ON SELMER GROUPS IN THE SUPERSINGULAR REDUCTION CASE

ANTONIO LEI AND R. SUJATHA

ABSTRACT. Let p be a fixed odd prime. Let E be an elliptic curve defined over a number field F with good supersingular reduction at all primes above p. We study both the classical and plus/minus Selmer groups over the cyclotomic $\mathbb{Z}_p$-extension of F. In particular, we give sufficient conditions for these Selmer groups to not contain a non-trivial sub-module of finite index. Furthermore, when p splits completely in F, we calculate the Euler characteristics of the plus/minus Selmer groups over the compositum of all $\mathbb{Z}_p$-extensions of F when they are defined.

1. INTRODUCTION

The theory of Galois representations for the absolute Galois group of a number field F plays a central role in Arithmetic Geometry. Two important examples that have been studied in depth are the Galois representations associated to an elliptic curve E defined over F (see [33]) and those arising from elliptic modular forms that originated in the results due to Eichler, Shimura, Deligne and Serre (see [11]). There is a well-defined notion of these Galois representations being ordinary at a prime number p (see [12]), which for simplicity we assume to be odd in this article. Iwasawa theory then intervenes effectively thereby enabling a deeper study that provides arithmetic information associated to the Galois representations. The important objects of study in this situation are the Selmer groups associated to the Galois representations when they have good ordinary reduction at an odd prime p. A central conjecture due to Mazur [28] in the case of p-ordinary elliptic curves, states that the dual Selmer group of the elliptic curve over the cyclotomic $\mathbb{Z}_p$-extension is finitely generated and torsion over the corresponding Iwasawa algebra. A generalised form of this conjecture is believed to be true for the Selmer groups of the Galois representation associated to modular forms as well, when the representation is ordinary at p (which is equivalent to the p-th Fourier coefficient of the modular form being a p-adic unit). Kato showed in [19] that this conjecture holds when $F/\mathbb{Q}$ is an abelian extension. Extensions of Mazur's conjecture on the dual Selmer group being torsion over the cyclotomic extension have been studied over other Galois extensions F_∞ of F whose Galois group $\mathrm{Gal}(F_\infty/F)$ is a p-adic Lie group. The main tools in these cases are Iwasawa theoretic in nature. It is

known that Mazur's conjecture on the dual Selmer group being a torsion module over the corresponding Iwasawa algebra is equivalent to the defining sequence for the Selmer group being short exact (see [15, Proposition 2.3]). This equivalence can also be generalised to the Iwasawa theoretic study over other p-adic Lie extensions. This in turn enables us to study the Galois cohomology of the Selmer group over the corresponding Iwasawa algebra (see [7]) as well as the Euler characteristic of the Selmer group, when it is defined (see [9]).

We now turn to the case when the elliptic curve has supersingular reduction at all the primes of F above p and consider the Selmer group over the cyclotomic $\mathbb{Z}_p$-extension F_{cyc} of F. The dual Selmer group over the cyclotomic extension, which is still finitely generated over the corresponding Iwasawa algebra is then far from being torsion, and is conjectured to have positive rank ([9, Conjecture 2.5]). Nevertheless, it is pertinent to ask whether the corresponding global to local map in the defining sequence for the Selmer group is exact. All these can be suitably extended to the Galois representation arising from elliptic modular forms, and these questions are investigated in this paper. In the last couple of decades, there are important subgroups of the Selmer groups, which we simply refer to as the 'signed Selmer groups' that have been defined by Kobayashi in [23] and later studied by various authors notably by Kim, Kitajima, Otsuki et al under the assumption that $a_p(E) = 0$ (see [21, 20, 22, 18, 24, 25, 26]). These Selmer groups exhibit properties remarkably similar to the Selmer groups in the ordinary case and results on their Galois cohomology and Euler characteristic are known ([20, Theorem 1.2]). When $a_p(E) \neq 0$, Sprung has defined and extensively studied similar Selmer groups in [36, 35]. In the present paper, we concentrate on the $a_p(E) = 0$ case, whenever we study the signed Selmer groups, for simplicity.

Our main results in this paper study the Selmer groups (see Theorem 2.14) and the signed Selmer groups in the supersingular case (see Theorem 4.8) along the lines undertaken in [9] for the ordinary case. Surprisingly, this lens affords simpler proofs of known results and makes the Galois cohomological study of the Selmer groups more explicit. Additionally, we consider the p-adic Lie extension F_∞ defined as the compositum of all $\mathbb{Z}_p$-extensions of F under the assumption that p splits completely in F. Our techniques make it possible to study the Galois cohomology of the signed Selmer groups over this extension and compute their Euler characteristics (see Theorem 5.15 below) in the case of elliptic curves. Thus this paper is largely a generalisation of the work in [9] from the case of ordinary reduction to that of supersingular reduction. Apart from studying the analogues to the representations associated to modular forms (see Theorem 3.5), our methods provide different and simpler proofs in the supersingular case, as well as the computation of the Euler characteristic over a larger p-adic Lie extension in a unified framework.

The paper consists of five sections including this introductory section. In section 2, we introduce and study the Galois cohomology of the Selmer groups of elliptic curves in the supersingular case. In section 3, we frame an analogous study for the representations arising from elliptic modular forms and prove results in that context. In section 4, we introduce the signed Selmer groups in the case of elliptic

curves under the assumption that p is unramified in F and study their Galois cohomology. In all three instances, we study the Selmer groups over F_{cyc} and give sufficient conditions for the Selmer groups to not contain a non-trivial sub-module of finite index. In section 5, we assume that p splits completely in F and consider the larger p-adic Lie extension F_∞ obtained as the compositum of all $\mathbb{Z}_p$-extensions of F. We compute the Euler characteristic of the signed Selmer group over this extension when they are defined. The reason that we restrict our study to the case of elliptic curves in sections 4 and 5 is that the theory of signed Selmer groups for modular forms in the non-ordinary case are not very well understood. We hope that our approach might be helpful towards understanding how the results can be extended to modular forms and hope to return to this subject in a subsequent paper.

Since the present paper was submitted, we learnt that Ahmed and Lim [1] independently studied the Euler characteristics of mixed-signed Selmer groups of an elliptic curve. They concentrated on signed Selmer groups over the cyclotomic $\mathbb{Z}_p$-extension of a number field. It would be interesting to investigate whether one may combine our work with theirs to study mixed-signed Selmer groups of elliptic curves over the compositum of all $\mathbb{Z}_p$-extensions of a number field.

2. Galois cohomology of the Selmer group

In this section, we study the Selmer group of an elliptic curve and the Galois cohomology of the Selmer group. Let E be an elliptic curve defined over a number field F. It is assumed throughout that E has supersingular reduction at all the primes of F lying above the odd prime p. Let S be the finite set of primes of F lying over p and the set of primes where E has bad reduction. Let F_S denote the maximal extension of F unramified outside S. For any finite extension L of F, and a prime v of L, the groups $J_v(E/L)$ are defined as follows:

$$J_v(E/L) = \bigoplus_{w|v} H^1(L_w, E)(p) \tag{2.1}$$

where the direct sum is taken over all primes w of L lying above the prime v of F. For an infinite extension $\mathcal{L}$ of F, we define

$$J_v(E/\mathcal{L}) = \varinjlim J_v(E/L), \tag{2.2}$$

where the inductive limit is taken over finite extensions L of F inside $\mathcal{L}$. The (p-adic) Selmer group of E over a finite extension L denoted $\mathrm{Sel}_p(E/L)$ is defined as the kernel of the natural map

$$\lambda_L : H^1(F_S/L, E_{p^\infty}) \longrightarrow \bigoplus_{v \in S} J_v(E/L). \tag{2.3}$$

