SIGNED SELMER GROUPS OVER P-ADIC LIE EXTENSIONS

ANTONIO LEI AND SARAH LIVIA ZERBES

Abstract. Let E be an elliptic curve over $\mathbb{Q}$ with good supersingular reduction at a prime $p \geq 3$ and $a_p = 0$. We generalise the definition of Kobayashi's plus/minus Selmer groups over $\mathbb{Q}(\mu_{p^\infty})$ to p-adic Lie extensions K_∞ of $\mathbb{Q}$ containing $\mathbb{Q}(\mu_{p^\infty})$, using the theory of (φ, Γ)-modules and Berger's comparison isomorphisms. We show that these Selmer groups can be equally described using the "jumping conditions" of Kobayashi via the theory of overconvergent power series. Moreover, we show that such an approach gives the usual Selmer groups in the ordinary case.

Contents

2000 *Mathematics Subject Classification.* 11R23,11G05.
The first author is supported by an ARC DP1092496 grant.
The second author is supported by EPSRC Postdoctoral Fellowship EP/F043007/1.

1. Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$ with good supersingular reduction at a prime $p \geq 3$ and $a_p = 0$. Kobayashi [Kob03] constructed two Λ-cotorsion Selmer groups $\mathrm{Sel}^i(E/\mathbb{Q}(\mu_p^\infty))$, $i = 1, 2$ (denoted by $\mathrm{Sel}^\pm(E/\mathbb{Q}(\mu_p^\infty))$ in *op.cit.*) by modifying the local condition at p in the definition of the usual Selmer group. In this paper, we propose an analogous definition of signed Selmer groups $\mathrm{Sel}^i(E/K_\infty)$ of E over K_∞ for $i = 1, 2$, where K_∞ is a p-adic Lie extension over $\mathbb{Q}$ which contains $\mathbb{Q}(\mu_{p^\infty})$.

The main idea of our construction is the use of Berger's comparison isomorphism in [Ber02]. Let us first recall the description of the signed Selmer groups $\mathrm{Sel}^i(E/\mathbb{Q}(\mu_{p^\infty}))$ in terms of p-adic Hodge theory as given in [LLZ10]. Let $V = \mathbb{Q}_p \otimes T$ where $T = T_pE$ is the Tate module of E at p, then V is a crystalline representation of $\mathcal{G}_{\mathbb{Q}_p}$, the absolute Galois group of $\mathbb{Q}_p$. We write $\mathbb{N}(T)$ for the Wach module of T (c.f. [Ber03, Wac96]). Then a result of Fontaine/Berger states that we have a canonical isomorphism $H^1_{\mathrm{Iw}}(\mathbb{Q}_p, T) \cong \mathbb{N}(T)^{\psi=1}$ (we will identify these two objects throughout the paper). Let $n^\pm$ be the canonical basis of $\mathbb{N}(T)$ as constructed in the appendix of *op.cit.*, and let $v^\pm$ be the induced basis of $\mathbb{D}_{\mathrm{cris}}(V)$. Via Berger's comparison isomorphism, any element $x \in \mathbb{N}(T)^{\psi=1}$ can be expressed in the form $x = x_1 v^+ + x_2 v^-$ where $x_i \in \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}$ for $i = 1, 2$. Define

$$H^1_{\mathrm{Iw}}(\mathbb{Q}_p, T)^i = \left\{ x \in \mathbb{N}(T)^{\psi=1} \mid \varphi(x_i) = -p\psi(x_i) \right\},$$

and let $H^1(\mathbb{Q}_p(\mu_{p^n}), T)^i$ be the image of $H^1_{\mathrm{Iw}}(\mathbb{Q}_p, T)^i$ under the natural projection map $H^1_{\mathrm{Iw}}(\mathbb{Q}_p, T) \to H^1(\mathbb{Q}_p(\mu_{p^n}), T)$. Define $H^1_{f,i}(\mathbb{Q}_p(\mu_{p^n}), E_{p^\infty})$ to be the exact annihilator of $H^1(\mathbb{Q}_p(\mu_{p^n}), T)^i$ under the Tate pairing. One then defines $\mathrm{Sel}^i(E/\mathbb{Q}(\mu_{p^n}))$ by replacing the usual local condition $H^1_f(\mathbb{Q}_p(\mu_{p^n}), E_{p^\infty})$ at the unique prime of $\mathbb{Q}(\mu_{p^n})$ above p by $H^1_{f,i}(\mathbb{Q}_p(\mu_{p^n}), E_{p^\infty})$.

If F is an arbitrary finite extension of $\mathbb{Q}_p$, then $H^1_{\mathrm{Iw}}(F, T)$ is canonically isomorphic to $\mathbb{D}_F(T)^{\psi=1}$, where $\mathbb{D}_F(T)$ denotes the (φ, Γ)-module of T over the base field $\mathbb{A}_F$. Moreover, every element $x \in \mathbb{D}_F(T)$ can be uniquely written as $x = x_1 v^+ + x_2 v^-$ with $x_i \in \mathbb{B}^\dagger_{\mathrm{rig},F}$. It therefore seems natural to make the following definition: for $i = 1, 2$, let

$$H^1_{\mathrm{Iw}}(F, T)^i = \left\{ x \in \mathbb{D}_F(T)^{\psi=1} \mid \varphi(x_i) = -p\psi(x_i) \right\}.$$

One can the repeat the above construction to define 'new' local conditions $H^1_{f,i}(F(\mu_{p^n}), E_{p^\infty})$ for $i = 1, 2$. If K is a finite extension of $\mathbb{Q}$, this allows us to define signed Selmer groups $\mathrm{Sel}^i(E/K(\mu_{p^n}))$ for $i = 1, 2$ and for all $n \geq 0$. By passing to the direct limit over n, we obtain the Selmer groups $\mathrm{Sel}^i(E/K_\infty)$. The details of this construction is given in Section 3.1.

When E has good ordinary reduction at p, we have defined $\mathrm{Sel}^i(E/\mathbb{Q}(\mu_{p^\infty}))$ for $i = 1, 2$ in [LLZ10] in the same way as the good supersingular case. To justify the proposed definition of signed Selmer groups over K_∞, we show in Section 3.2 that on extending our construction to the good ordinary case, $\mathrm{Sel}^2(E/K_\infty)$ again agrees with the usual Selmer group $\mathrm{Sel}(E/K_\infty)$ for any finite extension K of $\mathbb{Q}$.

In Section 4, we give a more explicit description of the local conditions we use to define the signed Selmer groups in the supersingular case. If F is a finite extension of $\mathbb{Q}_p$, we write $F_n = F(\mu_{p^n})$. We define for a large integer N, which depends on F,

$$\hat{E}^i_N(\mathcal{O}_{F_n}) := \left\{ x \in \hat{E}(\mathcal{O}_{F_n}) : \mathrm{Tr}_{F_n/F_m}\, x \in \hat{E}(\mathcal{O}_{F_{m-1}}) \text{ for all } m \in S^n_{N,i'} \text{ and } \mathrm{Tr}_{F_n/F_N}\, x = 0 \right\},$$

where

$$S^n_{N,1'} = \{m \in [N+1, n] : m \text{ even}\};$$
$$S^n_{N,2'} = \{m \in [N+1, n] : m \text{ odd}\}.$$

We show that if we define $\mathrm{Sel}^{(i)}_N(E/K_n)$ by replacing the local conditions at places above p in the definition of $\mathrm{Sel}(E/K_n)$ by these "jumping conditions", then for $i = 1, 2$ we have isomorphisms

$$\mathrm{Sel}^{(i)}_N(E/K_\infty) \cong \mathrm{Sel}^i(E/K_\infty)$$

on taking direct limits.

In Section 5, we extend the definition of signed Selmer groups to p-adic Lie extensions and formulate a $\mathfrak{M}_H(G)$-conjecture, analogous to the one for the good ordinary case in [CFK+05]. Finally, we will explain some of the difficulties we encountered when attempting to extract information on the conjecture in Section 6.

Acknowledgements. We would like to thank John Coates and David Loeffler for their interest, and the latter for many helpful comments. Part of this paper was written while the authors were visiting the University of Warwick; they would like to thank the number theory group for their hospitality.

2. Notation and background

Let F be a finite extension of $\mathbb{Q}_p$. Write $\mathrm{Rep}_{\mathbb{Z}_p}(\mathcal{G}_F)$ (resp. $\mathrm{Rep}_{\mathbb{Q}_p}(\mathcal{G}_F)$) for the category of finitely generated $\mathbb{Z}_p$-modules (resp. finite-dimensional $\mathbb{Q}_p$-vector spaces) with a continuous action of $\mathcal{G}_F$.

For an integer $n \geq 1$, we write $\mathbb{Q}_{p,n} = \mathbb{Q}_p(\mu_{p^n})$, $\mathbb{Q}_{p,\infty} = \varinjlim \mathbb{Q}_{p,n}$ and $\Gamma = \mathrm{Gal}(\mathbb{Q}_{p,\infty}/\mathbb{Q}_p)$. More generally, if F is a finite extension of $\mathbb{Q}_p$, we write $F_n = F(\mu_{p^n})$, $F_\infty = \varinjlim F_n$, $H_F = \mathrm{Gal}(\overline{\mathbb{Q}_p}/F_\infty)$ and $\Gamma_F = \mathrm{Gal}(F_\infty/F)$. For $T \in \mathrm{Rep}_{\mathbb{Z}_p}(\mathcal{G}_F)$, define $H^1_{\mathrm{Iw}}(F, T) = \varprojlim H^1(F_n, T)$ where the connecting maps are corestrictions $\mathrm{cor}_{n/m} : H^1(F_n, T) \to H^1(F_m, T)$ for $n \geq m$. If $V \in \mathrm{Rep}_{\mathbb{Q}_p}(\mathcal{G}_F)$, let $H^1_{\mathrm{Iw}}(F, V) = H^1_{\mathrm{Iw}}(F, T) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, where T is a $\mathcal{G}_F$-invariant lattice of V. If G is a compact p-adic Lie group, we write $\Lambda(G) = \mathbb{Z}_p[[G]]$ for its completed group ring over $\mathbb{Z}_p$.

For a finite set S of primes of $\mathbb{Q}$, let F_S denote the maximal algebraic extension of $\mathbb{Q}$ unramified outside S. For an extension K of $\mathbb{Q}$ contained in F_S, we write $G_S(K) = \mathrm{Gal}(F_S/K)$.

2.1. Rings of periods.

Let $\overline{\mathbb{Q}_p}$ be an algebraic closure of $\mathbb{Q}_p$, and write $\mathbb{C}_p$ for its p-adic completion. Let $\mathcal{O}_{\mathbb{C}_p}$ be its ring of integers. Define

$$\tilde{\mathbb{E}} = \varprojlim_{x \to x^p} \mathbb{C}_p = \left\{(x^{(0)}, x^{(1)}, \dots) \mid \left(x^{(i+1)}\right)^p = x^{(i)}\right\},$$

and let $\tilde{\mathbb{E}}^+ = \left\{x \in \tilde{\mathbb{E}} \mid x^{(0)} \in \mathcal{O}_{\mathbb{C}_p}\right\}$. If $x = (x^{(i)})$ and $y = y^{(i)}$ are elements of $\tilde{\mathbb{E}}$, define their sum and product by

$$(xy)^{(i)} = x^{(i)} y^{(i)}$$
$$(x+y)^{(i)} = \lim_{n \to +\infty} \left(x^{(i+n)} + y^{(i+n)}\right)^{p^n}.$$

Under these operations, $\tilde{\mathbb{E}}$ is an algebraically closed field of characteristic p. Note that by construction $\tilde{\mathbb{E}}$ is equipped with a continuous action of $\mathcal{G}_{\mathbb{Q}_p}$. Define a valuation on $\tilde{\mathbb{E}}$ by $v_{\tilde{\mathbb{E}}}(x) = v_p(x^{(0)})$. Let $\varepsilon = (\varepsilon^{(i)})$ be a fixed element of $\tilde{\mathbb{E}}$ such that $\varepsilon^{(0)} = 1$ and $\varepsilon^{(1)} \neq 1$, and let $\overline{\pi} = \varepsilon - 1$. Let $\mathbb{E}_{\mathbb{Q}_p} = \mathbb{F}_p((\overline{\pi}))$, and define $\tilde{\mathbb{E}}$ to

be a separable closure of $\mathbb{E}_{\mathbb{Q}_p}$ in $\mathbb{E}$. Then $\mathbb{E}$ is equipped with a continuous action of $\mathcal{G}_{\mathbb{Q}_p}$, and one can show that $\mathbb{E}^{H_{\mathbb{Q}_p}} = \mathbb{E}_{\mathbb{Q}_p}$.

