{rel}(\mathfrak{p})}(K)(\mathfrak{p}^*)| \cdot [E(K_{\mathfrak{p}^*}) \otimes_{O_K} O_{K,\mathfrak{p}^*} : \mathrm{loc}_{\mathfrak{p}^*}(\check{\mathrm{Sel}}(K,T^*))].$$

Proof. Let $y_1, \dots, y_{r-1}$ be an $O_{K,\mathfrak{p}^*}$-basis of $E_{1,\mathfrak{p}^*}(K)$, and extend it to an $O_{K,\mathfrak{p}^*}$-basis $y_1, \dots, y_{r-1}, y_{\mathfrak{p}^*}$ of $E(K) \otimes_{O_K} O_{K,\mathfrak{p}^*}$. There is an exact sequence

$$0 \to O_{K,\mathfrak{p}^*} \cdot y_{\mathfrak{p}^*} \to E(K_{\mathfrak{p}^*}) \otimes_{O_K} O_{K,\mathfrak{p}^*} \to U \to 0,$$

with

$$\begin{aligned} |U| &= [E(K_{\mathfrak{p}^*}) \otimes_{O_K} O_{K,\mathfrak{p}^*} : \mathrm{loc}_{\mathfrak{p}^*}(E(K) \otimes_{O_K} O_{K,\mathfrak{p}^*})] \\ &= [E(K_{\mathfrak{p}^*}) \otimes_{O_K} O_{K,\mathfrak{p}^*} : \mathrm{loc}_{\mathfrak{p}^*}(\check{\mathrm{S}}\mathrm{el}(K, T^*))]. \end{aligned}$$

Tensoring this sequence with $D_{\mathfrak{p}^*}$ yields an exact sequence

$$0 \to V \to (O_{K,\mathfrak{p}^*} \cdot y_{\mathfrak{p}^*}) \otimes_{O_K} D_{\mathfrak{p}^*} \to E(K_{\mathfrak{p}^*}) \otimes_{O_K} D_{\mathfrak{p}^*} \to 0,$$

with $|U| = |V|$. As

$$E(K) \otimes_{O_K} O_{K,\mathfrak{p}^*} \simeq E_{1,\mathfrak{p}^*}(K) \oplus (O_{K,\mathfrak{p}^*} \cdot y_{\mathfrak{p}^*}),$$

it follows that the kernel of the localisation map

$$E(K) \otimes_{O_K} D_{\mathfrak{p}^*} \to E(K_{\mathfrak{p}^*}) \otimes_{O_K} D_{\mathfrak{p}^*}$$

is isomorphic to $(E_{1,\mathfrak{p}^*}(K) \otimes_{O_K} D_{\mathfrak{p}^*}) \oplus V$.

Define

$$Ш(K)_{\mathrm{rel}} := \mathrm{Ker}\left[H^1(K, E) \to \prod_{v \nmid p} H^1(K_v, E) \right];$$

then we have an exact sequence

$$0 \to E(K) \otimes D_{\mathfrak{p}^*} \to \mathrm{Sel}_{\mathrm{rel}}(K, W^*) \to Ш_{\mathrm{rel}}(K)(\mathfrak{p}^*) \to 0.$$

Now consider the following commutative diagram, in which the vertical arrows are the obvious localisation maps:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K) \otimes D_{\mathfrak{p}^*} & \longrightarrow & \mathrm{Sel}_{\mathrm{rel}}(K, W^*) & \longrightarrow & Ш_{\mathrm{rel}}(K)(\mathfrak{p}^*) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & E(K_{\mathfrak{p}^*}) \otimes D_{\mathfrak{p}^*} & \longrightarrow & H^1(K_{\mathfrak{p}^*}, W^*) & \longrightarrow & H^1(K_{\mathfrak{p}^*}, E)(\mathfrak{p}^*) & \longrightarrow & 0 \end{array}$$

Applying the Snake Lemma to this diagram yields the exact sequence

$$0 \to (E_{1,\mathfrak{p}^*}(K) \otimes D_{\mathfrak{p}^*}) \oplus V \to \Sigma_{\mathfrak{p}^*}(K, W^*) \to Ш_{\mathrm{rel}(\mathfrak{p})}(K)(\mathfrak{p}^*) \to 0.$$

As $Ш_{\mathrm{rel}}(K)(\mathfrak{p}^*)$ is finite (see Proposition 6.10) and $E_{1,\mathfrak{p}^*}(K) \otimes_{O_K} D_{\mathfrak{p}^*}$ is divisible, it follows that

$$\begin{aligned} \Sigma_{\mathfrak{p}^*}(K, W^*)_{/\,\mathrm{div}} &= |Ш_{\mathrm{rel}}(K)(\mathfrak{p}^*)| \cdot |V| \\ &= |Ш_{\mathrm{rel}(\mathfrak{p})}(K)(\mathfrak{p}^*)| \cdot [E(K_{\mathfrak{p}^*}) \otimes_{O_K} O_{K,\mathfrak{p}^*} : \mathrm{loc}_{\mathfrak{p}^*}(\check{\mathrm{S}}\mathrm{el}(K, T^*))], \end{aligned}$$

as asserted. ∎

7. Proof of Theorem A

Proposition 7.1. *Suppose that $r = 0$. Then*

$$|\Sigma_{\mathfrak{p}^*}(K, W^*)_{/\,\mathrm{div}}| \sim (1 - \psi(\mathfrak{p}^*)) \cdot \frac{|Ш(K)_{\mathrm{rel}(\mathfrak{p})}(\mathfrak{p}^*)_{/\,\mathrm{div}}|}{[H^1(K_{\mathfrak{p}^*}, T) : \mathrm{loc}_{\mathfrak{p}^*}(\Sigma_{\mathfrak{p}}(K, T))]}.$$