For an infinite extension $\mathcal{L}$ of F, the Selmer group $\mathrm{Sel}_p(E/\mathcal{L})$ is defined by taking the direct limits of $\mathrm{Sel}_p(E/L)$ as L varies over finite extensions L in $\mathcal{L}$. If $\mathcal{L}$ is contained in F_S, there is an exact sequence

$$0 \to \mathrm{Sel}_p(E/\mathcal{L}) \to H^1(F_S/\mathcal{L}, E_{p^\infty}) \xrightarrow{\lambda_{\mathcal{L}}} \bigoplus_{v \in S} J_v(E/\mathcal{L}). \tag{2.4}$$

Let us first consider the case when $\mathcal{L}$ is the cyclotomic $\mathbb{Z}_p$-extension F_{cyc} of F, with $\Gamma := \mathrm{Gal}(F_{\mathrm{cyc}}/F)$. Denote the map $\lambda_{F_{\mathrm{cyc}}}$ occurring in (2.4) by λ_{cyc}. Let $X(E/F_{\mathrm{cyc}})$ be the Pontryagin dual of $\mathrm{Sel}_p(E/F_{\mathrm{cyc}})$. Then $X(E/F_{\mathrm{cyc}})$ is a finitely generated module over the Iwasawa algebra $\Lambda(\Gamma) := \mathbb{Z}_p[[\Gamma]]$. When E has good ordinary reduction at all the primes of F above p, under the hypothesis that $\mathrm{Sel}_p(E/F)$ is finite, the Γ-Euler characteristic of $\mathrm{Sel}_p(E/F_{\mathrm{cyc}})$ has been studied in the context of its relation to the exact formula for the L-value predicted by the Birch and Swinnerton-Dyer conjecture. Further, $X(E/F_{\mathrm{cyc}})$ being $\Lambda(\Gamma)$-torsion is equivalent to the surjectivity of the map λ_{cyc} occurring in (2.4). Another important result that plays a key role in computing the Euler characteristic is the vanishing of $H_1(\Gamma, X(E/F_{\mathrm{cyc}}))$ under certain additional hypothesis (see [9, Theorem 3.11]).

The big difference in the case when E has supersingular reduction at the primes of F above p is that $X(E/F_{\mathrm{cyc}})$ is no longer torsion as a $\Lambda(\Gamma)$-module, even though it is finitely generated. Nevertheless, in this section, we prove that $H_1(\Gamma, X(E/F_{\mathrm{cyc}}))$ vanishes under the assumption that the map λ_{cyc} is surjective and

$$H^2(F_S/F, E_{p^\infty}) = 0, \qquad (2.5)$$

which can be considered as the analogue of the Leopoldt Conjecture on number fields for E_{p^∞} over F. Furthermore, this is equivalent to the finiteness of the fine Selmer group of E over F as defined in [8] (see [14, Lemma 3.2]; we thank Meng Fai Lim for reminding us of this fact).

Remark 2.1. *The equation* (2.5) *holds when both $E(F)$ and $\Sha(E/F)(p)$ are finite, as shown in* [9, Proposition 1.9].

Our proof surprisingly follows the arguments in [9] for the ordinary reduction case and is rendered simpler in the supersingular case. It involves a detailed analysis of the so called fundamental diagram (2.6) below that is used in proving control theorems in Iwasawa theory.

$$
\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Sel}_p(E/F_{\mathrm{cyc}})^\Gamma & \longrightarrow & H^1(F_S/F_{\mathrm{cyc}}, E_{p^\infty})^\Gamma & \xrightarrow{\lambda_{\mathrm{cyc}}^\Gamma} & \bigoplus_{v \in S} J_v(E/F_{\mathrm{cyc}})^\Gamma \\
& & \alpha \uparrow & & \beta \uparrow & & \gamma = \oplus \gamma_v \uparrow \\
0 & \longrightarrow & \mathrm{Sel}_p(E/F) & \longrightarrow & H^1(F_S/F, E_{p^\infty}) & \xrightarrow{\lambda} & \bigoplus_{v \in S} J_v(E/F).
\end{array}
$$
$$(2.6)$$

This diagram gives a natural map

$$\delta : \ker\gamma \to \mathrm{Coker}\,\lambda \qquad (2.7)$$

and analysing this map is important in proving the surjectivity of λ. We begin by collecting a few lemmas.

Lemma 2.2. *In the diagram* (2.6) *above, the map β is surjective and has finite kernel.*

Proof. The assertion follows from an easy application of the Hochschild-Serre spectral sequence and noting that the p-cohomological dimension of Γ is one. Indeed, the kernel of β is isomorphic to $H^1(\Gamma, E_{p^\infty}(F_{\mathrm{cyc}}))$ and this group is finite since $E_{p^\infty}(F_{\mathrm{cyc}})$ is finite, by a theorem of Imai [17]. From the Hochschild-Serre spectral sequence, it follows that the cokernel of β is isomorphic to $H^2(\Gamma, E_{p^\infty}(F_{\mathrm{cyc}}))$ which is zero as Γ has p-cohomological dimension one. $\qquad\square$

Remark 2.3. *When p is unramified over F, then* [23, Proposition 8.7] *shows that $E_{p^\infty}(F_{\mathrm{cyc}}) = 0$. In particular, β is in fact an isomorphism.*

Lemma 2.4. *In the diagram* (2.6) *above, the map γ is surjective. Furthermore, $\bigoplus_{v|p} J_v(E/F) \subset \ker\gamma$ and the containment is of finite index.*

Proof. When $v \nmid p$, it is shown in [9, Lemma 1.11] that $J_v(E/F) = H^1(F_v, E_{p^\infty})$ is finite, so $\ker\gamma_v$ is finite. The surjectivity of γ_v is once again a consequence of the Hochschild-Serre spectral sequence and the fact that the p-cohomological dimension of Γ is one.

Let us now consider the case $v|p$. Let w be any prime of F_{cyc} above v and write $\hat{E}$ for the formal group attached to E at this prime. Since E is supersingular at w, we have $E_{p^\infty}(F_{\mathrm{cyc},w}) = \hat{E}_{p^\infty}(F_{\mathrm{cyc},w})$. In particular, we have

$$H^1(F_{\mathrm{cyc},w}, E)(p) \cong \frac{H^1(F_{\mathrm{cyc},w}, E_{p^\infty})}{E(F_{\mathrm{cyc},w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} = \frac{H^1(F_{\mathrm{cyc},w}, \hat{E}_{p^\infty})}{\hat{E}(F_{\mathrm{cyc},w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}.$$

The last quotient is zero by [5, Proposition 4.3]. Alternatively, we may consider the Pontryagin dual of $H^1(F_{\mathrm{cyc},w}, E)(p)$, which is given by the universal norm $\varprojlim_L \hat{E}(L)$, where L runs through finite extensions of F_v contained inside $F_{\mathrm{cyc},w}$. This inverse limit is zero by [32, Theorem 2]. In particular, γ_v is surjective and $\ker\gamma_v = J_v(E/F)$. $\qquad\square$

Remark 2.5. *The proof of Lemma 2.4 tells us that*

$$\bigoplus_{v\in S} J_v(E/F_{\mathrm{cyc}}) = \bigoplus_{v\in S, v\nmid p} J_v(E/F_{\mathrm{cyc}}) = \bigoplus_{w|v\in S, v\nmid p} H^1(F_{\mathrm{cyc},w}, E_{p^\infty}).$$

Proposition 2.6. *Suppose that λ_{cyc} in* (2.4) *(with $\mathcal{L} = F_{\mathrm{cyc}}$) is surjective. If $H^2(F_S/F, E_{p^\infty}) = 0$, then the following are equivalent:*