Let $\tilde{\mathbb{A}} = W(\tilde{\mathbb{E}})$ be the ring of Witt vectors of $\tilde{\mathbb{E}}$ and

$$\tilde{\mathbb{B}} = \tilde{\mathbb{A}}[p^{-1}] = \left\{ \sum_{k \gg -\infty} p^k [x_k] \mid x_k \in \tilde{\mathbb{E}} \right\},$$

where $[x]$ denotes the Teichmüller lift of $x \in \tilde{\mathbb{E}}$. By construction, both rings are equipped with continuous semi-linear actions of a Frobenius operator φ and $\mathcal{G}_{\mathbb{Q}_p}$. Let $\pi = [\varepsilon] - 1$ and $q = \varphi(\pi)/\pi$, and define $\mathbb{A}_{\mathbb{Q}_p}$ to be the completion of $\mathbb{Z}_p[[\pi]][\pi^{-1}]$ in the p-adic topology. Then $\mathbb{A}_{\mathbb{Q}_p}$ is closed under the actions of φ and $\mathcal{G}_{\mathbb{Q}_p}$, and moreover the action of $\mathcal{G}_{\mathbb{Q}_p}$ factors through $\Gamma_{\mathbb{Q}_p}$. Let $\mathbb{B}$ be the p-adic completion of the maximal unramified extension of $\mathbb{B}_{\mathbb{Q}_p} = \mathbb{A}_{\mathbb{Q}_p}[p^{-1}]$ in $\tilde{\mathbb{B}}$, and let $\mathbb{A} = \mathbb{B} \cap \tilde{\mathbb{A}}$. These rings are stable under the actions of φ and $\mathcal{G}_{\mathbb{Q}_p}$. For a finite extension F of $\mathbb{Q}_p$, put $\mathbb{A}_F = \mathbb{A}^{H_F}$. If F_∞ is Galois over $\mathbb{Q}_p$, then $\mathbb{A}_F$ is equipped with a continuous action of $\mathcal{G}_F$ which commutes with φ.

For a p-adic representation $T \in \mathrm{Rep}_{\mathbb{Z}_p}(\mathcal{G}_{\mathbb{Q}_p})$ (resp. $V \in \mathrm{Rep}_{\mathbb{Q}_p}(\mathcal{G}_{\mathbb{Q}_p})$), define $\mathbb{D}_F(T) = (\mathbb{A} \otimes_{\mathbb{Z}_p} T)^{H_F}$ (resp. $\mathbb{D}_F(V) = (\mathbb{B} \otimes_{\mathbb{Q}_p} V)^{H_F}$). Then $\mathbb{D}_F(T)$ (resp. $\mathbb{D}_F(V)$) is a free finitely generated module over $\mathbb{A}_F$ of rank $d = \mathrm{rank}_{\mathbb{Z}_p}(T)$ (resp. a finite dimensional vector space over $\mathbb{B}_{\mathbb{Q}_p}$ of dimension $d = \dim_{\mathbb{Q}_p}(V)$), equipped with commuting semi-linear actions of φ and Γ_F. Note that $\mathbb{D}_F(T) = \mathbb{D}_{\mathbb{Q}_p}(T) \otimes_{\mathbb{A}_{\mathbb{Q}_p}} \mathbb{A}_F$ (resp. $\mathbb{D}_F(V) = \mathbb{D}_{\mathbb{Q}_p}(V) \otimes_{\mathbb{B}_{\mathbb{Q}_p}} \mathbb{B}_F$).

Remark 2.1. *If F_∞ is Galois over $\mathbb{Q}_p$, then the action of Γ_F extends to an action of $G_F = \mathrm{Gal}(F_\infty/\mathbb{Q}_p)$. Moreover, the action of G_F commutes with the action of φ.*

Every element $x \in \tilde{\mathbb{B}}$ can be written uniquely of the form $x = \sum_{k \gg -\infty} p^k [x_k]$ with $x_k \in \tilde{\mathbb{E}}$. For an integer $n \geq 0$, define

$$\tilde{\mathbb{B}}^{\dagger,n} = \left\{ x \in \tilde{\mathbb{B}} \mid \lim_{k \to +\infty} \left(k + p^{-n} v_{\tilde{\mathbb{E}}}(x_k) \right) = +\infty \right\}$$

and let $\mathbb{B}^{\dagger,n} = \tilde{\mathbb{B}}^{\dagger,n} \cap \mathbb{B}$ and $\mathbb{B}_F^{\dagger,n} = \left(\mathbb{B}^{\dagger,n}\right)^{H_F}$ for any finite extension F of $\mathbb{Q}_p$. Also, let $\tilde{\mathbb{A}}^{\dagger,n} = \{x \in \tilde{\mathbb{B}}^{\dagger,n} \cap \tilde{\mathbb{A}} \mid k + p^{-n} v_{\tilde{\mathbb{E}}}(x_k) \geq 0 \text{ for all } k\}$, $\mathbb{A}^{\dagger,n} = \tilde{\mathbb{A}}^{\dagger,n} \cap \mathbb{A}$ and $\mathbb{A}_F^{\dagger,n} = \left(\mathbb{A}^{\dagger,n}\right)^{H_F}$. Finally, define $\mathbb{B}^\dagger = \bigcup_n \mathbb{B}^{\dagger,n}$, $\mathbb{A}^\dagger = \bigcup_n \mathbb{A}^{\dagger,n}$, $\mathbb{B}_F^\dagger = \bigcup_n \mathbb{B}_F^{\dagger,n}$ and $\mathbb{A}_F^\dagger = \bigcup_n \mathbb{A}_F^{\dagger,n}$. Explicitly, one can describe the ring $\mathbb{A}_F^{\dagger,n}$ for $n \gg 0$ as follows (c.f. [Ber02, Proposition 1.4]): there exists $N_F > 0$ and $\pi_F \in \mathbb{A}_F^{\dagger,N_F}$ whose reduction mod p is a uniformizer $\overline{\pi_F}$ of $\mathbb{E}_F$. Moreover, if $n \geq N_F$, then every element $x \in \mathbb{B}_F^{\dagger,n}$ can be written as $\sum_{k \in \mathbb{Z}} a_k \pi_F^k$, where the a_k are elements in the maximal unramified extension F' of $\mathbb{Q}_p$ in F_∞, and where the series $\sum_{k \in \mathbb{Z}} a_k X^k$ is holomorphic and bounded on the annulus $p^{-1/e_F p^{n-1}(p-1)} \leq |\, X \,| < 1$.

Let F be a finite extension of $\mathbb{Q}_p$. For $V \in \mathrm{Rep}_{\mathbb{Q}_p}(\mathcal{G}_{\mathbb{Q}_p})$, define $\mathbb{D}_F^{\dagger,r}(V) = \left(\mathbb{B}^{\dagger,r} \otimes_{\mathbb{Q}_p} V\right)^{H_F}$ and $\mathbb{D}_F^\dagger(V) = \left(\mathbb{B}^\dagger \otimes_{\mathbb{Q}_p} V\right)^{H_F}$. Note that $\mathbb{D}_F^\dagger(V) = \mathbb{D}_{\mathbb{Q}_p}^\dagger(V) \otimes_{\mathbb{B}_{\mathbb{Q}_p}^\dagger} \mathbb{B}_F^\dagger$. The main result of [CC98] shows that every p-adic representation V of $\mathcal{G}_{\mathbb{Q}_p}$ is overconvergent, i.e. there exists $r(V) > 0$ such that

$$\mathbb{D}_{\mathbb{Q}_p}(V) = \mathbb{B}_{\mathbb{Q}_p} \otimes_{\mathbb{B}_{\mathbb{Q}_p}^{\dagger,r(V)}} \mathbb{D}^{\dagger,r(V)}(V).$$

If V is a crystalline representation of $\mathcal{G}_{\mathbb{Q}_p}$, then a stronger result is true: V is of finite hight, i.e. let $\tilde{\mathbb{B}}^+ = W(\tilde{\mathbb{A}}^+)[p^{-1}]$, $\mathbb{B}^+ = \mathbb{B} \cap \tilde{\mathbb{B}}^+$ and $\mathbb{B}_{\mathbb{Q}_p}^+ = (\mathbb{B}^+)^{H_{\mathbb{Q}_p}}$, and define $\mathbb{D}_{\mathbb{Q}_p}^+(V) = (\mathbb{B}^+ \otimes_{\mathbb{Q}_p} V)^{H_{\mathbb{Q}_p}}$. Then

$$\mathbb{D}_{\mathbb{Q}_p}(V) = \mathbb{D}_{\mathbb{Q}_p}^+(V) \otimes_{\mathbb{B}_{\mathbb{Q}_p}^+} \mathbb{B}_{\mathbb{Q}_p}.$$

2.2. **The Robba ring.** We write $\mathbb{B}^{+}_{\mathrm{rig},\mathbb{Q}_p}$ for the set of $f(\pi)$ where $f(X) \in \mathbb{Q}_p[[X]]$ converges everywhere on the open unit p-adic disc. In particular, $t = \log(1+\pi) \in \mathbb{B}^{+}_{\mathrm{rig},\mathbb{Q}_p}$. Let F be a finite extension of $\mathbb{Q}_p$. For $n \geq 0$, define $\mathbb{B}^{\dagger,n}_{\mathrm{rig},F}$ to be the completion of $\mathbb{B}^{\dagger,n}_{F}$ in the Fréchet topology, and define the Robba ring $\mathbb{B}^{\dagger}_{\mathrm{rig},F} = \bigcup_n \mathbb{B}^{\dagger,n}_{\mathrm{rig},F}$. By [Ber02, Lemme 3.13] we have

$$\mathbb{B}^{\dagger,n}_{\mathrm{rig},F} = \mathbb{B}^{\dagger,n}_{\mathrm{rig},\mathbb{Q}_p} \otimes_{\mathbb{B}^{\dagger,n}_{\mathbb{Q}_p}} \mathbb{B}^{\dagger,n}_{F}.$$

By [Ber03, Proposition I.3], we can identify $\mathbb{B}^{\dagger,n}_{\mathrm{rig},\mathbb{Q}_p}$ with the ring of power series

$$\mathbb{B}^{\dagger,n}_{\mathrm{rig},\mathbb{Q}_p} = \big\{ f(\pi) \mid f(X) \in \mathbb{Q}_p\{\{X\}\} \text{ converges for } p^{-1/p^{n-1}(p-1)} \leq \mid X \mid < 1 \big\}.$$

Note that the actions of φ and Γ_F extend to $\mathbb{B}^{+}_{\mathrm{rig},F}$ and $\mathbb{B}^{\dagger}_{\mathrm{rig},F}$.