Proof. Consider the following diagram in which all columns are exact and f_1, f_2 are the obvious localisation maps:

$$\begin{array}{ccccccccc}
 & & 0 & \longrightarrow & \Sigma_{\mathfrak{p}^*}(K, W^*) & \longrightarrow & Ш_{\mathrm{rel}(\mathfrak{p})}(K)(\mathfrak{p}^*) & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E(K) \otimes D_{\mathfrak{p}^*} = 0 & \longrightarrow & \mathrm{Sel}_{\mathrm{rel}}(K, W^*) & \longrightarrow & Ш_{\mathrm{rel}}(K)(\mathfrak{p}^*) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & \\
0 & \longrightarrow & E(K_{\mathfrak{p}^*}) \otimes D_{\mathfrak{p}^*} & \longrightarrow & H^1(K_{\mathfrak{p}^*}, W^*) & \longrightarrow & H^1(K_{\mathfrak{p}^*}, E)(\mathfrak{p}^*) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & E(K_{\mathfrak{p}^*}) \otimes D_{\mathfrak{p}^*} & \longrightarrow & \mathrm{Coker}(f_1) & \longrightarrow & \mathrm{Coker}(f_2) & &
\end{array}$$

Applying the Snake Lemma to this diagram yields an exact sequence

$$0 \to \Sigma_{\mathfrak{p}^*}(K, W^*) \to Ш_{\mathrm{rel}(\mathfrak{p})}(K)(\mathfrak{p}^*) \to E(K_{\mathfrak{p}^*}) \otimes D_{\mathfrak{p}^*} \to \mathrm{Coker}(f_1) \to \mathrm{Coker}(f_2) \to 0. \quad (7.1)$$

Let us first determine $\mathrm{Coker}(f_1)$. The Poitou-Tate exact sequence gives

$$0 \to \Sigma_{\mathfrak{p}^*}(K, W^*) \to \mathrm{Sel}_{\mathrm{rel}}(K, W^*) \xrightarrow{f_1} H^1(K_{\mathfrak{p}^*}, W^*) \to \check{\Sigma}_{\mathfrak{p}}(K, T)^{\wedge} \to H^2(G_{K,S_K}, W^*),$$

where G_{K,S_K} denotes the Galois group over K of the maximal extension of K that is unramified away from p. Since $r = 0$, Propositions 6.1 and 6.2 imply that $H^2(G_{K,S_K}, W^*) = 0$, and so we have

$$\mathrm{Coker}(f_1) \simeq \check{\Sigma}_{\mathfrak{p}}(K, T)^{\wedge}. \quad (7.2)$$

In particular, it follows from Lemma 3.6 and Proposition 6.7 that $\mathrm{Coker}(f_1)$ is divisible of $O_{K,\mathfrak{p}^*}$-corank one.

In order to determine $\mathrm{Coker}(f_2)$, we observe that $E(K_{\mathfrak{p}^*}) \otimes D_{\mathfrak{p}^*}$ is divisible of $O_{K,\mathfrak{p}^*}$-corank one, and the kernel of the map

$$E(K_{\mathfrak{p}^*}) \otimes D_{\mathfrak{p}^*} \to \mathrm{Coker}(f_1)$$

in (7.1) is isomorphic to $Ш_{\mathrm{rel}(\mathfrak{p})}(K)(\mathfrak{p}^*)/\Sigma_{\mathfrak{p}^*}(K, W^*)$. This last group is finite, because both $Ш_{\mathrm{rel}(\mathfrak{p})}(K)(\mathfrak{p}^*)$ and $\Sigma_{\mathfrak{p}^*}(K, W^*)$ have $O_{K,\mathfrak{p}^*}$-corank one (see Propositions 6.10(b) and 6.7). It therefore follows that $\mathrm{Coker}(f_2) = 0$.