(i) The map $\lambda_{\mathrm{cyc}}^\Gamma$ in (2.6) *is surjective;*
(ii) $H^1(\Gamma, \mathrm{Sel}_p(E/F_{\mathrm{cyc}})) = 0$;
(iii) The map δ in (2.7) *is surjective.*

Proof. The assumption $H^2(F_S/F, E_{p^\infty}) = 0$, together with the Hochschild-Serre spectral sequence imply that

$$H^1(\Gamma, H^1(F_S/F_{\mathrm{cyc}}, E_{p^\infty})) = 0$$

(c.f. [9, Equation (33)]). Therefore, the equivalence of (i) and (ii) follows from the Γ-Galois cohomology exact sequence attached to the short exact sequence

$$0 \to \mathrm{Sel}_p(E/F_{\mathrm{cyc}}) \to H^1(F_S/F_{\mathrm{cyc}}, E_{p^\infty}) \to \bigoplus_{v\in S} J_v(E/F_{\mathrm{cyc}}) \to 0.$$

$(i) \Rightarrow (iii)$: Consider the following commutative diagram:

$$
\begin{array}{ccc}
H^1(F_S/F_{\mathrm{cyc}}, E_{p^\infty})^\Gamma & \xrightarrow{\lambda_{\mathrm{cyc}}^\Gamma} & \bigoplus_{v\in S} J_v(E/F_{\mathrm{cyc}})^\Gamma \\
\beta \uparrow & & \gamma \uparrow \\
H^1(F_S/F, E_{p^\infty}) & \xrightarrow{\lambda} & \bigoplus_{v\in S}(J_v(E/F)) \longrightarrow \mathrm{Coker}\lambda \longrightarrow 0.
\end{array}
\tag{2.8}
$$

Lemmas 2.2 and 2.4 say that β and γ are surjective. In particular, $\lambda_{\mathrm{cyc}}^\Gamma \circ \beta = \gamma \circ \lambda$ is surjective under condition (i). By a simple diagram chase, there is a short exact sequence

$$
\ker\gamma \xrightarrow{\delta} \mathrm{Coker}\lambda \longrightarrow \mathrm{Coker}(\gamma \circ \lambda) \longrightarrow \mathrm{Coker}\gamma = 0,
\tag{2.9}
$$

where the vanishing of $\mathrm{Coker}\gamma$ is given by Lemma 2.4. Hence, δ is surjective and (iii) holds.

$(iii) \Rightarrow (i)$ If δ is surjective, then the surjectivity of γ implies that $\gamma \circ \lambda$ is surjective. Hence, $\lambda_{\mathrm{cyc}}^\Gamma$ is also surjective by the commutative diagram (2.8). $\qquad\square$

The following proposition is a partial converse to the above proposition.

Proposition 2.7. *Assume $H^2(F_S/F, E_{p^\infty}) = 0$. With notation as before, suppose that the map $\lambda_{\mathrm{cyc}}^\Gamma$ in (2.6) is surjective. Then the map λ_{cyc} is surjective and $H^1(\Gamma, \mathrm{Sel}_p(E/F_{\mathrm{cyc}})) = 0$.*

Proof. Put $\mathrm{Im}_{\mathrm{cyc}} = \mathrm{Im}(\lambda_{\mathrm{cyc}})$. The sequence (2.4) gives the two short exact sequences

$$
0 \longrightarrow \mathrm{Sel}_p(E/F_{\mathrm{cyc}}) \longrightarrow H^1(F_S/F_{\mathrm{cyc}}, E_{p^\infty}) \xrightarrow{\lambda_{\mathrm{cyc}}} \mathrm{Im}_{\mathrm{cyc}} \longrightarrow 0
$$

$$
0 \longrightarrow \mathrm{Im}_{\mathrm{cyc}} \longrightarrow \bigoplus_{v\in S} J_v(E/F_{\mathrm{cyc}}) \longrightarrow \mathrm{Coker}\lambda_{\mathrm{cyc}} \longrightarrow 0.
\tag{2.10}
$$

The long exact Γ-Galois cohomology sequence associated to the first sequence, along with the Hochschild-Serre spectral sequence gives $H^1(\Gamma, \mathrm{Im}_{\mathrm{cyc}}) = 0$. Using this in the long exact Γ-cohomology sequence of the second short exact sequence in (2.10), it follows that the natural map

$$
\left(\bigoplus_{v\in S} J_v(E/F_{\mathrm{cyc}}) \right)^\Gamma \to (\mathrm{Coker}(\lambda_{\mathrm{cyc}}))^\Gamma
$$

is surjective. Consider the natural commutative diagram below

$$
\begin{array}{ccc}
H^1(F_S/F_{\mathrm{cyc}}, E_{p^\infty})^\Gamma & \longrightarrow & (\mathrm{Im}_{\mathrm{cyc}})^\Gamma \\
& \searrow & \downarrow \\
& & \left(\bigoplus_{v\in S} J_v(E/F_{\mathrm{cyc}}) \right)^\Gamma.
\end{array}
\tag{2.11}
$$

From the two Γ-Galois cohomology sequences associated to the two short exact sequences in (2.10), the vertical arrow is injective and the cokernel of the horizontal arrow is $H^1(\Gamma, \mathrm{Sel}_p(E/F_{\mathrm{cyc}}))$. Further, under the hypothesis of the surjectivity of $\lambda_{\mathrm{cyc}}^\Gamma$, we conclude that the vertical arrow in (2.11) is an isomorphism. In particular, the horizontal map is surjective whence clearly

$$
\mathrm{Coker}(\lambda_{\mathrm{cyc}})^\Gamma = 0, \quad \text{and} \quad H^1(\Gamma, \mathrm{Sel}_p(E/F_{\mathrm{cyc}})) = 0.
\tag{2.12}
$$

In particular, $\mathrm{Coker}(\lambda_{\mathrm{cyc}}) = 0$ by Nakayama's lemma, which proves the surjectivity of λ_{cyc}. $\qquad\square$

Corollary 2.8. *Assume that $H^2(F_S/F, E_{p^\infty}) = 0$ and that $\mathrm{III}(E/F)(p)$ is finite. Then the surjectivity of δ is equivalent to the injectivity of*

$$E(F)^* \to \bigoplus_{v|p} E(F_v)^* \oplus \bigoplus_{v\nmid p} E_{p^\infty}(F_{\mathrm{cyc},v})_{\Gamma_v}, \qquad (2.13)$$

where M^* denotes the p-adic completion $\varprojlim M/p^n$ for an abelian group M.

Proof. The proof is along similar lines of the arguments in the orrdinary case considered in [9]. It follows from the proof of Proposition 1.9 in [9] that $\mathrm{Coker}\,\lambda$ is isomorphic to the Pontryagin dual $\widehat{E(F)^*}$ of $E(F)^*$. By Lemma 2.4, we have

$$\ker \gamma = \bigoplus_{v|p} J_v(E/F) \oplus \bigoplus_{v\nmid p} \ker \gamma_v. \qquad (2.14)$$

For $v|p$, local Tate duality implies that

$$\widehat{J_v(E/F)} = E(F_v)^*.$$

For $v \nmid p$, the Hochschild-Serre spectral sequence says that

$$\ker \gamma_v = H^1(\Gamma_v, E_{p^\infty}(F_{\mathrm{cyc},v})) = E_{p^\infty}(F_{\mathrm{cyc},v})_{\Gamma_v},$$

where the second equality is a consequence of the fact that Γ_v is pro-cyclic. Thus the dual of δ may be written as

$$\widehat{\delta} \,:\, E(F)^* \to \bigoplus_{v|p} E(F_v)^* \oplus \bigoplus_{v\nmid p} E_{p^\infty}(F_{\mathrm{cyc},v})_{\Gamma_v}.$$

By duality, the surjectivity of δ is equivalent to the injectivity of $\widehat{\delta}$. The result now follows. $\qquad\square$

Corollary 2.9. *Suppose that E satisfies the following hypotheses:*

(i) $\mathrm{III}(E/F)(p)$ is finite;
(ii) The Mordell-Weil rank of E/F is ≤ 1.