The most important application of $\mathbb{B}^{\dagger}_{\mathrm{rig},F}$ is Berger's comparison isomorphism: if V is a crystalline representation of $\mathcal{G}_F$, we write $\mathbb{D}_{\mathrm{cris}}(V)$ and $\mathbb{N}(V)$ for the Dieudonné module and the Wach module of V respectively, then there is a canonical isomorphism

$$\iota : \mathbb{D}^{\dagger}_{F}(V) \otimes_{\mathbb{B}^{\dagger}_{F}} \mathbb{B}^{\dagger}_{\mathrm{rig},F}[t^{-1}] \cong \mathbb{D}_{\mathrm{cris}}(V) \otimes_{F^{\mathrm{nr}}} \mathbb{B}^{\dagger}_{\mathrm{rig},F}[t^{-1}] \tag{1}$$

which is compatible

$$\mathrm{Sel}^{i}(E/L_\infty) = \ker\left(H^1(G_S(L_\infty), E_{p^\infty}) \to \bigoplus_{v \in S} J^{i}_{v}(L_\infty) \right).$$

with the actions of $\mathcal{G}_F$ and φ. If V is a crystalline representation of $\mathcal{G}_{\mathbb{Q}_p}$, then we indeed have a comparison isomorphism

$$\iota : \mathbb{N}(V) \otimes_{\mathbb{B}^{+}_{\mathbb{Q}_p}} \mathbb{B}^{+}_{\mathrm{rig},\mathbb{Q}_p}[t^{-1}] \cong \mathbb{D}_{\mathrm{cris}}(V) \otimes_{\mathbb{Q}_p} \mathbb{B}^{+}_{\mathrm{rig},\mathbb{Q}_p}[t^{-1}].$$

2.3. **The operator ψ.** Note that the extension $\mathbb{E}$ over $\varphi(\mathbb{E})$ is inseparable of degree p. One can hence define a left inverse ψ of φ on $\mathbb{A}$. Explicitly, a basis of $\mathbb{A}$ over $\varphi(\mathbb{A})$ is given by $1, 1+\pi, \ldots, (1+\pi)^{p-1}$. For $x \in \mathbb{A}$, we may write $x = \sum_{i=0}^{p-1} \varphi(x_i)(1+\pi)^i$ where $x_i \in \mathbb{A}$. We set $\psi(x) = x_0$.

If F is a finite extension of $\mathbb{Q}_p$ and $V \in \mathrm{Rep}_{\mathbb{Z}_p}(\mathcal{G}_F)$ or $\mathrm{Rep}_{\mathbb{Q}_p}(\mathcal{G}_F)$, then ψ extends to a left inverse of φ $\mathbb{D}_F(V)$. If F_∞ is Galois over $\mathbb{Q}_p$, then by Remark 2.1 we have an action of G_F on $\mathbb{D}_F(T)$ which commutes with φ and hence with ψ.

2.4. **Tate twists.** Let F be a finite extension of $\mathbb{Q}_p$. We write χ for the p-cyclotomic character of $\mathcal{G}_F$. If m is an integer and $V \in \mathrm{Rep}_{\mathbb{Q}_p}(\mathcal{G}_F)$ (resp. $T \in \mathrm{Rep}_{\mathbb{Z}_p}(\mathcal{G}_F)$), we denote by $V(m)$ (resp. $T(m)$) the $\mathcal{G}_F$-representations $V \otimes_{\mathbb{Q}_p} \mathbb{Q}_p \cdot e_m$ (resp. $T \otimes_{\mathbb{Z}_p} \mathbb{Z}_p \cdot e_m$) where $\mathcal{G}_F$ acts on e_m via χ^m. In particular, we have

$$\mathbb{D}_{\mathrm{cris}}(V(m)) = \mathbb{D}_{\mathrm{cris}}(V) \otimes t^{-m} e_m, \quad \mathbb{N}(T(m)) = \mathbb{N}(T) \otimes \pi^{-m} e_m \quad \text{and} \quad \mathbb{N}(V(m)) = \mathbb{N}(V) \otimes \pi^{-m} e_m.$$

2.5. **The Herr complex.** We first review some results from p-adic Hodge theory. Let F be a finite extension of $\mathbb{Q}_p$. Let $T \in \mathrm{Rep}_{\mathbb{Z}_p}(\mathcal{G}_{\mathbb{Q}_p})$. Recall the following result from [Her98] (see also [CC99, §2]). Let γ be a topological generator of Γ_F. For $f = \varphi$ or ψ, define the complex

$$\mathcal{C}^{\bullet}_{f,\gamma}\big(\mathbb{D}_F(T)\big) : 0 \to \mathbb{D}_F(T) \xrightarrow{\alpha_f} \mathbb{D}_F(T) \oplus \mathbb{D}_F(T) \xrightarrow{\beta_f} \mathbb{D}_F(T) \to 0,$$

where $\alpha_f(x) = \big((\gamma-1)x, (f-1)x\big)$ and $\beta_f(x,y) = (f-1)x - (\gamma-1)y$. Denote by $H^i\big(\mathcal{C}^{\bullet}_{f,\gamma}(\mathbb{D}_F(V))\big)$ the i-th cohomology group of the complex.

Theorem 2.2. *For $f = \varphi$ or ψ, $H^i\big(\mathcal{C}^\bullet_{f,\gamma}(\mathbb{D}_F(T))\big)$ is canonically isomorphic to $H^i(F,T)$. In particular, if $(x,y) \in \mathbb{D}_F(T)^{\oplus 2}$ satisfies $\beta_\varphi(x,y) = 0$, then the corresponding cohomology class in $H^1(F,T)$ is given by the cocycle*

$$c_{(x,y)} : \sigma \mapsto \frac{\sigma - 1}{\gamma - 1} x - (\sigma - 1)z,$$

where $z \in \mathbb{A} \otimes_{\mathbb{Z}_p} T$ is such that $(\varphi - 1)z = y$.

Theorem 2.3. *We have an $\Lambda(\Gamma_F)$-equivariant isomorphism $H^1_{\mathrm{Iw}}(F,T) \cong \mathbb{D}_F(T)^{\psi=1}$. If F_∞ is Galois over $\mathbb{Q}_p$, then the isomorphism is compatible with the action of $G = \mathrm{Gal}(F_\infty/\mathbb{Q}_p)$.*

Proof. See [CC99, Théorème II.1.3]. □

From now on, we will identify $H^1_{\mathrm{Iw}}(F,T)$ with $\mathbb{D}_F(T)^{\psi=1}$ under the isomorphism given by Theorem 2.3.

3. The signed Selmer groups

Let E be an elliptic curve defined over $\mathbb{Q}$, and fix a prime $p \geq 3$. In this section, we use the theory of (φ,Γ)-modules to define signed Selmer groups $\mathrm{Sel}^i(E/L(\mu_{p^\infty}))$ for any number field L, when E has either good supersingular or good ordinary reduction at p. If E has good ordinary reduction at p, then Theorem 3.15 shows that $\mathrm{Sel}^2(E/L_\infty)$ agrees with the usual Selmer group $\mathrm{Sel}(E/L_\infty)$.

3.1. **Good supersingular elliptic curves.** Assume throughout this section that $a_p = 0$. Let $T_p(E)$ be the Tate module of E at p and write $V = T_pE \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, so as a representation of $\mathcal{G}_{\mathbb{Q}_p}$, V is crystalline with Hodge-Tate weights $0, 1$. Let v_1 be a basis of $\mathrm{Fil}^0 \mathbb{D}_{\mathrm{cris}}(V)$, and extend it to a basis v_1, v_2 of $\mathbb{D}_{\mathrm{cris}}(V)$ such that the matrix of φ on $\mathbb{D}_{\mathrm{cris}}(V)$ in this basis is $\begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix}$.

Define $\log^-(1+\pi) = \prod_{i\geq 0} \frac{\varphi^{2i}(q)}{p}$ and $\log^+(1+\pi) = \prod_{i\geq 0} \frac{\varphi^{2i+1}(q)}{p}$, which are elements of $\mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}$. Since the Hodge-Tate weights of V are non-negative, we have

$$\mathbb{N}(T) \subset \mathbb{D}_{\mathrm{cris}}(V) \otimes \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}$$

by [Ber03, Proposition II.2.1], and it follows form Appendice (3) in *op.cit.* that a basis n_1, n_2 of $\mathbb{N}(T)$ is given by $\begin{pmatrix} n_1 \\ n_2 \end{pmatrix} = M \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$, where

$$M = \begin{pmatrix} \log^-(1+\pi) & 0 \\ 0 & \log^+(1+\pi) \end{pmatrix}. \tag{2}$$

Let K be a finite extension of $\mathbb{Q}_p$. For $x \in \mathbb{D}^\dagger_K(T)^{\psi=1}$, we write

$$x = x_1 v_1 + x_2 v_2 = x_1' n_1 + x_2' n_2$$

with $x_i \in \mathbb{B}^{\dagger,N}_{\mathrm{rig},K}$ and $x_i' \in \mathbb{A}^{\dagger,N}_K$. By (2), we have

$$x_1 = x_1' \log^-(1+\pi) \quad \text{and} \quad x_2 = x_2' \log^+(1+\pi). \tag{3}$$

Definition 3.1. *For $i = 1, 2$, let*

$$H^1_{\mathrm{Iw}}(K,T)^i = \left\{ x \in \mathbb{D}^\dagger_K(T)^{\psi=1} : \varphi(x_i) = -p\psi(x_i) \right\}.$$

For $n \geq 1$, define $H^1(K_n, T)^i$ to be the image of $H^1_{\mathrm{Iw}}(K, T)^i$ under the natural projection map $H^1_{\mathrm{Iw}}(K, T) \to H^1(K_n, T)$.

Remark 3.2. *As show in* [LLZ10, §5.2.1]*, we have $H^1_{\mathrm{Iw}}(\mathbb{Q}_p, T)^i = H^1_{\mathrm{Iw}}(\mathbb{Q}_p, T) \cap \ker(\underline{\mathrm{Col}}_i)$ for the Coleman maps*

$$\underline{\mathrm{Col}}_i : H^1_{\mathrm{Iw}}(\mathbb{Q}_p, T) \longrightarrow \Lambda(\Gamma)$$

defined in op.cit.

Definition 3.3. *Let $H^1_{f,i}(K_n, E_{p^\infty})$ be the orthogonal complement of $H^1(K_n, T)^i$ under the Pontryagin duality*

$$[\sim, \sim] : H^1(K_n, T) \times H^1(K_n, E_{p^\infty}) \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p$$

for $i = 1, 2$.

We now return to the global situation. As above, let L be a finite extension of $\mathbb{Q}$. For a prime ν of L, denote by L_ν be the completion of L at ν, and let $L_{\nu,n} = L_\nu(\mu_{p^n})$. Let S be the finite set of primes of $\mathbb{Q}$ containing p, all the primes where E has bad reduction and the infinite prime. Let $i = 1, 2$. For all $v \in S$, define

$$J^i_v(L_n) = \bigoplus_{w_n | v} \frac{H^1(L_{w_n,n}, E_{p^\infty})}{H^1_{f,i}(L_{w_n,n}, E_{p^\infty})},$$

where the direct sum is taken over all primes w_n of L_n above v and $H^1_{f,i}(L_{w_n,n}, E_{p^\infty}) = H^1_f(L_{w_n,n}, E_{p^\infty})$ whenever $v \neq p$. We write $J^i_v(L_\infty) = \varinjlim J^i_v(L_n)$.

Definition 3.4. *For $i = 1, 2$, define*

$$\mathrm{Sel}^i(E/L_\infty) = \ker\left(H^1(G_S(L_\infty), E_{p^\infty}) \longrightarrow \bigoplus_{v \in S} J^i_v(L_\infty) \right).$$

For $n \geq 0$, we also define

$$\mathrm{Sel}^i(E/L_n) = \ker\left(H^1(G_S(L_n), E_{p^\infty}) \longrightarrow \bigoplus_{v \in S} J^i_v(L_{n,v}) \right).$$

Taking direct limits then gives

$$\mathrm{Sel}^i(E/L_\infty) = \varinjlim \mathrm{Sel}^i(E/L_n).$$

3.2. **Good ordinary elliptic curves.** In this section, let E be an elliptic curve defined over $\mathbb{Q}$ with good ordinary reduction at a prime $p \geq 3$. As above, let S be the finite set of primes of $\mathbb{Q}$ containing p, all the primes where E has bad reduction and the infinite prime.