From (7.1) and (7.2), we obtain the sequence

$$0 \to \frac{Ш_{\mathrm{rel}(\mathfrak{p})}(K)(\mathfrak{p}^*)}{\Sigma_{\mathfrak{p}^*}(K, W^*)} \to E(K_{\mathfrak{p}^*}) \otimes D_{\mathfrak{p}^*} \to \check{\Sigma}_{\mathfrak{p}}(K, T)^{\wedge} \to 0. \tag{7.3}$$

Dualising this sequence yields

$$0 \to \check{\Sigma}_{\mathfrak{p}}(K, T) \to \frac{H^1(K_{\mathfrak{p}^*}, T)}{H^1_f(K_{\mathfrak{p}^*}, T)} \to \left[\frac{Ш_{\mathrm{rel}(\mathfrak{p})}(K)(\mathfrak{p}^*)}{\Sigma_{\mathfrak{p}^*}(K, W^*)}\right]^{\wedge} \to 0.$$

We therefore have

$$\begin{aligned}\left|\left[\frac{Ш_{\mathrm{rel}(\mathfrak{p})}(K)(\mathfrak{p}^*)}{\Sigma_{\mathfrak{p}^*}(K, W^*)}\right]^{\wedge}\right| &= \left|\frac{Ш_{\mathrm{rel}(\mathfrak{p})}(K)(\mathfrak{p}^*)}{\Sigma_{\mathfrak{p}^*}(K, W^*)}\right| \\ &= \left|\frac{Ш_{\mathrm{rel}(\mathfrak{p})}(K)(\mathfrak{p}^*)_{/\,\mathrm{div}}}{\Sigma_{\mathfrak{p}^*}(K, W^*)_{/\,\mathrm{div}}}\right| \\ &= [H^1(K_{\mathfrak{p}^*}, T) : \mathrm{loc}_{\mathfrak{p}^*}(\check{\Sigma}_{\mathfrak{p}}(K, T))] \cdot |H^1_f(K_{\mathfrak{p}^*}, T)|^{-1},\end{aligned}$$

which in turn implies that

$$|\Sigma_{\mathfrak{p}^*}(K, W^*)_{/\,\mathrm{div}}| = \frac{|Ш_{\mathrm{rel}(\mathfrak{p})}(K)(\mathfrak{p}^*)_{/\,\mathrm{div}}|}{[H^1(K_{\mathfrak{p}^*}, T) : \mathrm{loc}_{\mathfrak{p}^*}(\check{\Sigma}_{\mathfrak{p}}(K, T))]} \cdot |H^1_f(K_{\mathfrak{p}^*}, T)|.$$

Since

$$|H^1_f(K_{\mathfrak{p}^*}, T)| \sim 1 - \psi(\mathfrak{p}^*)$$

(see Lemma 6.3), we finally obtain

$$|\Sigma_{\mathfrak{p}^*}(K, W^*)_{/\,\mathrm{div}}| \sim (1 - \psi(\mathfrak{p}^*)) \cdot \frac{|Ш(K)_{\mathrm{rel}(\mathfrak{p})}(\mathfrak{p}^*)_{/\,\mathrm{div}}|}{[H^1(K_{\mathfrak{p}^*}, T) : \mathrm{loc}_{\mathfrak{p}^*}(\Sigma_{\mathfrak{p}}(K, T))]},$$

as claimed. □

Proof of Theorem A. We first note that, as $[\,,\,]_{K,\mathfrak{p}^*}$ is non-degenerate (by hypothesis), we have $\mathrm{ord}_{s=1} L^*_{\mathfrak{p}}(s) = 1$ (Corollary 6.8(b)). Hence from (5.1), (2.7), Proposition 7.1 and Remark 3.4, we have

$$\begin{aligned}\lim_{s\to 1} \frac{L^*_{\mathfrak{p}}(s)}{s-1} &\sim \log_p(\psi^*(\gamma)) \cdot \left.\frac{H_K}{t}\right|_{t=0} \\ &\sim \log_p(\psi^*(\gamma)) \cdot \left|\Sigma_{\mathfrak{p}^*}(K, W^*)_{/\,\mathrm{div}}\right| \cdot \mathcal{R}_{K,\mathfrak{p}^*} \\ &\sim \log_p(\psi^*(\gamma)) \cdot (1 - \psi(\mathfrak{p}^*) \cdot \frac{|Ш_{\mathrm{rel}(\mathfrak{p})}(K)(\mathfrak{p}^*)_{/\,\mathrm{div}}|}{[H^1(K_{\mathfrak{p}^*}, T) : \mathrm{loc}_{\mathfrak{p}^*}(\Sigma_{\mathfrak{p}}(K, T))]} \cdot \mathcal{R}_{K,\mathfrak{p}^*}.\end{aligned}$$

This completes the proof of Theorem A. □

8. Proof of Theorem B

Suppose now that $r \geq 1$. Then $E(K) \otimes O_{K,\mathfrak{p}^*}$ is a free $O_{K,\mathfrak{p}^*}$-module of rank r. Proposition 6.2 implies that the kernel of the localisation map

$$\mathrm{loc}_{\mathfrak{p}^*} : E(K) \otimes_{O_K} O_{K,\mathfrak{p}^*} \to E(K_{\mathfrak{p}^*}) \otimes O_{K,\mathfrak{p}^*}$$

has $O_{K,\mathfrak{p}^*}$-rank $r-1$. Let $y_1, \ldots, y_{r-1}$ be an $O_{K,\mathfrak{p}^*}$-basis of this kernel, and extend it to an $O_{K,\mathfrak{p}^*}$-basis $y_1, \ldots, y_{r-1}, y_{\mathfrak{p}^*}$ of $E(K) \otimes O_{K,\mathfrak{p}^*}$.