Then λ_{cyc} is surjective, $H^2(F_S/F, E_{p^\infty}) = 0$ and the equivalent conditions in Proposition 2.6 hold.

Proof. By the same proof of Theorem 12 in [6] (where the authors worked over $\mathbb{Q}$ instead of a general number field F), (i) and (ii) imply that $H^2(F_S/F, E_{p^\infty}) = 0$.

Since the Mordell-Weil rank of E/F is assumed to be ≤ 1, the quotient $E(F)^*$ is either $E_{p^\infty}(F)$ or $E_{p^\infty}(F) \oplus \mathbb{Z}_p \cdot P$ for some non-torsion $P \in E(F)$. Consequently, the localization map $E(F)^* \to E(F_v)^*$ is an injection for any $v|p$ (see also [6, Lemma 8]). In particular, the map in (2.13) has to be injective.

We can now apply Corollary 2.8, which tells us that δ is surjective. By (2.9), $\gamma \circ \lambda$ is also surjective. In particular, $\lambda_{\mathrm{cyc}}^\Gamma$ in (2.6) is surjective. Proposition 2.7 gives the surjectivity of λ_{cyc}. Proposition 2.6 now applies. $\qquad\square$

We now give a sufficient condition for the surjectivity of λ_{cyc}.

Lemma 2.10. *If the localization map*

$$\mathrm{loc} : \varprojlim_n H^1(F_S/F_n, T_p(E)) \to \bigoplus_{v|p} \varprojlim_n H^1(F_{n,v}, T_p(E))$$

is injective. Then λ_{cyc} is surjective.

Proof. The description of $J_v(E/F_{\mathrm{cyc}})$ in Remark 2.5 gives the following Poitou-Tate exact sequence

$$0 \to \mathrm{Sel}_p(E/F_{\mathrm{cyc}}) \to H^1(F_S/F_{\mathrm{cyc}}, E_{p^\infty}) \to \bigoplus_{v\in S} J_v(E/F_{\mathrm{cyc}}) \to \widehat{\ker \mathrm{loc}},$$

from which the result follows. $\qquad\square$

Remark 2.11. *When $F = \mathbb{Q}$, the injectivity of the localization map in Lemma 2.10 has been established by Kobayashi [23, Theorem 7.3].*

Remark 2.12. *We shall see in §4 that it is possible to deduce the surjectivity of λ_{cyc} from the theory of plus/minus Selmer groups when the latter are defined. See in particular Lemma 4.6 below.*

Another sufficient condition for the surjectivity of λ_{cyc} is the finiteness of $\mathrm{Sel}_p(E/F)$.

Proposition 2.13. *Suppose that $\mathrm{Sel}_p(E/F)$ is finite, then λ_{cyc} is surjective.*

Proof. Recall from [9, proof of Proposition 3.9] that the finiteness of $\mathrm{Sel}_p(E/F)$ implies the surjectivity of the map

$$\lambda'_{\mathrm{cyc}} : H^1(F_S/F, E_{p^\infty}) \to \bigoplus_{v\in S, v\nmid p} J_v(F_{\mathrm{cyc}}).$$

But λ'_{cyc} coincides with λ_{cyc} by Remark 2.5. Hence the result. $\qquad\square$

Theorem 2.14. *Let E be an elliptic curve over F such that the following hypotheses are satisfied:*

(i) E has supersingular reduction at all the primes v of F lying above p.
(ii) The map λ_{cyc} in (2.4) (with $\mathcal{L} = F_{\mathrm{cyc}}$) is surjective.
(iii) $H^2(F_S/F, E_{p^\infty}) = 0$.
(iv) The equivalent conditions in Proposition 2.6 and Corollary 2.8 hold.

Then the $\Lambda(\Gamma)$-module $X(E/F_{\mathrm{cyc}})$ admits no non-trivial finite sub-module.

Proof. The hypotheses implies that

$$H_1(\Gamma, X(E/F_{\mathrm{cyc}})) = 0$$

by duality. The result now follows from [9, Lemma A.1.5]. $\qquad\square$

Remark 2.15. *In [13, Proposition 4.1.1], Greenberg has given sufficient conditions for $X(E/F_{\mathrm{cyc}})$ to contain no non-trivial finite sub-module. It is thus possible to obtain an alternative proof to Theorem 2.14 under different hypotheses. Indeed, our hypothesis on the surjectivity of λ_{cyc} implies the condition labelled $\mathrm{CRK}(\mathcal{D}, \mathcal{L})$ in loc. cit., which says that*

$$\mathrm{rank}_\Lambda \widehat{\mathrm{Sel}_p(E/F_{\mathrm{cyc}})} + \mathrm{rank}_\Lambda \bigoplus_{v\in S} \widehat{J_v(E/F_{\mathrm{cyc}})} = \mathrm{rank}_\Lambda \widehat{H^1(F_S/F_{\mathrm{cyc}}, E_{p^\infty})}.$$

The hypothesis $\mathrm{RFX}(\mathcal{D})$, *which asserts that* $T_p(E) \otimes \Lambda$ *is a reflexive* Λ-*module, holds unconditionally. Under the weak Leopoldt conjecture, i.e.* $H^2(F_S/F_{\mathrm{cyc}}, E_{p^\infty}) = 0$, *Greenberg's hypothesis* $\mathrm{LEO}(\mathcal{D})$, *which says that the kernel of the localization map*

$$H^2(F_S/F_{\mathrm{cyc}}, E_{p^\infty}) \to \bigoplus_{v \in \Sigma, w|v} H^2(F_{\mathrm{cyc},w}, E_{p^\infty})$$

is Λ-*cotorsion, holds trivially. Therefore,* [13, Proposition 4.1.1] *applies if we further assume*

- $\mathrm{LOC}_v^{(1)}(\mathcal{D})$ *holds for some non-archimedian prime* v, *that is,* $(T_p(E) \otimes \Lambda)^{G_{F_v}} = 0$;
- $\mathrm{LOC}_v^{(2)}(\mathcal{D})$ *holds for all* $v \in S$, *that is, the* Λ-*module* $T_p(E) \otimes \Lambda / (T_p(E) \otimes \Lambda)^{G_{F_v}}$ *is reflexive;*
- *One of the following conditions holds:*
  - (a) $E[p]$ *has no quotient isomorphic to* μ_p *as a* G_F-*module;*
  - (b) *There exists* $v \in S$ *such that* $\mathrm{LOC}_v^{(1)}(\mathcal{D})$ *holds and* $J_v(\widehat{E/F_{\mathrm{cyc}}})$ *is a reflexive* Λ-*module.*

3. Modular forms

Let $f = \sum a_n q^n \in S_k(\Gamma_0(N), \epsilon)$ be a normalized new cuspidal modular eigenform of level N. Assume that $(p, N) = 1$. Let E be the subfield of the complex numbers obtained by adjoining the Fourier coefficients of f to $\mathbb{Q}$. It is well known that E is a number field, and we denote its ring of integers by $\mathcal{O}$. For each prime l, let

$$\mathcal{O}_l = \mathcal{O} \otimes \mathbb{Z}_l, \quad E_l = E \otimes \mathbb{Q}_l$$

so that $\mathcal{O}_l$ is the product of the completions $\mathcal{O}_\lambda$ of $\mathcal{O}$ at the primes λ of $\mathcal{O}$ dividing l. Similarly E_l is the product of the corresponding completions E_λ. By the results of Eichler, Shimura, Deligne, there is a system of l-adic Galois representation

$$\rho_f : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathcal{O}_l) \subset \mathrm{GL}_2(E_l) \tag{3.1}$$

of $G_{\mathbb{Q}}$ attached to f (see [11], also [31] and [19, §8.3]). For simplicity, we denote by V_f the corresponding 2-dimensional representation over E_λ, where λ is a fixed prime of E above p, and we fix a two dimensional lattice T_f of V_f so that T_f is a free $\mathcal{O}_\lambda$-module of rank two. The representation is crystalline, with Hodge-Tate weights 0 and $1 - k$. We assume that V_f is non-ordinary, that is $a_p \in \lambda$.