3.2.1. *Coleman maps and signed Selmer groups.* We first recall our construction of the signed Selmer groups from [LLZ10]. Let $\bar{\nu}_1, \bar{\nu}_2$ and $\bar{n}_1, \bar{n}_2$ be the bases of $\mathbb{D}_{\mathrm{cris}}(V(-1))$ and $\mathbb{N}(V(-1))$, respectively, as defined in [LLZ10, §3.2]. In particular, if $\hat{E}$ denotes the formal group of E and $\hat{V} = T_p\hat{E} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, then $\bar{\nu}_1$ is a basis vector of $\mathbb{D}_{\mathrm{cris}}(\hat{V}(-1))$ and $\bar{n}_1 = \bar{\nu}_1$ is a basis of $\mathbb{N}(\hat{V}(-1))$. If M' is the change of basis matrix with

$$\begin{pmatrix} \bar{\nu}_1 \\ \bar{\nu}_2 \end{pmatrix} = M' \begin{pmatrix} \bar{n}_1 \\ \bar{n}_2 \end{pmatrix}, \tag{4}$$

then M' is lower triangular, with 1 and $\frac{t}{\pi}$ on the diagonal. If $x \in \mathbb{N}(V)$, then there exist unique $x_1, x_2 \in \mathbb{B}^+_{\mathbb{Q}_p}$ such that $x = (x_1\bar{n}_1 + x_2\bar{n}_2) \otimes \pi^{-1}e_1$. By (4), we can find unique $x_1', x_2' \in \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}$ such that

$$x = (x_1'\bar{\nu}_1 + x_2'\bar{\nu}_2) \otimes t^{-1}e_1 \tag{5}$$

with $x_2' = x_2$. If P denotes the matrix of φ with respect to the basis $\bar{n}_1, \bar{n}_2$, then P is upper-triangular. Let α be the unit root of the polynomial $X^2 - a_pX + p$, then P is in fact of the form

$$P = \begin{pmatrix} \alpha & \star \\ 0 & uq \end{pmatrix}$$

for some $u \in (\mathbb{B}^+_{\mathbb{Q}_p})^\times$ which is congruent to $\alpha^{-1} \mod \pi$.

In [LLZ10], we have defined two pairs of Coleman maps (with respect to the chosen basis),

$$\mathrm{Col}_i : \mathbb{N}(V)^{\psi=1} \longrightarrow (\mathbb{B}^+_{\mathbb{Q}_p})^{\psi=0}, \quad \text{and}$$
$$\underline{\mathrm{Col}}_i : \mathbb{N}(V)^{\psi=1} \longrightarrow \Lambda_{\mathbb{Q}_p}(\Gamma)$$

for $i = 1, 2$ with the following properties: for $x \in \mathbb{N}(V)^{\psi=1}$, write $x = (x_1\bar{n}_1 + x_2\bar{n}_2) \otimes \pi^{-1}e_1$ where $x_1, x_2 \in \mathbb{B}^+_{\mathbb{Q}_p}$. Then

$$(1-\varphi)(x) = \begin{pmatrix} \mathrm{Col}_1(x) & \mathrm{Col}_2(x) \end{pmatrix} M \begin{pmatrix} \bar{\nu}_1 \\ \bar{\nu}_2 \end{pmatrix} \otimes t^{-1}e_1 \tag{6}$$

$$= \begin{pmatrix} \underline{\mathrm{Col}}_1(x) & \underline{\mathrm{Col}}_2(x) \end{pmatrix} \cdot [(1+\pi)M] \begin{pmatrix} \bar{\nu}_1 \\ \bar{\nu}_2 \end{pmatrix} \otimes t^{-1}e_1 \tag{7}$$

where $M = \frac{t}{\pi q} P^T (M')^{-1}$.

Definition 3.5. *Let $H^1(\mathbb{Q}_{p,n}, T)^i$ be the image of $\ker(\underline{\mathrm{Col}}_i) \cap \mathbb{N}(T)^{\psi=1}$ under the natural maps $\mathbb{N}(T)^{\psi=1} \to H^1_{\mathrm{Iw}}(\mathbb{Q}_p, T) \to H^1(\mathbb{Q}_{p,n}, T)$ and write $H^1_{f,i}(\mathbb{Q}_{p,n}, E_{p^\infty})$ for the exact annihilator of $H^1(\mathbb{Q}_{p,n}, T)^i$ under the Tate pairing.*

If E is defined over $\mathbb{Q}$, we can then define the signed Selmer groups $\mathrm{Sel}^i(E/\mathbb{Q}(\mu_{p^\infty}))$ analogously to the construction when E is supersingular at p.

Definition 3.6. *Define*

$$\mathrm{Sel}^i(E/\mathbb{Q}(\mu_{p^n})) = \ker\left(\mathrm{Sel}(E/\mathbb{Q}(\mu_{p^n})) \to \frac{H^1(\mathbb{Q}_p(\mu_{p^n}), E_{p^\infty})}{H^1_{f,i}(\mathbb{Q}_p(\mu_{p^n}), E_{p^\infty})})\right)$$

where $\mathrm{Sel}(E/\mathbb{Q}(\mu_{p^n}))$ denotes the usual Selmer group and we define $\mathrm{Sel}^i(E/\mathbb{Q}(\mu_{p^\infty}))$ to be the direct limit of $\mathrm{Sel}^i(E/\mathbb{Q}(\mu_{p^n}))$.

We now show that on choosing an appropriate basis, we can describe $\ker(\underline{\mathrm{Col}}_2)$ in a manner similar to the good supersingular case (c.f. Remark 3.2).

Lemma 3.7. *We can choose $\bar{n}_2$ such that $u = \alpha^{-1}$.*

Proof. If we let $\bar{n}_1' = \bar{n}_1$ and $\bar{n}_2' = v\bar{n}_2$ where $v \in (\mathbb{B}^+_{\mathbb{Q}_p})^\times$, then $\bar{n}_1', \bar{n}_2'$ is also a basis of $\mathbb{N}(V(-1))$. The matrix of φ with respect to this basis is of the form

$$P' = \begin{pmatrix} \alpha & \star \\ 0 & v^{-1}\varphi(v)uq \end{pmatrix}.$$

Note that $\alpha u \equiv 1 \mod \pi$ implies that $\varphi^n(\alpha u) \to 1$ as $n \to \infty$. In particular, the product $\prod_{n\geq 0}\varphi^n(\alpha u)$ converges to an element $u' \in (\mathbb{B}^+_{\mathbb{Q}_p})^\times$. Since $u'\varphi(u')^{-1} = \alpha u$, we deduce that P' is of the required form if we take $v = u'$. □

Lemma 3.8. *With respect to the basis given by Lemma 3.7,*

$$\ker(\underline{\mathrm{Col}}_2) = \left\{ x \in \mathbb{N}(V)^{\psi=1} | \varphi(x_2) = \alpha x_2 \text{ where } x = (x_1\bar{n}_1 + x_2\bar{n}_2)\otimes \pi^{-1}e_1 \text{ with } x_i \in \mathbb{B}^+_{\mathbb{Q}_p} \right\}.$$

Proof. By (6), we have $\mathrm{Col}_2(x) = \alpha x_2 - \varphi(x_2)$. Moreover, M is lower triangular with $\alpha\frac{t}{\pi q}$ and α^{-1} on the diagonal. Therefore, $\ker(\underline{\mathrm{Col}}_2) = \ker(\mathrm{Col}_2)$ and we are done. □

Corollary 3.9. *With respect to the basis given by Lemma 3.7,*

$$\ker(\underline{\mathrm{Col}}_2) = \left\{ x \in \mathbb{N}(V)^{\psi=1} | \varphi(x_2) = \alpha x_2 \text{ where } x = (x_1\bar{\nu}_1 + x_2\bar{\nu}_2)\otimes t^{-1}e_1 \text{ with } x_i \in \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p} \right\}.$$

Proof. This follows from Lemma 3.8 and (5). □

Let L be a finite extension of $\mathbb{Q}$, and let $L_\infty = L(\mu_{p^\infty})$. Using Corollary 3.9, we define $\mathrm{Sel}^2(E/L_\infty)$ as follows. Let ν be a prime of L above p. If $x \in \mathbb{D}^\dagger_{L_\nu}(T)^{\psi=1}$ then we can use Berger's comparison isomorphism (1) we can write $x = (x_1\bar{\nu}_1 + x_2\bar{\nu}_2)\otimes t^{-1}e_1$ with $x_i \in \mathbb{B}^\dagger_{\mathrm{rig},L_\nu}$ as in the supersingular case. Define

$$H^1_{\mathrm{Iw}}(L_\nu, T)^2 = \left\{ x \in \mathbb{D}_{L_\nu}(T)^{\psi=1} | \varphi(x_2) = \alpha x_2 \right\}$$

and $H^1(L_{\nu,n}, T)^2$ is defined to be the projection of $H^1_{\mathrm{Iw}}(L_\nu, T)^2$ in $H^1(L_{\nu,n}, T)$. Let $H^1_{f,2}(L_{\nu,n}, E_{p^\infty})$ be the exact annihilator of $H^1_{\mathrm{Iw}}(L_\nu, T)^2$.

Definition 3.10. *For all $v \in S$, define*

$$J^2_v(L_n) = \bigoplus_{w_n | v} \frac{H^1(L_{w_n,n}, E_{p^\infty})}{H^1_{f,2}(L_{w_n,n}, E_{p^\infty})},$$

where the direct sum is taken over all primes w_n of L_n above v. Here, $H^1_{f,2}(L_{w_n,n}, E_{p^\infty}) = H^1_f(L_{w_n,n}, E_{p^\infty})$ whenever $v \nmid p$. Define $J^2_v(L_\infty) = \varinjlim J^{(2)}_v(L_n)$. Define

$$\mathrm{Sel}^2(E/L_\infty) = \ker\left(H^1(G_S(L_\infty), E_{p^\infty}) \to \bigoplus_{v\in S} J^2_v(L_\infty) \right).$$

3.2.2. *Properties of* $\mathrm{Sel}^2(E/L_\infty)$. Let us now study the group $H^1_{\mathrm{Iw}}(L_\nu, T)^2$ a bit further. To simplify notation, let $K = L_\nu$.

Lemma 3.11. *Let $a \in \mathbb{Z}_p^\times$, and assume that a is not a root of unity. If $x \in \mathbb{B}^\dagger_{\mathrm{rig},K}$ satisfies*

$$ax - \varphi(x) = 0 \tag{8}$$

then $x = 0$.

Proof. If $x \in \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}$, then we can substitute $\pi = e^t - 1$ to write x of the form $\sum_{n\geq 0} c_n t^n$ with $c_n \in \mathbb{Q}_p$. Since $\varphi(t) = pt$, it is clear from this description that for any $a \neq 1$ and $x \neq 0$, we have $\varphi(x) \neq ax$.

Let $x \in \mathbb{B}^\dagger_{\mathrm{rig},\mathbb{Q}_p} - \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}$. Assume that there exists $n \geq 0$ be such that $x \in \mathbb{B}^{\dagger,n}_{\mathrm{rig},\mathbb{Q}_p}$ and $x \notin \mathbb{B}^{\dagger,n-1}_{\mathrm{rig},\mathbb{Q}_p}$. Then $\varphi(x) \in \mathbb{B}^{\dagger,n+1}_{\mathrm{rig},\mathbb{Q}_p} - \mathbb{B}^{\dagger,n}_{\mathrm{rig},\mathbb{Q}_p}$, so $\varphi(x) \neq ax$.

If $x \in \mathbb{B}^{\dagger,n}_{\mathrm{rig},\mathbb{Q}_p}$ for all $n \geq 0$ and $x \notin \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}$, then $\varphi^{-1}(x)$ converges in $\mathbb{B}^+_{\mathrm{dR}}$, so if we write $x = f(\pi)$, then $f(T)$ does not have a pole at $\varepsilon^{(1)} - 1$. But $f(T)$ has a pole at $T = 0$ as $x \notin \mathbb{B}^+_{\mathrm{rig},\mathbb{Q}_p}$, so $f\big((T+1)^p - 1\big)$ has poles at the $\{(\varepsilon^{(1)})^i - 1 : 0 \leq i < p\}$. Hence $\varphi(x) \neq ax$.