Proposition 8.1. *With the above assumptions and notation, we have*

$$[E(K_{\mathfrak{p}^*}) \otimes_{O_K} O_{K,\mathfrak{p}^*} : \mathrm{loc}_{\mathfrak{p}^*}(E(K) \otimes_{O_K} O_{K,\mathfrak{p}^*})] \sim p^{-1} \log_{E,\mathfrak{p}^*}(y_{\mathfrak{p}^*}),$$

where $\log_{E,\mathfrak{p}^*}$ *denotes the* $\mathfrak{p}^*$*-adic logarithm associated to* E. *Similarly, we also have*

$$[E(K_{\mathfrak{p}}) \otimes_{O_K} O_{K,\mathfrak{p}} : \mathrm{loc}_{\mathfrak{p}}(E(K) \otimes_{O_K} O_{K,\mathfrak{p}})] \sim p^{-1} \log_{E,\mathfrak{p}}(y_{\mathfrak{p}}),$$

when $y_{\mathfrak{p}} \in E(K_{\mathfrak{p}}) \otimes_{O_K} O_{K,\mathfrak{p}}$ *is defined analogously to* $y_{\mathfrak{p}^*}$.

Proof. We give the proof of the first assertion; that of the second is of course essentially identical.

We first observe that, from the definitions, we have

$$[E(K_{\mathfrak{p}^*}) \otimes_{O_K} O_{K,\mathfrak{p}^*} : \mathrm{loc}_{\mathfrak{p}^*}(E(K) \otimes_{O_K} O_{K,\mathfrak{p}^*})] = [E(K_{\mathfrak{p}^*}) \otimes O_{K,\mathfrak{p}^*} : \mathrm{loc}_{\mathfrak{p}^*}(O_{K,\mathfrak{p}^*} \cdot y_{\mathfrak{p}^*})].$$

Let E_0 denote the kernel of reduction modulo $\mathfrak{p}^*$ of E, so we have an exact sequence

$$0 \to E_0(K_{\mathfrak{p}^*}) \to E(K_{\mathfrak{p}^*}) \to \tilde{E}_{\mathfrak{p}^*}(k_{\mathfrak{p}^*}) \to 0.$$

Set

$$Z := O_{K,\mathfrak{p}^*} \cdot y_{\mathfrak{p}^*}, \quad Z_0 := \mathrm{loc}_{\mathfrak{p}^*}(Z) \cap E_0(K_{\mathfrak{p}^*}), \quad C := \mathrm{loc}_{\mathfrak{p}^*}(Z)/Z_0.$$

Write $\lambda_{\mathfrak{p}^*}$ for the restriction of $\mathrm{loc}_{\mathfrak{p}^*}$ to Z. We have the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Z_0 & \longrightarrow & Z & \longrightarrow & C \otimes_{O_K} O_{K,\mathfrak{p}^*} & \longrightarrow & 0 \\ & & \downarrow \rho & & \downarrow \lambda_{\mathfrak{p}^*} & & \downarrow \rho' & & \\ 0 & \longrightarrow & E_0(K^*_{\mathfrak{p}}) \otimes_{O_K} O_{K,\mathfrak{p}^*} & \longrightarrow & E(K_{\mathfrak{p}^*}) \otimes_{O_K} O_{K,\mathfrak{p}^*} & \longrightarrow & \tilde{E}_{\mathfrak{p}^*}(k_{\mathfrak{p}^*}) \otimes_{O_K} O_{K,\mathfrak{p}^*} & \longrightarrow & 0 \end{array}$$

Observe that ρ is injective since $\lambda_{\mathfrak{p}^*}$ is injective, and that $\tilde{E}_{\mathfrak{p}^*}(k_{\mathfrak{p}^*}) \otimes_{O_K} O_{K,\mathfrak{p}^*} = 0$ because $\tilde{E}_{\mathfrak{p}^*}(k_{\mathfrak{p}^*})(p) = \tilde{E}_{\mathfrak{p}^*}(k_{\mathfrak{p}^*})(\mathfrak{p})$ (see e.g. [12, p. 28]). Applying the Snake Lemma to the diagram yields the exact sequence

$$0 \to \mathrm{Ker}(\rho') \to \mathrm{Coker}(\rho) \to \mathrm{Coker}(\lambda_{\mathfrak{p}^*}) \to 0,$$

and so we have

$$|\,\mathrm{Coker}(\lambda_{\mathfrak{p}^*})| = |C \otimes_{O_K} O_{K,\mathfrak{p}^*}|^{-1} \cdot |\,\mathrm{Coker}(\rho)|.$$

Set $k = [Z : Z_0] = |C \otimes O_{K,\mathfrak{p}^*}|$; then $ky_{\mathfrak{p}^*}$ is an $O_{K,\mathfrak{p}^*}$-generator of Z_0. Since there is an isomorphism

$$\log_{E,\mathfrak{p}^*} : E_0(K_{\mathfrak{p}^*}) \xrightarrow{\sim} \mathfrak{p}^* O_{K,\mathfrak{p}^*},$$

it follows that we have

$$|\operatorname{Coker}(\rho)| \sim p^{-1} \log_{E,\mathfrak{p}^*}(ky_{\mathfrak{p}^*}) = kp^{-1} \log_{E,\mathfrak{p}^*}(y_{\mathfrak{p}^*}).$$