Fix an integer $j \in [1, k-1]$ and write $T = T_f(j)$, $V = V_f(j)$. The corresponding divisible module V/T is denoted by A, and A is isomorphic to two copies of $E_\lambda/\mathcal{O}_\lambda$ equipped with a $G_{\mathbb{Q}}$-action. There is a tautological short exact sequence

$$0 \to T \xrightarrow{\iota} V \xrightarrow{\pi} A \to 0. \tag{3.2}$$

Given a number field L and v a place of L, we recall that Bloch and Kato [4] defined the canonical subgroups

$$H_f^1(L_v, V) := \begin{cases} \ker\left(H^1(L_v, V) \to H^1(L_v, V \otimes \mathbb{B}_{\mathrm{cris}})\right) & v|p, \\ \ker\left(H^1(L_v, V) \to H^1(L_v^{\mathrm{ur}}, V)\right) & v \nmid p, \end{cases}$$

9

where L_v^{ur} denotes the maximal unramified extension of L_v and

$$H_f^1(L_v, T) := \iota^* \left(H_f^1(L_v, V) \right);$$
$$H_f^1(L_v, A) := \pi_* \left(H_f^1(L_v, V) \right).$$

If q is a rational prime, we write

$$J_q(A/L) = \bigoplus_{v|q} \frac{H^1(L_v, A)}{H_f^1(L_v, A)},$$

where the direct sum is taken over all primes of L over q. If $\mathcal{L}$ is an infinite extension of $\mathbb{Q}$, we define

$$J_q(A/\mathcal{L}) = \varinjlim J_q(A/L),$$

where the inductive limit is taken over number fields L that are contained inside $\mathcal{L}$.

Let S be the set of primes dividing pN. We have the Selmer group sitting inside the following exact sequence

$$0 \to \mathrm{Sel}(A/\mathcal{L}) \to H^1(\mathcal{L}_S/\mathcal{L}, A) \xrightarrow{\lambda_{\mathcal{L}}} \bigoplus_{v \in S} J_v(A/\mathcal{L}). \tag{3.3}$$

Fix a number field F and let F_{cyc} be the cyclotomic $\mathbb{Z}_p$-extension of F as before. Throughout, we assume that the analogue of (2.5) holds for A over F, namely

$$H^2(F_S/F, A) = 0. \tag{3.4}$$

Similar to (2.6), we have the following fundamental diagram:

$$
\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Sel}(A/F_{\mathrm{cyc}})^{\Gamma} & \longrightarrow & H^1(F_S/F_{\mathrm{cyc}}, A)^{\Gamma} & \xrightarrow{\lambda_{\mathrm{cyc}}^{\Gamma}} & \bigoplus_{v \in S} J_v(A/F_{\mathrm{cyc}})^{\Gamma} \\
& & \alpha \uparrow & & \beta \uparrow & & \gamma = \oplus \gamma_v \uparrow \qquad (3.5) \\
0 & \longrightarrow & \mathrm{Sel}(A/F) & \longrightarrow & H^1(F_S/F, A) & \xrightarrow{\lambda} & \bigoplus_{v \in S} J_v(A/F).
\end{array}
$$

As in (2.7), this diagram gives rise to a natural map

$$\delta : \ker\gamma \to \mathrm{Coker}\,\lambda. \tag{3.6}$$

Lemma 3.1. *In the diagram (3.5) above, the map β is surjective and has finite kernel.*

Proof. As in Lemma 2.2, the surjectivity is a consequence of Hochschild-Serre. The finiteness of $\ker\beta$ is proven in [34, Lemma 2.2]. $\qquad\square$

Below is a generalization of Lemma 2.4.

Lemma 3.2. *In the diagram (3.5) above, the map γ is surjective. Furthermore, $J_p(A/F) \subset \ker\gamma$ and the containment is of finite index.*

10

Proof. For $v \nmid p$, the finiteness of $\ker \gamma_v$ is studied in [16, proof of Proposition 3.3]. If $w|p$ is a place of F_{cyc}, Perrin-Riou and Berger showed that $\varprojlim\limits_{L \subset F_{\mathrm{cyc},w}} H^1_f(L,T) = 0$ (see [30, 3]), which generalizes the vanishing of the universal norm for supersingular elliptic curves. Therefore, if we replace $\hat{E}(L)$ by $H^1_f(L,T)$, the proof of Lemma 2.4 generalizes to the setting of modular forms. □

The analogue of Proposition 2.6 holds.

Proposition 3.3. *Suppose that λ_{cyc} in (3.3) (with $\mathcal{L} = F_{\mathrm{cyc}}$) is surjective. If $H^2(F_S/F, A) = 0$, then the following are equivalent:*

(i) $\lambda^\Gamma_{\mathrm{cyc}}$ in (3.5) is surjective;
(ii) $H^1(\Gamma, \mathrm{Sel}(A/F_{\mathrm{cyc}})) = 0$;
(iii) The map δ in (3.6) is surjective.

We prove a sufficient condition for the equivalent conditions in Proposition 3.3.

Lemma 3.4. *Let $T^* = \mathrm{Hom}(T, \mathcal{O}_\lambda)$ denote the linear dual of T and define*

$$\mathrm{III}_p(T^*(1)/F) := \ker \left(H^1(F, T^*(1)) \to \prod_{v|p} H^1(F_v, T^*(1)) \right).$$

Suppose that the the following hypotheses hold for f and F.

i) $\mathrm{III}_p(T^*(1)/F) = 0$.
ii) $H^2(F_S/F, A) = 0$.

Then the map δ in (3.6) is surjective.

Proof. On the one hand, the Poitou-Tate exact sequence and (3.4) imply that

$$\widehat{\mathrm{Coker}\lambda} \cong H^1_f(F, T^*(1)).$$

On the other hand, [4, Proposition 3.8] together with local Tate duality give

$$\frac{\widehat{H^1(F_v, A)}}{H^1_f(F_v, A)} \cong H^1_f(F_v, T^*(1))$$

for all places $v|p$. Hypothesis (i) implies that the localization map

$$H^1_f(F, T^*(1)) \to \prod_{v|p} H^1_f(F_v, T^*(1))$$

is injective. In particular, Lemma 3.2 implies that

$$\widehat{\delta} : \widehat{\mathrm{Coker}\lambda} \to \widehat{\ker \gamma} = \widehat{J_p(A/F)} \oplus \bigoplus_{v \in S \backslash \{p\}} \widehat{\ker \gamma_v}$$

is injective. Hence, δ is surjective. □

Finally, we conclude this section with the following analogue of Theorem 2.14.

Theorem 3.5. *Let f be a normalized new cuspidal modular eigenform of level N with $p \nmid N$. Suppose that the following hypotheses are satisifed:*

i) f is non-ordinary at p.

ii) The map λ_{cyc} in (3.3) (with $\mathcal{L} = F_{\text{cyc}}$) is surjective.

iii) $H^2(F_S/F, A) = 0$.

iv) The equivalent conditions in Proposition 3.3 hold.

Then the $\Lambda(\Gamma)$-module $\widehat{\text{Sel}(A/F_{\text{cyc}})}$ admits no non-trivial finite sub-module.