Assume now that $x \in \mathbb{B}^\dagger_{\mathrm{rig},K}$ satisfies $\varphi(x) = ax$, and that $x \notin \mathbb{B}^\dagger_{\mathrm{rig},\mathbb{Q}_p}$. On replacing K by its Galois closure, if necessary, we may assume that $K/\mathbb{Q}_p$, and hence $K_\infty/\mathbb{Q}_{p,\infty}$, are Galois. Let $H = \mathrm{Gal}(K_\infty/\mathbb{Q}_{p,\infty})$. Since φ is H-equivariant, $\sigma(x)$ also satisfies (8) for all $\sigma \in H$. More generally, if $\sigma_1, \dots, \sigma_i \in H$, then $y = \sigma_1(x_2) \dots \sigma_i(x_2)$ satisfies $a^i y = \varphi(y)$. The coefficients of the polynomial

$$f(Y) = \prod_{\sigma \in H} (Y - \sigma(x))$$

are elements in $\mathbb{B}^\dagger_{\mathrm{rig},\mathbb{Q}_p}$ which satisfy an equation of the form (8), so they must all be zero by the above argument. But the minimal polynomial of x over $\mathbb{B}^\dagger_{\mathrm{rig},\mathbb{Q}_p}$ divides $f(Y)$, which gives a contradiction. □

Remark 3.12. *The unit root α of the polynomial $X^2 - a_p X + p$ is a Weil number of complex absolute value $\sqrt{p}$, so it cannot be a root of unity.*

Proposition 3.13. *Let $x \in \mathbb{D}^\dagger_{K_\nu}(V)^{\psi=1}$, and write $x = (x_1\bar{\nu}_1 + x_2\bar{\nu}_2) \otimes t^{-1}e_1$ with $x_i \in \mathbb{B}^\dagger_{\mathrm{rig},\mathbb{Q}_p}$. Then $x \in H^1_{\mathrm{Iw}}(K_\nu, T)^2$ if and only if $x_2 = 0$.*

Proof. Immediate from Lemma 3.11 and Remark 3.12. □

Corollary 3.14. *$x \in H^1_{\mathrm{Iw}}(K, T)^2$ if and only if $x \in \mathbb{D}_K(\hat{T})^{\psi=1}$.*

Proof. It follows immediately from the comparison isomorphism and the fact that $\bar{\nu}_1 = \bar{n}_1$ that any $x \in \mathbb{D}_K(T)^{\psi=1}$ which satisfies $\iota(x) = x_1\bar{\nu}_1 \otimes t^{-1}e_1$ must indeed lie in $\mathbb{D}_K(\hat{T})$. □

We can now conclude this section with the following theorem.

Theorem 3.15. *We have* $\mathrm{Sel}(E/L_\infty) = \mathrm{Sel}^2(E/L_\infty)$.

Proof. Since $L/\mathbb{Q}$ is finite and E had good ordinary reduction at p, we have $V^{H_{L_\nu}} = 0$ for all primes ν of L above p. This implies that

$$H^1_{\mathrm{Iw}}(L_\nu, \hat{T}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = \varprojlim H^1_g(L_{\nu,n}, T) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

by [PR00, Proposition 0.1] (or [Ber05, Theorem A]). But $H^1_f(L_{\nu,n}, T) = H^1_g(L_{\nu,n}, T)$ by [BK90, (3.11.2)]), we have

$$H^1_{\mathrm{Iw}}(L_\nu, \hat{T}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = \varprojlim H^1_f(L_{\nu,n}, T) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

It is clear that the quotients $\mathbb{D}_K(T)^{\psi=1}/\mathbb{D}_K(\hat{T})^{\psi=1}$ and $H^1(L_{\nu,n}, T)/H^1_f(L_{\nu,n}, T)$ are torsion-free over $\mathbb{Z}_p$. We can therefore deduce that

$$H^1_{\mathrm{Iw}}(L_\nu, \hat{T}) = \varprojlim H^1_f(L_{\nu,n}, T).$$

On taking Pontryagin duals, we have $J^2_\nu(L_\infty) = J_\nu(L_\infty)$, which finishes the proof. □

4. An alternative definition of the signed Selmer groups

Let E be an elliptic curve defined over $\mathbb{Q}$ with good supersingular reduction at a prime $p \geq 3$ such that $a_p = 0$, and let L be a finite extension of $\mathbb{Q}$. The main result of this section is Proposition 4.18 below, which shows that the local conditions at the primes above p in the definition of the signed Selmer groups $\mathrm{Sel}^i(E/L_\infty)$ using some "jumping conditions" similar to those introduced in [Kob03].

4.1. **Preliminary results on $\mathbb{B}_K^\dagger$.** Let K be a finite extension of $\mathbb{Q}_p$, and let K' be the maximal unramified extension of $\mathbb{Q}_p$ contained in K_∞. It is easy to see from the description of the ring $\mathbb{A}_K^{\dagger,n}$ given in Section 2.1 that it is complete in the p-adic topology.

Lemma 4.1. *For all $n \geq N_K$, $\mathbb{A}_K^{\dagger,n}$ is the p-adic completion of $\mathcal{O}_{K'}[\![\pi_K]\!][\pi_K^{-1}] \cap \mathbb{A}_K^{\dagger,n}$.*

Proof. Note that the condition that $\sum_{k\in\mathbb{Z}} a_k X^k$ is holomorphic and bounded above by 1 on the annulus $p^{-1/e_K p^{n-1}(p-1)} \leq |\ X\ | < 1$ is equivalent to the condition that

$$v_p(a_k) + \frac{k}{e_K(p-1)p^{n-1}} \geq 0 \quad \text{and} \to +\infty \text{ as } k \to -\infty.$$

□

Lemma 4.2. *Let $x \in \mathbb{A}_K^{\dagger,N}$ where $N \geq N_K$. If $\theta \circ \varphi^{-n}(x) = 0$ for infinitely many $n \geq N$, then $x = 0$.*

Proof. Firstly, we assume that $x \in \mathcal{O}_{K'}[\![\pi_K]\!][\pi_K^{-1}]$. We write σ for the Frobenious in $\mathrm{Gal}(K'/\mathbb{Q}_p)$. Let

$$F(X) = \sum_{m\geq -r} b_m X^m \in \mathcal{O}_{K'}[\![X]\!][X^{-1}]$$

such that $F(\pi_K) = x$. For $i = 1, \ldots, [K' : \mathbb{Q}_p]$, write

$$F_i(X) = \sum_{m\geq -r} \sigma^i(b_m) X^m.$$

Then $\theta \circ \varphi^{-n}(x) = F_i(\pi_n)$, where $i + n \equiv 0 \mod [K' : \mathbb{Q}_p]$ and $\pi_n = \theta \circ \varphi^{-n}(\pi_K)$. Therefore, there exists an i such that F_i has infinitely many zeros. But $F_i \in X^{-r}\mathcal{O}_{K'}[\![X]\!]$, so $F_i = 0$ by the Weierstrass preparation theorem. This implies that $b_m = 0$ for all m, so $x = 0$.

To conclude, note that if $n \geq N$, $\{x \in \mathbb{A}_K^{\dagger,N} : \theta \circ \varphi^{-n}(x) = 0\}$ is a closed set of $\mathbb{A}_K^{\dagger,N}$ under the p-adic topology and $\mathbb{A}_K^{\dagger,N}$ is the p-adic completion of $\mathcal{O}_{K'}[\![\pi_K]\!][\pi_K^{-1}] \cap \mathbb{A}_K^{\dagger,N}$ by Lemma 4.1. □

Lemma 4.3. *Let $n \gg 0$ and $x \in \mathbb{B}_K^{\dagger,n}$, then*

$$\mathrm{Tr}_{K_n/K_{n-1}} \circ \theta \circ \varphi^{-n}(x) = \theta \circ \varphi^{-n} \circ \mathrm{Tr}_{\mathbb{B}/\varphi(\mathbb{B})}(x).$$

Proof. We let n be an integer such that $[K_n : K_{n-1}] = p$ and $n \geq a(K) + 1$ where $a(K)$ is the integer as in [CC99, Proposition III.2.1]. Write

$$x = \sum_{i=0}^{p-1} [\varepsilon]^i \varphi(x_i)$$

where $x_i \in \mathbb{B}_K^{\dagger,n-1}$. Then,

$$\theta \circ \varphi^{-n+1}(x_i) \in K_{n-1}$$

for all i. Therefore,

$$\begin{aligned}\mathrm{Tr}_{K_n/K_{n-1}} \circ\theta\circ\varphi^{-n}(x) &= \mathrm{Tr}_{K_n/K_{n-1}}\left(\sum_{i=0}^{p-1}\zeta_{p^n}^i\theta\circ\varphi^{1-n}(x_i)\right)\\ &= p\theta\circ\varphi^{1-n}(x_0).\end{aligned}$$

But we have $\mathrm{Tr}_{\mathbb{B}/\varphi(\mathbb{B})}(x) = p\varphi(x_0)$, which finishes the proof. □

4.2. **The local conditions.** Write $\mathbb{D}_K^\dagger(T)$ for the overconvergent (φ,Γ)-module of T over K. It is clear from the definition that

$$\mathbb{D}_K^\dagger(T) = \mathbb{A}_K^\dagger \otimes_{\mathbb{A}_{\mathbb{Q}_p}^+} \mathbb{N}(T),$$

so in particular the basis n_1, n_2 of $\mathbb{N}(T)$ given in Section 3.1 is a basis of $\mathbb{D}_K^\dagger(T)$ over $\mathbb{A}_K^\dagger$.

As shown in [CC99, Proposition III.3.2], we have $\mathbb{D}_K^\dagger(T)^{\psi=1} \subset \mathbb{D}_K^{\dagger,N}(T)$ for $N \geq N(K,V)$. Fix such an N; note that it is not uniquely defined. Let $x \in \mathbb{D}_K^\dagger(T)^{\psi=1}$. Then as in Section 3.1, we can write

$$x = x_1v_1 + x_2v_2 = x_1'n_1 + x_2'n_2$$

with $x_i \in \mathbb{B}_{\mathrm{rig},K}^{\dagger,N}$ and $x_i' \in \mathbb{B}_K^{\dagger,N}$ for $i = 1,2$.

Lemma 4.4. *Let $x \in \mathbb{D}_K^\dagger(T)^{\psi=1}$, then*

$$\mathrm{Tr}_{K_n/K_{n-1}} \circ\theta\circ\varphi^{-n}(x_1) = -\theta\circ\varphi^{2-n}(x_1)$$

for all odd integers $n \geq N+2$ and

$$\mathrm{Tr}_{K_n/K_{n-1}} \circ\theta\circ\varphi^{-n}(x_2) = -\theta\circ\varphi^{2-n}(x_2)$$

for all even integers $n \geq N+2$.

Proof. By definitions, we have $\varphi(\log^+(1+\pi)) = \frac{p}{q}\log^-(1+\pi)$ and $\varphi(\log^-(1+\pi)) = \log^+(1+\pi)$, and that similar relations hold when replacing φ by ψ. The relations (3) therefore imply that

$$\varphi(x_1) + p\psi(x_1) = (\varphi(x_1') + \psi(qx_1'))\log^+(1+\pi); \tag{9}$$

$$\varphi(x_2) + p\psi(x_2) = (\varphi(x_2') + q\psi(x_2'))\,p/q\log^-(1+\pi). \tag{10}$$

If $n \geq 2$ is an even integer, then $\theta\circ\varphi^{-n}\left(\log^+(1+\pi)\right) = 0$. Therefore, (9) implies that

$$\theta\circ\varphi^{-n+1}(x_1) + \theta\circ\varphi^{-n-1}\left(p\varphi\circ\psi(x_1)\right) = 0.$$

Recall that $p\varphi\circ\psi = \mathrm{Tr}_{\mathbb{B}/\varphi(\mathbb{B})}$, so Lemma 4.3 implies the first part of the lemma. Similarly, the second half the lemma follows from (10) and the fact that

$$\theta\circ\varphi^{-n}\left(p/q\log^-(1+\pi)\right) = 0$$

for all odd integers $n \geq 3$. □

Proposition 4.5. *Let $x \in \mathbb{D}_K^\dagger(T)^{\psi=1}$, then $x \in H^1_{\mathrm{Iw}}(K,T)^i$ if and only if*

$$\mathrm{Tr}_{K_n/K_{n-1}} \circ\theta\circ\varphi^{-n}(x_i) = -\theta\circ\varphi^{2-n}(x_i)$$

for all $n \geq N+2$.