Therefore

$$|\operatorname{Coker}(\lambda_{\mathfrak{p}^*})| \sim p^{-1} \log_{E,\mathfrak{p}^*}(y_{\mathfrak{p}^*}),$$

and this establishes the desired result. □

Corollary 8.2. *Suppose that $r \geq 1$ and assume that $Ш(K)(\mathfrak{p}^*)$ is finite. Then*

$$|Ш_{\mathrm{rel}(\mathfrak{p})}(K)(\mathfrak{p}^*)| = p^{-1} \cdot |Ш(K)(\mathfrak{p}^*)| \cdot \log_{E,\mathfrak{p}}(y_{\mathfrak{p}}).$$

Proof. This follows directly from Propositions 6.10(a) and 8.1. □

Proof of Theorem B. By hypothesis, $[\, ,\,]_{K,\mathfrak{p}^*}$ is non-degenerate, $r \geq 1$, and $Ш(K)(p)$ is finite; hence we have that $\operatorname{ord}_{s=1} L^*_{\mathfrak{p}}(s) = r - 1$ (Corollary 6.8(a)). Proposition 6.11 and Corollary 8.2 imply that

$$\begin{aligned} |\Sigma_{\mathfrak{p}^*}(K, W^*)_{/\operatorname{div}}| &= |Ш_{\mathrm{rel}(\mathfrak{p})}(K)(\mathfrak{p}^*)| \cdot [E(K_{\mathfrak{p}^*}) \otimes_{O_K} O_{K,\mathfrak{p}^*} : \operatorname{loc}_{\mathfrak{p}^*}(\check{\operatorname{Sel}}(K, T^*))] \\ &\sim p^{-2} \cdot |Ш(K)(\mathfrak{p}^*)| \cdot \log_{E,\mathfrak{p}^*}(y_{\mathfrak{p}^*}) \cdot \log_{E,\mathfrak{p}}(y_{\mathfrak{p}}). \end{aligned}$$

We therefore deduce from (5.1), (2.7) and Remark 3.4 that

$$\lim_{s\to 1} \frac{L^*_{\mathfrak{p}}(s)}{(s-1)^{r-1}} \sim$$
$$[\log_p(\psi^*(\gamma))]^{r-1} \cdot p^{-2} \cdot |Ш(K)(\mathfrak{p}^*)| \cdot \log_{E,\mathfrak{p}^*}(y_{\mathfrak{p}^*}) \cdot \log_{E,\mathfrak{p}}(y_{\mathfrak{p}}) \cdot \mathcal{R}_{K,\mathfrak{p}^*},$$

as asserted.

This completes the proof of Theorem B. □

9. Canonical elements in restricted Selmer groups

The goal of this section is to explain how the methods of [14] may be used to produce an exact formula for $\lim_{s\to 1} L^*_{\mathfrak{p}}(s)/(s-1)$ when $r = 0$ (see Theorem 9.5 below). The arguments involved are quite similar to those of [14], and so, in what follows, we assume that the reader has a copy of [14] and is willing to refer to it from time to time for some of the details we omit.

We begin by introducing the following notation (some of which differs from that of [14]):

$$U_{n,\mathfrak{p}} := \text{units in } \mathcal{K}_{n,\mathfrak{p}} \text{ congruent to 1 modulo } \mathfrak{p};$$
$$U_{n,\mathfrak{p}^*} := \text{units in } \mathcal{K}_{n,\mathfrak{p}^*} \text{ congruent to 1 modulo } \mathfrak{p}^*;$$
$$U_{\infty,\mathfrak{p}} := \varprojlim U_{n,\mathfrak{p}}, \quad U_{\infty,\mathfrak{p}^*} := \varprojlim U_{n,\mathfrak{p}^*};$$
$$U^*_{n,\mathfrak{p}} := \text{units in } \mathcal{K}^*_{n,\mathfrak{p}} \text{ congruent to 1 modulo } \mathfrak{p};$$
$$U^*_{n,\mathfrak{p}^*} := \text{units in } \mathcal{K}^*_{n,\mathfrak{p}^*} \text{ congruent to 1 modulo } \mathfrak{p}^*;$$
$$U^*_{\infty,\mathfrak{p}} := \varprojlim U^*_{n,\mathfrak{p}}, \quad U^*_{\infty,\mathfrak{p}^*} := \varprojlim U_{n,\mathfrak{p}^*},$$

where all inverse limits are taken with respect to norm maps. We also set

$$\mathcal{E}_n := \text{global units of } \mathcal{K}_n, \quad \mathcal{E}^*_n := \text{global units of } \mathcal{K}^*_n;$$
$$\overline{\mathcal{E}}_n := \text{the closure of the projection of } \mathcal{E}_n \text{ into } U_{n,\mathfrak{p}};$$
$$\overline{\mathcal{E}}^*_n := \text{the closure of the projection of } \mathcal{E}^*_n \text{ into } U^*_{n,\mathfrak{p}^*};$$
$$\overline{\mathcal{E}}_\infty := \varprojlim \overline{\mathcal{E}}_n, \quad \overline{\mathcal{E}}^*_\infty := \varprojlim \overline{\mathcal{E}}^*_n.$$