4. SIGNED SELMER GROUPS

Let F be a number field and F' a subfield of F. Let E/F' be an elliptic curve with good reduction at all primes above p. We write S_p^{ss} be the set of primes of F' lying above p where E has supersingular reduction. Assume that $S_p^{ss} \neq \emptyset$. Furthermore, for all $v \in S_p^{ss}$, assume that

(i) $F_v' = \mathbb{Q}_p$;

(ii) $a_v = 1 + p - \#\tilde{E}(F_v') = 0$;

(iii) v is unramified in F.

The condition (i) is necessary to apply Honda's theory of formal group to define the plus and minus conditions on E (c.f. [22, §3.1]).

Recall that F_{cyc} denotes the cyclotomic $\mathbb{Z}_p$-extension of F. For each integer $n \geq 0$, let F_n denote the sub-extension of F_{cyc}/F such that F_n/F is a cyclic extension of degree p^n. Let $S_{p,F}^{ss}$ denote the set of primes of F lying above those inside S_p^{ss}. For each $v \in S_{p,F}^{ss}$, define

$$E^+(F_{n,v}) = \{P \in \hat{E}(F_{n,v}) \big| \text{Tr}_{n/m+1} P \in \hat{E}(F_{m,v}) \,\forall \text{ even } m, 0 \leq m \leq n-1\}, \quad (4.1)$$

$$E^-(F_{n,v}) = \{P \in \hat{E}(F_{n,v}) \big| \text{Tr}_{n/m+1} P \in \hat{E}(F_{m,v}) \,\forall \text{ odd } m, 0 \leq m \leq n-1\}, \quad (4.2)$$

where $\text{Tr}_{n/m+1}$ is the trace map from $\hat{E}(F_{n,v})$ to $\hat{E}(F_{m+1,v})$. By an abuse of notation, we have denoted the unique prime of F_n lying above v by v as well. The plus and minus Selmer groups over F_n are defined by

$$\text{Sel}_p^\pm(E/F_n) = \ker\left(\text{Sel}_p(E/F_n) \to \bigoplus_{v \in S_{p,F}^{ss}} \frac{H^1(F_{n,v}, E_{p^\infty})}{E^\pm(F_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}\right),$$

where $E^\pm(F_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ are identified with their images inside $H^1(F_{n,v}, E_{p^\infty})$ via the Kummer map. By [22, Proposition 3.32], there is an isomorphism of $\Lambda(\Gamma)$-modules

$$\varinjlim_n \frac{H^1(F_{n,v}, E_{p^\infty})}{E^\pm(F_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \cong \widehat{\Lambda(\Gamma)}^{\oplus[F_v:\mathbb{Q}_p]} \quad (4.3)$$

for all $v \in S_{p,F}^{ss}$.

Remark 4.1. *When $n = 0$, the $\pm$-Selmer groups $\text{Sel}_p^\pm(E/F)$ coincide with $\text{Sel}_p(E/F)$ as $E^\pm(F_v) = \hat{E}(F_v)$.*

The plus and minus Selmer groups over F_{cyc} are defined by

$$\text{Sel}_p^\pm(E/F_{\text{cyc}}) = \varinjlim_n \text{Sel}_p^\pm(E/F_n).$$

The Pontryagin dual of $\text{Sel}_p^\pm(E/F_{\text{cyc}})$ will be denoted by $X^\pm(E/F_{\text{cyc}})$.

For any $n \geq 0$ and a prime $v \in S_{p,F}^{\mathrm{ss}}$, define

$$J_v^\pm(E/F_n) = \bigoplus_{w|v} \frac{H^1(F_{n,w}, E_{p^\infty})}{E^\pm(F_{n,w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}$$

where the direct sum is taken over all primes w of F_n lying above the prime v of F and

$$J_v^\pm(E/F_{\mathrm{cyc}}) = \varinjlim J_v^\pm(E/F_n).$$

If $v \notin S_{p,F}^{\mathrm{ss}}$, define $J_v^\pm(E/F_n) = J_v(E/F_n)$ and $J_v^\pm(E/F_{\mathrm{cyc}}) = J_v(E/F_{\mathrm{cyc}})$ as in (2.1) and (2.2). There is a natural morphism

$$\lambda_{\mathrm{cyc}}^\pm : H^1(F_S/F_{\mathrm{cyc}}, E_{p^\infty}) \to \bigoplus_{v \in S} J_v^\pm(E/F_{\mathrm{cyc}}), \tag{4.4}$$

and a fundamental diagram analogous to (2.6):

$$
\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Sel}_p^\pm(E/F_{\mathrm{cyc}})^\Gamma & \longrightarrow & H^1(F_S/F_{\mathrm{cyc}}, E_{p^\infty})^\Gamma & \xrightarrow{\lambda_{\mathrm{cyc}}^{\pm,\Gamma}} & \bigoplus_{v \in S} J_v^\pm(E/F_{\mathrm{cyc}})^\Gamma \\
& & \alpha^\pm \uparrow & & \beta \uparrow & & \gamma^\pm = \oplus \gamma_v^\pm \uparrow \\
0 & \longrightarrow & \mathrm{Sel}_p(E/F) & \longrightarrow & H^1(F_S/F, E_{p^\infty}) & \xrightarrow{\lambda} & \bigoplus_{v \in S} J_v(E/F).
\end{array}
\tag{4.5}
$$

This diagram gives a natural map

$$\delta^\pm : \ker \gamma^\pm \to \mathrm{Coker}\, \lambda. \tag{4.6}$$

Proposition 2.6 generalizes verbatim to this setting:

Proposition 4.2. *Suppose that $\lambda_{\mathrm{cyc}}^\pm$ in (4.4) is surjective. If $H^2(F_S/F, E_{p^\infty}) = 0$, then the following are equivalent:*

(i) The map $\lambda_{\mathrm{cyc}}^{\pm,\Gamma}$ in (4.5) is surjective;
(ii) $H^1(\Gamma, \mathrm{Sel}_p^\pm(E/F_{\mathrm{cyc}})) = 0$;
(iii) The map $\delta^\pm$ in (4.6) is surjective.

Remark 4.3. *As in Lemma 2.10, it is possible to deduce the surjectivity of $\lambda_{\mathrm{cyc}}^\pm$ using Poitou-Tate exact sequences when the following map is injective:*

$$\varprojlim_n H^1(F_S/F_n, T_p(E)) \to \bigoplus_{v|p, v \notin S_{p,F}^{\mathrm{ss}}} \varprojlim_n \frac{H^1(F_{n,v}, T_p(E))}{H_f^1(F_{n,v}, T_p(E))} \oplus \bigoplus_{v \in S_{p,F}^{\mathrm{ss}}} \varprojlim_n \frac{H^1(F_{n,v}, T_p(E))}{H_\pm^1(F_{n,v}, T_p(E))},$$

where $H_\pm^1(F_{n,v}, T_p(E))$ is the exact annihilator of $E^\pm(F_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ under local Tate duality. When $F = \mathbb{Q}$ (so that $S_{p,F}^{\mathrm{ss}} = \{p\}$), this map is indeed injective thanks to the cotorsionness of $\mathrm{Sel}_p^\pm(E/\mathbb{Q}_{\mathrm{cyc}})$ (c.f. [26, Lemma 6.2]). In fact, we shall see below that the surjectivity of $\lambda_{\mathrm{cyc}}^\pm$ is directly related to the cotorsionness of $\mathrm{Sel}_p^\pm(E/\mathbb{Q}_{\mathrm{cyc}})$ in a much more general setting.