Proof. If $x \in H^1_{\mathrm{Iw}}(K,T)^i$, then

$$\varphi^2(x_i) = -p\varphi\circ\psi(x_i) = -\operatorname{Tr}_{\mathbb{B}/\varphi(\mathbb{B})}(x_i).$$

On applying $\theta\circ\varphi^{-n}$ to both sides, we have by Lemma 4.3 that

$$\theta\circ\varphi^{2-n}(x_i) = -\operatorname{Tr}_{K_n/K_{n-1}}\circ\theta\circ\varphi^{-n}(x_i)$$

as required.

Conversely, we assume that

$$\operatorname{Tr}_{K_n/K_{n-1}}\circ\theta\circ\varphi^{-n}(x_i) = -\theta\circ\varphi^{2-n}(x_i)$$

for all $n \geq N+2$. Then $\theta\circ\varphi^{-n}\left(\varphi(x_i)+p\psi(x_i)\right) = 0$ by Lemma 4.3. Our assumption implies that $\varphi(x_1')+\psi(qx_1') = 0$ for $i=1$ and $\varphi(x_2')+q\psi(x_2') = 0$ for $i=2$ by Lemma 4.2 and the equations (9) and (10). Therefore, we have $x \in H^1_{\mathrm{Iw}}(K,T)^i$ as required. □

Remark 4.6. *By Lemma 4.4, we can rewrite Proposition 4.5 as follows:*

$$\begin{aligned} H^1_{\mathrm{Iw}}(K,T)^1 &= \left\{x\in\mathbb{D}^\dagger_K(T)^{\psi=1} : \operatorname{Tr}_{K_n/K_{n-1}}\circ\theta\circ\varphi^{-n}(x_1) = -\theta\circ\varphi^{2-n}(x_1) \text{ for all even } n\geq N+2\right\};\\ H^1_{\mathrm{Iw}}(K,T)^2 &= \left\{x\in\mathbb{D}^\dagger_K(T)^{\psi=1} : \operatorname{Tr}_{K_n/K_{n-1}}\circ\theta\circ\varphi^{-n}(x_2) = -\theta\circ\varphi^{2-n}(x_2) \text{ for all odd } n\geq N+2\right\}. \end{aligned}$$

We can now describe $H^1_{\mathrm{Iw}}(K,T)^i$ as follows.

Corollary 4.7. *We have*

$$\begin{aligned} H^1_{\mathrm{Iw}}(K,T)^1 &= \left\{x\in\mathbb{D}_K(T)^{\psi=1} : \exp^*_{K_n}\circ h^1_{\mathrm{Iw},n}(x)\in K_{n-1}\cdot v_1 \text{ for all odd } n\geq N+1\right\},\\ H^1_{\mathrm{Iw}}(K,T)^2 &= \left\{x\in\mathbb{D}_K(T)^{\psi=1} : \exp^*_{K_n}\circ h^1_{\mathrm{Iw},n}(x)\in K_{n-1}\cdot v_1 \text{ for all even } n\geq N+1\right\}. \end{aligned}$$

Proof. By [CC99, Théorème IV.2.1],

$$\exp^*_{K_n}\circ h^1_{\mathrm{Iw},n}(x) = \partial_V\circ\varphi^{-n}(x)$$

for all $n \geq N$. Since

$$\partial_V\circ\varphi^{-n}(x) = \theta\circ\varphi^{-n}(x_1)\varphi^{-n}(v_1)+\theta\circ\varphi^{-n}(x_2)\varphi^{-n}(v_2)$$

and the image of $\exp^*_{K_n}$ lies in $K_n\otimes\operatorname{Fil}^0\mathbb{D}_{\mathrm{cris}}(V)$, it follows that

$$\exp^*_{K_n}\circ h^1_{\mathrm{Iw},n}(x) = \begin{cases} (-1)^m p^{-m}\theta\circ\varphi^{-2m}(x_1)v_1 & \text{if } n=2m\geq N,\\ (-1)^m p^{-m}\theta\circ\varphi^{-(2m+1)}(x_2)v_1 & \text{if } n=2m+1\geq N. \end{cases}$$

Extend the trace map $\operatorname{Tr}_{K_n/K_{n-1}}$ to the map $\operatorname{Tr}_{K_n/K_{n-1}}\circ\mathrm{id}$ on $K_n\otimes_{\mathbb{Q}_p}\mathbb{D}_{\mathrm{cris}}(V)$. Then, $x\in H^1_{\mathrm{Iw}}(K,T)^1$ if and only if

$$\operatorname{Tr}_{K_n/K_{n-1}}\circ\exp^*_{K_n}\circ h^1_{\mathrm{Iw},n}(x) = p^{-1}\exp^*_{K_{n-2}}\circ h^1_{\mathrm{Iw},n-2}(x)$$

for all even $n\geq N+2$. But

$$\operatorname{Tr}_{K_m/K_{m-1}}\circ\exp^*_{K_m} = \exp^*_{K_{m-1}}\circ\mathrm{cor}_{K_m/K_{m-1}}$$

for all $m\geq 0$, so we deduce that $x\in H^1_{\mathrm{Iw}}(K,T)^1$ if and only if

$$\exp^*_{K_{n-1}}\circ h^1_{\mathrm{Iw},n-1}(x) = p^{-1}\operatorname{Tr}_{K_{n-1}/K_{n-2}}\circ\exp^*_{K_{n-1}}\circ h^1_{\mathrm{Iw},n-1}(x)$$

for all even $n \geq N-2$. □

As a important consequence, we can characterise $H^1_{\mathrm{Iw}}(K,T)^i$ completely in terms of the conditions on the finite levels:

Corollary 4.8. *For $i \in \{1,2\}$ and $n \geq N+1$, define*

$$H^1_N(K_n,T)^{(i)} = \left\{x \in H^1(K_n,T) : \mathrm{Tr}_{K_n/K_m} \circ \exp^*_{K_n}(x) \in K_{m-1} \cdot v_1 \quad \text{for all } m \in S^n_{N,i}\right\}.$$

where $S^n_{N,i}$ is given by

$$\begin{aligned} S^n_{N,1} &= \{m \in [N+1,n] : m \text{ odd }\}, \\ S^n_{N,2} &= \{m \in [N+1,n] : m \text{ even }\}. \end{aligned}$$

Then $H^1_{\mathrm{Iw}}(K,T)^i = \varprojlim H^1_N(K_n,T)^{(i)}$.

Proof. Immediate from Corollary 4.7. □

Notation. Let F be a finite extension of $\mathbb{Q}_p$. For an integer $n \geq 1$, we write $F^{(0)}_n = \ker(\mathrm{Tr}_{F_n/F_{n-1}})$. Then we have

$$F_n = F \oplus \bigoplus_{i=1}^{n} F_i^{(0)}. \tag{11}$$

Lemma 4.9. *Let $n \geq N+1$ be an integer, then*

$$H^1_N(K_n,T)^{(i)} = \left(\exp^*_{K_n}\right)^{-1}\left(K_N \oplus \bigoplus_{m \in S^n_{N,i'}} K_m^{(0)} \cdot v_1\right)$$

where $\{i'\} = \{1,2\} \setminus \{i\}$.

Proof. Let $x \in K_n$. By definition, the projection of x under (11) into $K_m^{(0)}$ is zero if and only if $\mathrm{Tr}_{K_n/K_m} x \in K_{m-1}$. Hence the result. □

From now on, we make the following assumption.

Assumption 4.10. *$E(K_\infty)$ has no p-torsion.*

Note that this is satisfied for example when $[K:\mathbb{Q}_p]$ is a power of p.

Remark 4.11. *Assumption 4.10 implies that the natural map $H^1(K_n,T) \longrightarrow H^1(K_n,V)$ is injective for all $n \geq 0$. In particular, we may embed $H^1(K_n,T)$ into $H^1(K_n,V)$ and consider the former as a lattice inside the latter.*

Proposition 4.12. *Let $H^1_{f,N,(i)}(K_n,T)$ be the exact annihilator of $H^1_N(K_n,T)^{(i)}$ under the Tate pairing. Then*

$$H^1_{f,N,(i)}(K_n,T) = H^1(K_n,T) \cap \exp_{K_n}\left(\bigoplus_{m \in S^n_{N,i}} K_m^{(0)} \otimes \mathbb{D}_{\mathrm{cris}}(V)\right)$$

Proof. By Lemma 4.9, we have

$$H^1_{f,N,(1)}(K_n,T) = \left(\left(\exp^*_{K_n}\right)^{-1} \left(K_N \oplus \bigoplus_{m\in S^n_{N,i'}} K^{(0)}_m \cdot v_1 \right) \right)^{\perp_{[,]}} \tag{12}$$

where $(\star)^{\perp_{[,]}}$ denotes the exact annihilator of $\star$ under the pairing $[\sim,\sim]$. But

$$[\exp_{K_n}(\sim),\sim] = \mathrm{Tr}_{K_n/\mathbb{Q}_p}\langle \sim, \exp^*_{K_n}(\sim)\rangle.$$

where $\langle\sim,\sim\rangle$ is the pairing

$$\langle\sim,\sim\rangle : \left(K_n \otimes \mathbb{D}_{\mathrm{cris}}(V)\right) \times \left(K_n \otimes \mathbb{D}_{\mathrm{cris}}(V)\right) \to K_n.$$

Therefore,

$$x \in \left(\left(\exp^*_{K_n}\right)^{-1} (\star \cdot v_1) \right)^{\perp_{[,]}} \quad \text{if and only if} \quad x \in \exp_{K_n}\left((\star)^{\perp} \otimes \mathbb{D}_{\mathrm{cris}}(V)\right) \tag{13}$$

where $(\star)^{\perp}$ denotes the orthogonal complement of $\star$ under the pairing

$$\begin{aligned} K_n \times K_n &\to \mathbb{Q}_p \\ (x,y) &\mapsto \mathrm{Tr}_{K_n/\mathbb{Q}_p}(xy). \end{aligned}$$

By linear algebra, we have

$$\left(K_N \oplus \bigoplus_{m\in S^n_{N,i'}} K^{(0)}_m \right)^{\perp} = \bigoplus_{m\in S^n_{N,i}} K^{(0)}_m.$$

Hence the result on combining (12) with (13). □

Recall that the exponential map $\exp_{K_n}$ gives an isomorphism

$$\exp_{K_n} : K_n \otimes \mathbb{D}_{\mathrm{cris}}(V)/\operatorname{Fil}^0 \mathbb{D}_{\mathrm{cris}}(V) \longrightarrow H^1_f(K_n,V).$$

We write $\exp^{-1}_{K_n}$ for its inverse.

By (11), we may define a projection map

$$P^n_{N,i} : K_n \longrightarrow K_N \oplus \bigoplus_{m\in S^n_{N,i'}} K^{(0)}_m.$$

We can then rewrite Proposition 4.12 as follows.