Remark 9.1. Note that since the strong Leopoldt conjecture holds for all abelian extensions of K (see [2]), we have that

$$\overline{\mathcal{E}}_n \simeq \overline{\mathcal{E}}_n \otimes_{\mathbf{Z}} \mathbf{Z}_p, \quad \overline{\mathcal{E}}^*_n \simeq \overline{\mathcal{E}}^*_n \otimes_{\mathbf{Z}} \mathbf{Z}_p,$$

and so we may also view $\overline{\mathcal{E}}_\infty$ as being a submodule of $U_{\infty,\mathfrak{p}^*}$ and $\overline{\mathcal{E}}^*_\infty$ as being a submodule of $U^*_{\infty,\mathfrak{p}}$. We shall do this without further comment several times in what follows. □

Proposition 9.2. *There are natural injections*

$$\rho : \mathrm{Hom}(T^*, (U^*_{\infty,\mathfrak{p}} \otimes \mathbf{Q})/\overline{\mathcal{E}}^*_\infty)^{\mathrm{Gal}(\mathcal{K}^*_\infty/K)} \hookrightarrow \check{\Sigma}_{\mathfrak{p}}(K,T),$$
$$\rho^* : \mathrm{Hom}(T, (U_{\infty,\mathfrak{p}} \otimes \mathbf{Q})/\overline{\mathcal{E}}_\infty)^{\mathrm{Gal}(\mathcal{K}_\infty/K)} \hookrightarrow \check{\Sigma}_{\mathfrak{p}^*}(K,T^*)$$

Proof. The proof of this result is essentially the same, *mutatis mutandis*, as that of [14, Proposition 2.4]. The map ρ is defined as follows.

For any $f \in \mathrm{Hom}(T^*, (U^*_{\infty,\mathfrak{p}} \otimes \mathbf{Q})/\overline{\mathcal{E}}^*_\infty)^{\mathrm{Gal}(\mathcal{K}^*_\infty/K)}$ and any integer $n \geq 1$, we define $f_n \in \mathrm{Hom}(E_{\pi^n}, \mathcal{E}^*_n/\mathcal{E}^{*p^n}_n)^{\mathrm{Gal}(\mathcal{K}_\infty/K)}$ to be the image of f under the following composition of maps:

$$\begin{aligned}\mathrm{Hom}(T^*, (U^*_{\infty,\mathfrak{p}} \otimes \mathbf{Q})/\overline{\mathcal{E}}^*_\infty)^{\mathrm{Gal}(\mathcal{K}^*_\infty/K)} &\to \mathrm{Hom}(T^*, (U^*_{n,\mathfrak{p}} \otimes \mathbf{Q})/\overline{\mathcal{E}}^*_n)^{\mathrm{Gal}(\mathcal{K}^*_\infty/K)} \\ &\to \mathrm{Hom}(E_{\pi^n}, \mathcal{E}^*_n/\mathcal{E}^{*p^n}_n)^{\mathrm{Gal}(\mathcal{K}^*_\infty/K)},\end{aligned}$$

where the first arrow is the map induced by the natural projection $U^*_{\infty,\mathfrak{p}} \to U^*_{n,\mathfrak{p}}$, and the second arrow is induced by raising to the p^n-th power in $U^*_{n,\mathfrak{p}}$.

Recall that, for each $n \geq 1$, there is an isomorphism

$$\rho_n : H^1(K, E_{\pi^n}) \xrightarrow{\sim} \operatorname{Hom}(E_{\pi^{*n}}, \mathcal{K}_n^{*\times}/\mathcal{K}_n^{*\times p^n})^{\operatorname{Gal}(\mathcal{K}_n^*/K)}$$

(see e.g. [14, Lemma 2.1] or [10, Lemme 12]). We define

$$\rho(f) := [(p-1)(\pi^*)^{2n}\rho_n^{-1}(f_n)] \in \varprojlim_n H^1(K, E_{\pi^n}).$$

It is not hard to check from the definition that ρ is injective. It follows from Theorem 3.1, Proposition 3.2, and Corollary 3.3 that $\rho_n^{-1}(f_n) \in \Sigma_{\mathfrak{p}}(K, E_{\pi^n})$ if and only if the restriction of $\rho_n^{-1}(f_n)$ to $H^1(\mathfrak{K}_\infty, E_{\pi^n})$ is unramified outside $\mathfrak{p}^*$. It may be shown via an argument very similar to that given in [14, Lemmas 2.1 and 2.3] that this in fact the case. □

We shall now explain how elliptic units may be used (following [14]) to construct canonical elements

$$s_{\mathfrak{p}}^{(1)} \in \check{\Sigma}_{\mathfrak{p}}(K, T), \quad s_{\mathfrak{p}^*}^{(1)} \in \check{\Sigma}_{\mathfrak{p}^*}(K, T^*)$$

when $r = 0$. These are the analogues in the present situation of the elements $x_{\mathfrak{p}}^{(1)} \in \check{\operatorname{Sel}}(K, T)$ and $x_{\mathfrak{p}^*}^{(1)} \in \check{\operatorname{Sel}}(K, T^*)$ constructed in [14] when $r = 1$.