Proposition 4.4. *The $\Lambda(\Gamma)$-module $\widehat{\mathrm{Sel}_p^\pm(E/F_{\mathrm{cyc}})}$ is torsion if and only if the map $\lambda_{\mathrm{cyc}}^\pm$ in (4.4) is surjective and $H^2(F_S/F_{\mathrm{cyc}}, E_{p^\infty}) = 0$.*

Proof. Let $T = T_p(E)$. For $i = 1, 2$, define

$$H^i_{\mathrm{Iw}}(F_S, T) = \varprojlim H^i(F_S/F_n, T).$$

For $v|p$, define

$$H^1_{\mathrm{Iw}}(F_v, T) = \varprojlim H^1(F_{n,v}, T)$$

and

$$H^1_{\mathrm{Iw},f}(F_v, T) = \varprojlim H^1_f(F_{n,v}, T) \text{ (for } v \notin S^{\mathrm{ss}}_{p,F}),$$
$$H^1_{\mathrm{Iw},\pm}(F_v, T) = \varprojlim H^1_\pm(F_{n,v}, T) \text{ (for } v \in S^{\mathrm{ss}}_{p,F}).$$

Consider the Poitou-Tate exact sequence

$$H^1_{\mathrm{Iw}}(F_S, T) \xrightarrow{\mathrm{loc}^\pm} \bigoplus_{v|p, v\notin S^{\mathrm{ss}}_{p,F}} \frac{H^1_{\mathrm{Iw}}(F_v, T)}{H^1_{\mathrm{Iw},f}(F_v, T)} \oplus \bigoplus_{v\in S^{\mathrm{ss}}_{p,F}} \frac{H^1_{\mathrm{Iw}}(F_v, T)}{H^1_{\mathrm{Iw},\pm}(F_v, T)}$$
$$\to \widehat{\mathrm{Sel}^\pm_p(E/F_{\mathrm{cyc}})} \to H^2_{\mathrm{Iw}}(F, T) \to 0 \qquad (4.7)$$

(c.f. [29, Proposition A.3.2]).

As explained in [9, page 23],

$$\mathrm{rank}_{\Lambda(\Gamma)} \frac{H^1_{\mathrm{Iw}}(F_v, T)}{H^1_{\mathrm{Iw},f}(F_v, T)} = [F_v : \mathbb{Q}_p]$$

for all $v|p$ and $v \notin S^{\mathrm{ss}}_{p,F}$. For all $v \in S^{\mathrm{ss}}_{p,F}$, local Tate duality and [22, Theorem 3.34] imply that

$$\mathrm{rank}_{\Lambda(\Gamma)} \frac{H^1_{\mathrm{Iw}}(F_v, T)}{H^1_{\mathrm{Iw},\pm}(F_v, T)} = [F_v : \mathbb{Q}_p].$$

Furthermore,

$$\mathrm{rank}_{\Lambda(\Gamma)} H^1_{\mathrm{Iw}}(F_S, T) - \mathrm{rank}_{\Lambda(\Gamma)} H^2_{\mathrm{Iw}}(F_S, T) = [F : \mathbb{Q}]$$

by the Euler characteristic formula (see proof of Proposition 1.3.2 in [29]). Therefore, on considering the rank of each term in (4.7), we deduce that

$$\mathrm{rank}_{\Lambda(\Gamma)} \ker \mathrm{loc}^\pm = \mathrm{rank}_{\Lambda(\Gamma)} \widehat{\mathrm{Sel}^\pm_p(E/F_{\mathrm{cyc}})}. \qquad (4.8)$$

If $\lambda^\pm_{\mathrm{cyc}}$ is surjective and $H^2(F_S/F_{\mathrm{cyc}}, E_{p^\infty}) = 0$, the second Poitou-Tate exact sequence given in [29, Proposition A.3.2] implies that

$$\widehat{\mathrm{Coker}\lambda^\pm_{\mathrm{cyc}}} \cong \ker \mathrm{loc}^\pm = 0.$$

Therefore, (4.8) tells us that $\widehat{\mathrm{Sel}^\pm_p(E/F_{\mathrm{cyc}})}$ is $\Lambda(\Gamma)$-torsion.

Conversely, suppose that $\widehat{\mathrm{Sel}^\pm_p(E/F_{\mathrm{cyc}})}$ is $\Lambda(\Gamma)$-torsion. Then (4.7) implies that $H^2_{\mathrm{Iw}}(F_S, T)$ is also $\Lambda(\Gamma)$-torsion. This is equivalent to $H^2(F_S/F_{\mathrm{cyc}}, E_{p^\infty}) = 0$ (see [27, Lemma 7.1] or [29, Proposition 1.3.2]). This then gives the isomorphism

$$\widehat{\mathrm{Coker}\lambda^\pm_{\mathrm{cyc}}} \cong \ker \mathrm{loc}^\pm.$$

14

via the Poitou-Tate exact sequence once again. In particular, (4.8) tells us that $\widehat{\mathrm{Coker}\lambda^{\pm}_{\mathrm{cyc}}}$ is $\Lambda(\Gamma)$-torsion. However, there is an injection

$$\widehat{\mathrm{Coker}\lambda^{\pm}_{\mathrm{cyc}}} \hookrightarrow \bigoplus_{v|p} \widehat{J^{\pm}_v(E/F_{\mathrm{cyc}})}$$

and that $\widehat{J^{\pm}_v(E/F_{\mathrm{cyc}})}$ is $\Lambda(\Gamma)$-torsion free for all $v|p$ (see [9, page 38] for $v \notin S^{\mathrm{ss}}_{p,F}$ and (4.3) for $v \in S^{\mathrm{ss}}_{p,F}$). Therefore, $\widehat{\mathrm{Coker}\lambda^{\pm}_{\mathrm{cyc}}}$ is zero as required. $\qquad\square$

Remark 4.5. *Suppose that $\mathrm{Sel}_p(E/F)$ is finite. By Remark 4.1, $\mathrm{Sel}^{\pm}_p(E/F)$ are also finite. Then $\widehat{\mathrm{Sel}^{\pm}_p(E/F_{\mathrm{cyc}})}$ are both $\Lambda(\Gamma)$-torsion by the control theorem (c.f. [23, Theorem 9.3] and [20, Lemma 3.9]).*

Lemma 4.6. *If $\lambda^{\pm}_{\mathrm{cyc}}$ is surjective, then the map λ_{cyc} defined in (2.3) is also surjective. Similarly, the surjectivity of $\lambda^{\pm,\Gamma}_{\mathrm{cyc}}$ in (2.6) implies that of $\lambda^{\Gamma}_{\mathrm{cyc}}$ in (4.5).*

Proof. By Remark 2.5,

$$\bigoplus_{v \in S} J^{\pm}_v(E/F_{\mathrm{cyc}}) = \bigoplus_{v \in S} J_v(E/F_{\mathrm{cyc}}) \oplus \bigoplus_{v \in S^{\mathrm{ss}}_{p,F}} J^{\pm}_v(E/F_{\mathrm{cyc}}).$$

Therefore, if $\lambda^{\pm}_{\mathrm{cyc}}$ is surjective onto $\bigoplus_{v \in S} J^{\pm}_v(E/F_{\mathrm{cyc}})$, then λ_{cyc} is surjective onto $\bigoplus_{v \in S} J_v(E/F_{\mathrm{cyc}})$. The proof for $\lambda^{\Gamma}_{\mathrm{cyc}}$ is the same. $\qquad\square$

Remark 4.7. *In particular, under the assumption that $\lambda^{\pm}_{\mathrm{cyc}}$ is surjective and $H^2(F_S/F, E_{p^\infty}) = 0$, there is an implication*

$$H^1(\Gamma, \mathrm{Sel}^{\pm}_p(E/F_{\mathrm{cyc}})) = 0 \quad \Rightarrow \quad H^1(\Gamma, \mathrm{Sel}_p(E/F_{\mathrm{cyc}})) = 0.$$

We conclude this section with the following analogue of Theorem 2.14.