Corollary 4.13. *For $i = 1, 2$, we have*

$$H^1_{f,N,(i)}(K_n,T) = \left\{ x \in H^1_f(K_n,T) : \left(P^n_{N,i} \otimes \mathrm{id}\right) \circ \exp^{-1}_{K_n}(x) = 0 \right\}.$$

Proof. Note that

$$K_n = \left(K_N \oplus \bigoplus_{m\in S^n_{N,i'}} K^{(0)}_m \right) \oplus \left(\bigoplus_{m\in S^n_{N,i}} K^{(0)}_m \right).$$

Therefore,

$$\left(P^n_{N,i} \otimes \mathrm{id}\right) \circ \exp^{-1}_{K_n}(x) = 0 \quad \text{if and only if} \quad \exp^{-1}_{K_n}(x) \in \bigoplus_{m\in S^n_{N,i}} K^{(0)}_m \otimes \mathbb{D}_{\mathrm{cris}}(V)/\operatorname{Fil}^0 \mathbb{D}_{\mathrm{cris}}(V).$$

□

Recall that we have a commutative diagram

$$\begin{array}{ccccccc}
\tan(\hat{E}/K_n) & \xleftarrow{\ \supset\ } & \log_{\hat{E}}(\mathcal{O}_{K_n}) & \xleftarrow{\log_{\hat{E}}} & \hat{E}(\mathcal{O}_{K_n}) & \xrightarrow{\ \subset\ } & \hat{E}(\mathcal{O}_{K_n})\otimes\mathbb{Q}_p \\
\cong\downarrow i & & & & & & \downarrow\delta \\
K_n\otimes\mathbb{D}_{\mathrm{cris}}(V)/\operatorname{Fil}^0\mathbb{D}_{\mathrm{cris}}(V) & & \xrightarrow{\qquad\exp_{K_n}\qquad} & & & & H^1(K_n,V)
\end{array}$$

where δ is the Kummer map. If we identify the image of $\hat{E}(\mathcal{O}_{K_n})$ under δ with $H^1_f(K_n,T)$, we have:

Corollary 4.14. *For $i\in\{1,2\}$, the image of $H^1_{f,N,(i)}(K_n,T)$ inside $\hat{E}(\mathcal{O}_{K_n})$ coincides with*

$$\begin{aligned}\hat{E}^i_N(\mathcal{O}_{K_n}) &:= \left\{x\in\hat{E}(\mathcal{O}_{K_n}) : \mathrm{Tr}_{K_n/K_m}\, x\in\hat{E}(\mathcal{O}_{K_{m-1}}) \text{ for all } m\in S^n_{N,i'} \text{ and } \mathrm{Tr}_{K_n/K_N}\, x = 0\right\}\\ &= \left\{x\in\hat{E}(\mathcal{O}_{K_n}) : P^n_{N,i}\circ\log_{\hat{E}}(x)=0\right\}.\end{aligned}$$

Proof. By the comutative diagram above and Proposition 4.12, we have

$$\delta(x)\in H^1_{f,N,(i)}(K_n,T) \quad \text{if and only if} \quad i\circ\log_{\hat{E}}(x)\in\bigoplus_{m\in S^n_{N,i}} K^{(0)}_m\otimes\mathbb{D}_{\mathrm{cris}}(V)/\operatorname{Fil}^0\mathbb{D}_{\mathrm{cris}}(V).$$

Since $\log_{\hat{E}}$ is injective (by Assumption 4.10) and compatible with the trace maps, we are done. □

4.3. **Signed Selmer groups revisited.** We now return to the global situation as set up at the beginning of Section 4. Throughout this section, we continue to assume that Assumption 4.10 holds at all the primes of L above p. We define the signed Selmer groups of E over L_∞ using the "jumping conditions" we obtained in the previous section.

Definition 4.15. *Let L be a number field and N is an integer such that $N\geq N(L_w,V)$ for all primes w of L above p. For $i=1,2$, we define the Selmer groups*

$$\mathrm{Sel}^{(i)}_N(E/L_n) = \ker\left(\mathrm{Sel}(E/L_n)\longrightarrow\bigoplus_{w|p}\frac{H^1(L_{n,w},E_{p^\infty})}{\hat{E}^i_N(\mathcal{O}_{L_{n,w}})\otimes\mathbb{Q}_p/\mathbb{Z}_p}\right)$$

for $n\geq N+1$. Moreover, we define

$$\mathrm{Sel}^{(i)}_N(E/L_\infty) = \varinjlim_{n\geq N+1}\mathrm{Sel}^{(i)}_N(E/L_n) = \ker\left(\mathrm{Sel}(E/L_\infty)\longrightarrow\bigoplus_{\omega|p}\frac{H^1(L_{\infty,\omega},E_{p^\infty})}{\hat{E}^i_N(\mathcal{O}_{L_{\infty,\omega}})\otimes\mathbb{Q}_p/\mathbb{Z}_p}\right)$$

where $\hat{E}^i_N(\mathcal{O}_{L_{\infty,\omega}}) = \varinjlim\hat{E}^i_N(\mathcal{O}_{L_{n,\omega\cap L_n}})$.

Lemma 4.16. *Let K be a finite extension of $\mathbb{Q}_p$ and $n\geq N(K,V)$. For $i=1,2$, the exact annihilator of $H^1_N(K_n,T)^{(i)}$ under the Pontryagin duality*

$$[\sim,\sim] : H^1(K_n,T)\times H^1(K_n,E_{p^\infty})\longrightarrow\mathbb{Q}_p/\mathbb{Z}_p$$

is isomorphic to $H^1_{f,N,(i)}(K_n,T)\otimes\mathbb{Q}_p/\mathbb{Z}_p$ for $i=1,2$.

Proof. This essentially follows from [Kob03, proofs of Lemma 8.17 and Proposition 8.18]. By definition, we have an exact sequence

$$0 \longrightarrow H^1_N(K_n,T)^{(i)} \longrightarrow H^1(K_n,T) \longrightarrow \mathrm{Hom}\left(H^1_{f,N,(i)}(K_n,T),\mathbb{Z}_p\right).$$

On taking Pontryagin duals, we obtain a second exact sequence

$$H^1_{f,N,(i)}(K_n,T)\otimes\mathbb{Q}_p/\mathbb{Z}_p \longrightarrow H^1(K_n,E_{p^\infty}) \longrightarrow H^1_N(K_n,T)^{(i),\vee} \longrightarrow 0.$$

Therefore, it remains to show that the first map above is injective. But $[px,y]=p[x,y]$ for all $x,y\in H^1(K_n,T)$. This implies that if $x\in H^1(K_n,T)$ such that $px\in H^1_{f,N,(i)}(K_n,T)$, then $x\in H^1_{f,N,(i)}(K_n,T)$. □

Corollary 4.17. *Let K be a finite extension of $\mathbb{Q}_p$ and $n\geq N(K,V)$. For $i=1,2$, the exact annihilator of $H^1_N(K_n,T)^{(i)}$ under the Pontryagin duality is isomorphic to $\hat{E}^i_N(\mathcal{O}_{K_n})\otimes\mathbb{Q}_p/\mathbb{Z}_p$ for $i=1,2$.*

Proof. This follows immediately from Corollary 4.14 and Lemma 4.16. □

Proposition 4.18. *The two definitions of signed Selmer groups coincide, namely,*

$$\mathrm{Sel}^{(i)}_N(E/L_\infty)=\mathrm{Sel}^i(E/L_\infty)$$

for $i=1,2$.

Proof. It suffices to show that for any finite extensions K of $\mathbb{Q}_p$, we have

$$\varinjlim_n \frac{H^1(K_n,E_{p^\infty})}{H^1_{f,i}(K_n,E_{p^\infty})} \cong \varinjlim_{n\geq N+1} \frac{H^1(K_n,E_{p^\infty})}{\hat{E}^i_N(\mathcal{O}_{K_n})\otimes\mathbb{Q}_p/\mathbb{Z}_p}$$

where $N\geq N(K,V)$. On taking Pontryagin duals, this is equivalent to showing

$$\varprojlim H^1(K_n,T)^i \cong \varprojlim H^1_N(K_n,T)^{(i)}$$

by Corollary 4.17. Therefore, we are done by Corollary 4.8. □

5. The supersingular $\mathfrak{M}_H(G)$-conjecture

Throughout this section, we assume that E is an elliptic curve over $\mathbb{Q}$ with good supersingular reduction at a prime $p\geq 3$ and $a_p=0$. Let L_∞ be a p-adic Lie extension of $\mathbb{Q}$ containing $\mathbb{Q}(\mu_{p^\infty})$, so $G=\mathrm{Gal}(L_\infty/\mathbb{Q})$ is a compact p-adic Lie group of finite rank. Let $H=\mathrm{Gal}(L_\infty/\mathbb{Q}(\mu_{p^\infty}))$. Choose a sequence of finite extensions L_m of $\mathbb{Q}$ such that $L_\infty=\varinjlim L_m$ and $L^{(m)}_\infty=L_m(\mu_{p^\infty})$ is Galois over $\mathbb{Q}$ for all $m\geq 0$. Recall that for $i=1,2$, we have defined $\mathrm{Sel}^i(E/L^{(m)}_\infty)$ in Section 3.1. This allows to make the following definition.

Definition 5.1. *For $i=1,2$, we define $\mathrm{Sel}^i(E/L_\infty):=\varinjlim_m \mathrm{Sel}^i(E/L^{(m)}_\infty)$ for $=1,2$ and write*

$$X_i(E/L_\infty)=\mathrm{Hom}_{\mathrm{cts}}\left(\mathrm{Sel}^i(E/L_\infty),\mathbb{Q}_p/\mathbb{Z}_p\right).$$

Definition 5.2. *Denote by $\mathfrak{M}_H(G)$ the category of finitely generated $\Lambda(G)$-modules M for which $M/M(p)$ is finitely generated over $\Lambda(H)$. Here $M(p)$ denotes the p-torsion part of M.*

The $\mathfrak{M}_H(G)$-conjecture in [CFK+05] states that the Pontryagin dual of the Selmer group of E over L_∞ is an element of $\mathfrak{M}_H(G)$ if E has good ordinary reduction at p. We therefore analogously propose the following conjecture.

Conjecture 5.3. *Let E be an elliptic curve over $\mathbb{Q}$ with good supersingular reduction at p and $a_p = 0$. Let L_∞ be a p-adic Lie extension of $\mathbb{Q}$ containing $\mathbb{Q}(\mu_{p^\infty})$. Define the Galois groups $G = \mathrm{Gal}(L_\infty/\mathbb{Q})$ and $H = \mathrm{Gal}(L_\infty/\mathbb{Q}(\mu_p))$. Then $X_i(E/L_\infty) \in \mathfrak{M}_H(G)$ for $i = 1, 2$.*

6. Difficulties

To simplify the notation, let $\mathbb{Q}_\infty = \mathbb{Q}(\mu_{p^\infty})$. In order to support Conjecture 5.3, we tried to prove the following result:

Conjecture 6.1. *Let E be an elliptic curve over $\mathbb{Q}$ with good supersingular reduction at p and $a_p = 0$. Let L_∞ be a p-adic Lie extension of $\mathbb{Q}$ containing $\mathbb{Q}(\mu_{p^\infty})$, and let $H = \mathrm{Gal}(L_\infty/\mathbb{Q}(\mu_{p^\infty}))$. Assume also that $E(L_{v,\infty})$ has no p-torsion for any prime v of L above p. Then for $i = 1, 2$, the kernel and cokernel of the restriction map*

$$\mathrm{Sel}^i(E/\mathbb{Q}_\infty) \longrightarrow \mathrm{Sel}^i(E/L_\infty)^H$$

are cofinitely generated $\mathbb{Z}_p$-modules.

Recall that $\mathrm{Sel}^i(E/\mathbb{Q}_\infty)$ is $\Lambda(\Gamma)$-cotorsion ([Kob03, Theorem 1.2]). Assume H is pro-p, and that Conjecture 6.1 holds. If $\mathrm{Sel}^i(E/\mathbb{Q}_\infty)$ is a cofinitely generated $\mathbb{Z}_p$-module, which is equivalent to the vanishing of the μ-invariant of $X_i(E//\mathbb{Q}_\infty)$ as conjectured in [Kob03, §10], then we can apply Nakayama's lemma (c.f. for example [CH01, Theorem 2.6]) to deduce that $X_i(E/L_\infty)$ is finitely generated over $\Lambda(H)$.

In this section, we will explain some of the difficulties that we encountered when trying to prove Conjecture 6.1 when L_∞ is a finite extension of $\mathbb{Q}_\infty$. We first establish a preliminary result (Corollary 6.3), which allows us to study a fundamental diagram (see the beginning of Section 6.2) analogous to the ordinary case.