Let $\mathcal{C}_\infty \subseteq \mathcal{E}_\infty$ and $\mathcal{C}_\infty^* \subseteq \mathcal{E}_\infty^*$ denote the norm-coherent systems of elliptic units constructed in [14, §3], and write $\overline{\mathcal{C}}_\infty$ and $\overline{\mathcal{C}}_\infty^*$ for the closure of $\mathcal{C}_\infty$ in $\overline{\mathcal{E}}_\infty$ and $\mathcal{C}_\infty^*$ in $\mathcal{E}_\infty^*$ respectively. Set

$$\mathcal{J}^* := \operatorname{Ker}(\psi^* : \Lambda(\mathcal{K}_\infty^*) \to \mathbf{Z}_p), \quad \mathcal{J} := \operatorname{Ker}(\psi : \Lambda(\mathcal{K}_\infty) \to \mathbf{Z}_p),$$

and let ϑ^* be the generator of $\mathcal{J}^*$ fixed in [14, §6] (so $\vartheta^* = \gamma\psi^*(\gamma^{-1}) - 1$, where γ is any topological generator of $\operatorname{Gal}(\mathcal{K}_\infty^*/K)$ satisfying $\log_p(\psi^*(\gamma)) = p$). Write $\mathfrak{f} \subseteq O_K$ for the conductor of the Grossencharacter associated to E, and let $\mathbf{N}(\mathfrak{f})$ denote the norm of this ideal. Fix $B \in E_{\mathfrak{f}}/\operatorname{Gal}(\overline{K}/K)$, and generators w of T and w^* of T^* according to the recipe described in [14, §6]. Let

$$\theta_B(\mathbf{N}(\mathfrak{f})^{-1}w^*) \in \overline{\mathcal{C}}_\infty^* \subseteq U_{\infty,\mathfrak{p}}^* \otimes \mathbf{Q}$$

denote the elliptic unit constructed in [14, §3].

Suppose that t is a positive integer such that

$$\overline{\mathcal{C}}_\infty^* \subseteq \mathcal{I}^{t-1}\overline{\mathcal{E}}_\infty^* \subseteq U_{\infty,\mathfrak{p}}^* \otimes \mathbf{Q} \quad \text{and} \quad \overline{\mathcal{C}}_\infty^* \subseteq \mathcal{I}^t(U_{\infty,\mathfrak{p}}^* \otimes \mathbf{Q}).$$

Proposition 9.3. *There exists a unique homomorphism* $\sigma_{\mathfrak{p}}^{(t)} \in \operatorname{Hom}(T^*, (U_{\infty,\mathfrak{p}}^* \otimes \mathbf{Q})/\overline{\mathcal{E}}_\infty^*)$ *such that*

$$\sigma_{\mathfrak{p}}^{(t)}(w^*)^{\vartheta^{*t}} = \theta_B(-\mathbf{N}(\mathfrak{f})^{-1}w^*)$$

in $\overline{\mathcal{E}}_\infty^*/\mathcal{J}^{*t}\overline{\mathcal{E}}_\infty^*$.

Proof. Theorem 7.2(i) of [14] implies that $U_{\infty,\mathfrak{p}}^*$ contains no ϑ^*-torsion elements. The existence of $\sigma_{\mathfrak{p}}^{(t)}$ therefore follows via an argument very similar to that of [14, Theorem 4.2]. □

We set

$$s_{\mathfrak{p}}^{(t)} := \rho(\sigma_{\mathfrak{p}}^{(t)}), \quad s_{\mathfrak{p}^*}^{(t)} := \rho^*(\sigma_{\mathfrak{p}^*}^{(t)}),$$

where of course the definition $\sigma_{\mathfrak{p}^*}^{(t)} \in \mathrm{Hom}(T, (U_{\infty,\mathfrak{p}^*} \otimes \mathbf{Q})/\overline{\mathcal{E}}_\infty)$ the same, *mutatis mutandis*, as that of $\sigma_{\mathfrak{p}}^{(t)}$.

Remark 9.4. In fact the only non-zero values of $s_{\mathfrak{p}}^{(t)}$ and $s_{\mathfrak{p}^*}^{(t)}$ occur when $r = 0$ and $t = 1$:

(a) Suppose that $r = 0$. Then $L_{\mathfrak{p}}(1) \neq 0$, and so we have (via [14, Theorem 7.2(i)], for example):

$$\overline{\mathcal{C}}_\infty \subseteq \overline{\mathcal{E}}_\infty \subset U_{\infty,\mathfrak{p}} \otimes \mathbf{Q} \quad \text{and} \quad \overline{\mathcal{C}}_\infty \not\subseteq \mathcal{I}(U_{\infty,\mathfrak{p}} \otimes \mathbf{Q}).$$