6.1. Analysis of Poitou-Tate exact sequences.

Write S_f for the set of finite places of S and let I_v^i be as defined in Section 3.1. By [PR95, §A.3], there are two exact sequences

$$0 \to \mathrm{Sel}^i(E/\mathbb{Q}(\mu_{p^n})) \longrightarrow H^1(G_S(\mathbb{Q}(\mu_{p^n})), E_{p^\infty}) \longrightarrow \bigoplus_{v\in S_f} J_v^i(\mathbb{Q}(\mu_{p^n})) \longrightarrow H_i^1(\mathbb{Q}, T)^\vee \longrightarrow \cdots \tag{14}$$

$$0 \to H_i^1(\mathbb{Q}(\mu_{p^n}), T) \xrightarrow{f_n} H^1(G_S(\mathbb{Q}(\mu_{p^n})), E_{p^\infty}) \xrightarrow{g_n} \bigoplus_{v\in S_f} I_v^i(\mathbb{Q}(\mu_{p^n})) \longrightarrow \cdots \tag{15}$$

where $H_i^1(\mathbb{Q}(\mu_{p^n}), T)$ is defined by

$$\ker\Big(H^1(\mathbb{Q}(\mu_{p^n}), T) \longrightarrow \prod_{v\in S_f} I_v^i(\mathbb{Q}(\mu_{p^n}))\Big)$$

and $M^\vee$ denotes the Pontryagin dual of M.

Lemma 6.2. *The natural map*

$$H^1\big(G_S(\mathbb{Q}_\infty), E_{p^\infty}\big) \longrightarrow \bigoplus_{v\in S_f} J_v^i(\mathbb{Q}_\infty)$$

is surjective.

Proof. On taking inverse limit, we have

$$\varprojlim_n \Big(\bigoplus_{v\in S_f} I_v^i(\mathbb{Q}(\mu_{p^n}))\Big) = \frac{H^1_{\mathrm{Iw}}(\mathbb{Q}_p, T)}{H^1_{\mathrm{Iw}}(\mathbb{Q}_p, T)^i}$$

and $\varprojlim_n g_n$ is injective by [Kob03, Theorem 7.3]. Therefore, on taking inverse limit in (15), we have

$$\varprojlim_n H_i^1(\mathbb{Q}(\mu_{p^n}), T) = 0,$$

which implies that $\varinjlim_n H_i^1(\mathbb{Q}(\mu_{p^n}), T)^\vee = 0$. Therefore, on taking direct limit in (14), we have an exact sequence

$$0 \longrightarrow \mathrm{Sel}^i(E/\mathbb{Q}_\infty) \longrightarrow H^1\big(G_S(\mathbb{Q}_\infty), E_{p^\infty}\big) \longrightarrow \bigoplus_{v\in S_f} J_v^i(\mathbb{Q}_\infty) \longrightarrow 0$$

and we are done. □

Corollary 6.3. *The natural map*

$$H^1\big(G_S(\mathbb{Q}_\infty), E_{p^\infty}\big) \longrightarrow \bigoplus_{v\in S} J_v^i(\mathbb{Q}_\infty)$$

is surjective.

Proof. This follows as $J_v^i(\mathbb{Q}_\infty) = 0$ for $p \neq 2$ if v is an infinite prime. □

6.2. **The fundamental diagram.** We attempted to prove Conjecture 6.1 by studying the following commutative diagram, which we call *the fundamental diagram*.

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Sel}^i(E/L_\infty)^H & \longrightarrow & H^1(G_S(L_\infty), E_{p^\infty})^H & \longrightarrow & \bigoplus_{v\in S} J_v^i(L_\infty)^H \\
 & & \uparrow{\scriptstyle \alpha} & & \uparrow{\scriptstyle \beta} & & \uparrow{\scriptstyle \gamma = (\gamma_v)} \\
0 & \longrightarrow & \mathrm{Sel}^i(E/\mathbb{Q}_\infty) & \longrightarrow & H^1(G_S(\mathbb{Q}_\infty, E_{p^\infty}) & \longrightarrow & \bigoplus_{v\in S} J_v^i(\mathbb{Q}_\infty) \longrightarrow 0
\end{array}$$

where the J_v^i are as defined in Section 3.1. Applying the snake lemma gives a long exact sequence

$$0 \longrightarrow \ker(\alpha) \longrightarrow \ker(\beta) \longrightarrow \ker(\gamma) \longrightarrow \mathrm{coker}(\alpha) \longrightarrow \mathrm{coker}(\beta).$$

In order to prove Conjecture 6.1, it is therefore sufficient to show that the kernel and cokernel of the map β and the kernel of γ are cofinitely generated $\mathbb{Z}_p$-modules. The results for β and for γ_v, $v \nmid p$, are easy consequences of the inflation-restriction exact sequences (c.f. [CS00]).

The main difficulty is the study of the kernel of the local restriction map γ_v when $v \mid p$. Let K be the completion of L at such a prime, and write $\mathcal{H}$ for the Galois group $\mathrm{Gal}(K_\infty/\mathbb{Q}_{p,\infty})$. In order to prove Conjecture 6.1, we may use the local conditions from Section 4 and attempt to show that the kernel of the map

$$\frac{H^1(\mathbb{Q}_{p,\infty}, E_{p^\infty})}{\hat{E}_N^i(\mathcal{O}_{\mathbb{Q}_{p,\infty}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \longrightarrow \left(\frac{H^1(K_\infty, E_{p^\infty})}{\hat{E}_N^i(\mathcal{O}_{K_\infty}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}\right)^{\mathcal{H}}$$

is a cofinitely generated $\mathbb{Z}_p$-module. Consider the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \hat{E}^i_N(\mathcal{O}_{\mathbb{Q}_{p,\infty}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p & \longrightarrow & H^1(\mathbb{Q}_{p,\infty}, E_{p^\infty}) & \longrightarrow & \dfrac{H^1(\mathbb{Q}_{p,\infty}, E_{p^\infty})}{\hat{E}^i_N(\mathcal{O}_{\mathbb{Q}_{p,\infty}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \left(\hat{E}^i_N(\mathcal{O}_{K_\infty}) \otimes \mathbb{Q}_p/\mathbb{Z}_p\right)^{\mathcal{H}} & \longrightarrow & \left(H^1(K_\infty, E_{p^\infty})\right)^{\mathcal{H}} & \longrightarrow & \left(\dfrac{H^1(K_\infty, E_{p^\infty})}{\hat{E}^i_N(\mathcal{O}_{K_\infty}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}\right)^{\mathcal{H}} & & \end{array}$$

where the vertical maps are restrictions. The the first two maps are injective by Assumption 4.10. By the snake lemma, the kernel of the third map is bounded by the cokernel of the first, so it is sufficient to show that the cokernel of the restriction map

$$\hat{E}^i_N(\mathcal{O}_{\mathbb{Q}_{p,\infty}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \left(\hat{E}^i_N(\mathcal{O}_{K_\infty}) \otimes \mathbb{Q}_p/\mathbb{Z}_p\right)^{\mathcal{H}}$$

is a cofinitely generated $\mathbb{Z}_p$-module. By taking $\mathcal{H}$-cohomology of the short exact sequence

$$0 \longrightarrow \hat{E}^i_N(\mathcal{O}_{K_\infty}) \longrightarrow \hat{E}^i_N(\mathcal{O}_{K_\infty}) \otimes \mathbb{Q}_p \longrightarrow \hat{E}^i_N(\mathcal{O}_{K_\infty}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 0,$$

we may reduce the validity of Conjecture 6.1 to the following conjecture.

Conjecture 6.4. *The cohomological group $H^1\left(\mathcal{H}, \hat{E}^i_N(\mathcal{O}_{K_\infty})\right)$ is a cofinitely generated $\mathbb{Z}_p$-module.*

Note that it is shown in [CG96, Theorem 3.1] that $H^1\left(\mathcal{H}, \hat{E}(\mathcal{O}_{K_\infty})\right) = 0$. It therefore might be possible to prove Conjecture 6.4 by showing that an exact sequence similar to [Kob03, (8.22)] holds, e.g., to give a bound on the cokernel of the last map of

$$0 \longrightarrow \hat{E}(\mathcal{O}_{K_N}) \xrightarrow{x \mapsto x \oplus x} \hat{E}^1_N(\mathcal{O}_{K_\infty}) \oplus \hat{E}^2_N(\mathcal{O}_{K_\infty}) \xrightarrow{x \oplus y \mapsto x - y} \hat{E}(\mathcal{O}_{K_\infty}).$$

Unfortunately, this does not seem to be straightforward as far as we can see.

References

[Ber02] Laurent Berger, *Représentations p-adiques et équations différentielles*, Invent. Math. **148** (2002), no. 2, 219–284. MR 1906150

[Ber03] ———, *Bloch and Kato's exponential map: three explicit formulas*, Doc. Math. Extra Vol. **3** (2003), 99–129, Kazuya Kato's fiftieth birthday. MR 2046596

[Ber05] ———, *Représentations de de Rham et normes universelles*, Bull. Soc. Math. France **133** (2005), no. 4, 601–618. MR 2233697

[BK90] Spencer Bloch and Kazuya Kato, *L-functions and Tamagawa numbers of motives*, The Grothendieck Festschrift, Vol. I, Progr. Math., vol. 86, Birkhäuser Boston, Boston, MA, 1990, pp. 333–400. MR 1086888

[CC98] Frédéric Cherbonnier and Pierre Colmez, *Représentations p-adiques surconvergentes*, Invent. Math. **133** (1998), no. 3, 581–611. MR 1645070

[CC99] ———, *Théorie d'Iwasawa des représentations p-adiques d'un corps local*, J. Amer. Math. Soc. **12** (1999), no. 1, 241–268. MR 1626273

[CG96] J. Coates and R. Greenberg, *Kummer theory for abelian varieties over local fields*, Invent. Math. **124** (1996), no. 1-3, 129–174. MR 1369413

[CS00] J. Coates and R. Sujatha, *Galois cohomology of elliptic curves*, Tata Institute of Fundamental Research Lectures on Mathematics, 88, Published by Narosa Publishing House, New Delhi, 2000. MR 1759312 (2001b:11046)

[CH01] J. H. Coates and S. Howson, *Euler characteristics and elliptic curves. II*, J. Math. Soc. Japan **53** (2001), no. 1, 175–235.

[CFK+05] John Coates, Takako Fukaya, Kazuya Kato, Ramdorai Sujatha, and Otmar Venjakob, *The GL_2 main conjecture for elliptic curves without complex multiplication*, Publ. Math. Inst. Hautes Études Sci. **101** (2005), 163–208. MR 2217048

[Her98] Laurent Herr, *Sur la cohomologie galoisienne des corps p-adiques*, Bull. Soc. Math. France **126** (1998), no. 4, 563–600. MR 1693457

[Kob03] Shin-ichi Kobayashi, *Iwasawa theory for elliptic curves at supersingular primes*, Invent. Math. **152** (2003), no. 1, 1–36. MR 1965358

[LLZ10] Antonio Lei, David Loeffler, and Sarah Livia Zerbes, *Wach modules and Iwasawa theory for modular forms*, to appear in Asian J. Math., 2010, `arXiv:0912.1263`.

[PR95] Bernadette Perrin-Riou, *Fonctions L p-adiques des représentations p-adiques*, Astérisque **229** (1995), 1–198. MR 1327803

[PR00] ———, *Représentations p-adiques et normes universelles. I. Le cas cristallin*, J. Amer. Math. Soc. **13** (2000), no. 3, 533–551 (electronic). MR 1758753 (2001g:11183)

[Wac96] Nathalie Wach, *Représentations p-adiques potentiellement cristallines*, Bull. Soc. Math. France **124** (1996), no. 3, 375–400.

(Lei) School of Mathematical Sciences, Monash University, Clayton, VIC 3800, Australia
E-mail address: `antonio.lei@monash.edu`

(Zerbes) Department of Mathematics, Harrison Building, University of Exeter, Exeter EX4 4QF, UK
E-mail address: `s.zerbes@exeter.ac.uk`