In particular, we have that $\overline{\mathcal{C}}_\infty \not\subseteq \mathcal{I}\overline{\mathcal{E}}_\infty \subseteq U_{\infty,\mathfrak{p}} \otimes \mathbf{Q}$. Similar remarks imply that also $\overline{\mathcal{C}}^*_\infty \not\subseteq \mathcal{I}^*\overline{\mathcal{E}}^*_\infty \subseteq U^*_{\infty,\mathfrak{p}^*} \otimes \mathbf{Q}$. Applying Remark 9.1, we deduce that

$$\overline{\mathcal{C}}^*_\infty \not\subseteq \mathcal{I}^*\overline{\mathcal{E}}^*_\infty \subseteq U^*_{\infty,\mathfrak{p}^*} \otimes \mathbf{Q}. \tag{9.1}$$

Now suppose in addition that $[\,,\,]_{K,\mathfrak{p}^*}$ is non-degenerate. Then Theorem A implies that $\mathrm{ord}_{s=1} L^*_{\mathfrak{p}}(s) = 1$, and so from [14, Theorem 7.2(i)], we have

$$\overline{\mathcal{C}}^*_\infty \subseteq \mathcal{I}^*(U^*_{\infty,\mathfrak{p}} \otimes \mathbf{Q}). \tag{9.2}$$

We now deduce from (9.1) and (9.2) and the definition of ρ that $s_{\mathfrak{p}}^{(1)} \neq 0$.

A similar argument shows that $s_{\mathfrak{p}^*}^{(1)} \neq 0$ also.

(b) Suppose now that $r \geq 1$. Assume that Ш$(K)(p)$ is finite, and that the height pairing $[\,,\,]_{K,\mathfrak{p}^*}$ is non-degenerate. Then Theorem B (or [14, Corollary 11.3]) implies that $\mathrm{ord}_{s=1} L^*_{\mathfrak{p}}(s) = r-1$, and so it follows from [14, Theorem 7.2(i)] that

$$\overline{\mathcal{C}}^*_\infty \subseteq \mathcal{I}^{*r-1}(U^*_{\infty,\mathfrak{p}} \otimes \mathbf{Q}). \tag{9.3}$$

On the other hand, Theorem 4.2 and Proposition 4.4 of [14] imply that

$$\overline{\mathcal{C}}^*_\infty \subseteq \mathcal{I}^{*r-1}\overline{\mathcal{E}}^*_\infty \subseteq U^*_{\infty,\mathfrak{p}^*} \otimes \mathbf{Q}, \quad \overline{\mathcal{C}}^*_\infty \not\subseteq \mathcal{I}^{*r}\overline{\mathcal{E}}^*_\infty \subseteq U^*_{\infty,\mathfrak{p}^*} \otimes \mathbf{Q},$$

and so applying Remark 9.1, we deduce that

$$\overline{\mathcal{C}}^*_\infty \subseteq \mathcal{I}^{*r-1}\overline{\mathcal{E}}^*_\infty \subseteq U^*_{\infty,\mathfrak{p}} \otimes \mathbf{Q}, \quad \overline{\mathcal{C}}^*_\infty \not\subseteq \mathcal{I}^{*r}\overline{\mathcal{E}}^*_\infty \subseteq U^*_{\infty,\mathfrak{p}} \otimes \mathbf{Q}. \tag{9.4}$$

It now follows from (9.3) and (9.4) that $s_{\mathfrak{p}}^{(t)} = 0$ for $1 \leq t \leq r-2$ and that $s_{\mathfrak{p}}^{(t)}$ is not defined for $t \geq r-1$.

(c) Suppose that $r = 0$, but that $\mathrm{ord}_{s=1} L^*_{\mathfrak{p}}(s) > 1$ (so, in particular, the pairing $[\,,\,]_{K,\mathfrak{p}^*}$ is degenerate, which we expect never to happen). Then an argument similar to that given in (b) above shows that $s_{\mathfrak{p}}^{(1)} = 0$, and that $s_{\mathfrak{p}}^{(t)}$ is not defined for $t > 1$. □

Theorem 9.5. *Suppose that $r = 0$ and that $[\ ,\ ]_{K,\mathfrak{p}^*}$ is non-degenerate, so* $\mathrm{ord}_{s=1} L^*_{\mathfrak{p}}(s) = 1$. *Then*

$$\lim_{s\to 1} \frac{L^*_{\mathfrak{p}}(s)}{s-1} = \mathbf{N}(\mathfrak{f})^{-1}(p-1)\left(1 - \frac{\psi^*(\mathfrak{p})}{p}\right) \lim_{n\to\infty} \log_{\mathfrak{p}}(\sigma^{(1)}_{\mathfrak{p},n}(w^*)).$$

Proof. This may be shown in exactly the same way as [14, Proposition 9.4(ii)]. □

Remark 9.6. The precise relationship between Theorem A and Theorem 9.5 is not clear, and it would be interesting to obtain a better understanding of this. □

References

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

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

[3] J. Cassels, *Arithmetic on curves of genus* 1 *(VIII). On Conjectures of Birch and Swinnerton-Dyer*, Crelle **217** (1965), 180–199.

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

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

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

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

[8] 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.

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

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

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

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

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

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

[15] 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.

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

Department of Mathematics, University of California, Santa Barbara, CA 93106.

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