Theorem 4.8. *Let E be an elliptic curve over F such that the following hypotheses are satisfied:*

(i) E has supersingular reduction at all the primes v of F lying above p.
(ii) The map $\lambda^{\pm}_{\mathrm{cyc}}$ is surjective.
(iii) $H^2(F_S/F, E_{p^\infty}) = 0$.
(iv) The equivalent conditions in Proposition 4.2 hold.

Then the $\Lambda(\Gamma)$-module $\widehat{\mathrm{Sel}^{\pm}_p(E/F_{\mathrm{cyc}})}$ admits no non-trivial finite sub-module.

Proof. As in the proof of Theorem 2.14, we have

$$H_1(\Gamma, \widehat{\mathrm{Sel}^{\pm}_p(E/F_{\mathrm{cyc}})}) = 0$$

and the result follows from [9, Lemma A.1.5]. $\qquad\square$

5. Euler characteristics of plus and minus Selmer groups over abelian p-adic Lie extensions

5.1. Plus and minus norm groups over $\mathbb{Z}^2_p$-extensions.
We review the plus and minus norm groups defined in [21, §2.1-§2.2]. Let $E/\mathbb{Q}_p$ be an elliptic curve with good supersingular reduction and $\#\tilde{E}(\mathbb{F}_p) = 1 + p$ and k a finite unramified

15

extension of $\mathbb{Q}_p$. Let k_{cyc} denote the $\mathbb{Z}_p$-cyclotomic extension of k. If $n \geq 0$ is an integer, let k_n denote the unique sub-field of k_{cyc} such that k_n/k is of degree p^n. The plus and minus norm groups $E^{\pm}(k_n)$ are defined as in (4.1) and (4.2).

Let k^{ur} denote the unramified $\mathbb{Z}_p$-extension of k and $k^{\mathrm{ur}}_{\mathrm{cyc}}$ the compositum of k_{cyc} and k^{ur}. In particular, $\mathrm{Gal}(k^{\mathrm{ur}}_{\mathrm{cyc}}/k) \cong \mathbb{Z}_p^2$. For an integer $m \geq 0$, let $k^{(m)}$ denote the unique sub-extension of k^{ur}, such that $k^{(m)}/k$ of degree p^m. Similarly, for $n \geq 1$, define k^{ur}_n to be the unramified $\mathbb{Z}_p$-extension of k_n and $k^{(m)}_n$ to the unique sub-extension such that $k^{(m)}_n/k_n$ of degree p^m. Note that $k^{\mathrm{ur}}_{\mathrm{cyc}} = \cup_{m,n} k^{(m)}_n$ and $\mathrm{Gal}(k^{(m)}_n/k) \cong \mathbb{Z}/p^m \times \mathbb{Z}/p^n$.

On replacing k by $k^{(m)}$, (4.1) and (4.2) give the plus and minus norm groups $E^{\pm}\left(k^{(m)}_n\right)$ for all $n \geq 0$. On taking union over m and n, this gives

$$E^{\pm}\left(k^{\mathrm{ur}}_{\mathrm{cyc}}\right) = \bigcup_{m,n \geq 0} E^{\pm}\left(k^{(m)}_n\right).$$

The following lemmas will be useful later.

Lemma 5.1. $E_{p^\infty}(k^{\mathrm{ur}}_{\mathrm{cyc}}) = 0$.

Proof. This follows from [22, Proposition 3.1], which says that $E_{p^\infty}\left(k^{(m)}_{\mathrm{cyc}}\right) = 0$ for all $m \geq 0$. $\qquad\square$

Lemma 5.2. *Let* $H_k = \mathrm{Gal}(k^{\mathrm{ur}}_{\mathrm{cyc}}/k_{\mathrm{cyc}}) \cong \mathbb{Z}_p$. *Then,*

(a) $H^1(H_k, E^+(k^{\mathrm{ur}}_{\mathrm{cyc}})) \oplus H^1(H_k, E^-(k^{\mathrm{ur}}_{\mathrm{cyc}})) \cong H^1(H_k, \hat{E}(k^{\mathrm{ur}}))$;

(b) $\left(E^{\pm}(k^{\mathrm{ur}}_{\mathrm{cyc}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p\right)^{H_k} = E^{\pm}(k_{\mathrm{cyc}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$.

Proof. Recall from [21, Proposition 2.6] and [23, Proposition 8.12] the short exact sequence

$$0 \to \hat{E}(k^{\mathrm{ur}}) \to E^+(k^{\mathrm{ur}}_{\mathrm{cyc}}) \oplus E^-(k^{\mathrm{ur}}_{\mathrm{cyc}}) \to \hat{E}(k^{\mathrm{ur}}_{\mathrm{cyc}}) \to 0, \qquad (5.1)$$

where the first map is given by the diagonal embedding $x \mapsto (x, x)$ and the second map is given by $(x, y) \mapsto x - y$. On taking H_k-cohomology, there is a long exact sequence

$$0 \to \hat{E}(k^{\mathrm{ur}}) \to \hat{E}(k^{\mathrm{ur}}) \oplus \hat{E}(k^{\mathrm{ur}}) \to \hat{E}(k^{\mathrm{ur}}) \to H^1\left(H_k, \hat{E}(k^{\mathrm{ur}})\right) \to$$

$$H^1\left(H_k, E^+(k^{\mathrm{ur}}_{\mathrm{cyc}})\right) \oplus H^1\left(H_k, E^-(k^{\mathrm{ur}}_{\mathrm{cyc}})\right) \to H^1\left(H_k, \hat{E}(k^{\mathrm{ur}}_{\mathrm{cyc}})\right).$$

The first three terms clearly form a short exact sequence and [5, Theorem 3.1] says that $H^1\left(H_k, \hat{E}(k^{\mathrm{ur}}_{\mathrm{cyc}})\right) = 0$. Part (a) follows.

The H_k-cohomology exact sequence attached to the short exact sequence

$$0 \to \hat{E}(k^{\mathrm{ur}}) \to \hat{E}(k^{\mathrm{ur}}) \otimes \mathbb{Q}_p \to \hat{E}(k^{\mathrm{ur}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to 0$$

gives the injectivity of $H^1\left(H_k, \hat{E}(k^{\mathrm{ur}})\right) \to H^1\left(H_k, \hat{E}(k^{\mathrm{ur}}) \otimes \mathbb{Q}_p\right)$. On combining this with part (a), the natural maps $H^1\left(H_k, E^{\pm}(k^{\mathrm{ur}}_{\mathrm{cyc}})\right) \to H^1\left(H_k, E^{\pm}(k^{\mathrm{ur}}_{\mathrm{cyc}}) \otimes \mathbb{Q}_p\right)$ are also injective. This implies part (b). $\qquad\square$

Proposition 5.3. *The Pontryagin dual of the quotient $\frac{H^1(k_{\mathrm{cyc}}^{\mathrm{ur}}, E_{p^\infty})}{E^\pm(k_{\mathrm{cyc}}^{\mathrm{ur}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}$ is a free $\mathbb{Z}_p[[\mathrm{Gal}(k_{\mathrm{cyc}}^{\mathrm{ur}}/k)]]$-module of rank $[k : \mathbb{Q}_p]$.*

Proof. Let $m \geq 0$ be an integer and write $H_m = \mathrm{Gal}(k_{\mathrm{cyc}}^{\mathrm{ur}}/k_{\mathrm{cyc}}^{(m)}) (= H_k^{p^m} \cong \mathbb{Z}_p)$. The proof for [25, (8.22)] gives

$$
\left(\frac{H^1(k_{\mathrm{cyc}}^{\mathrm{ur}}, E_{p^\infty})}{E^\pm(k_{\mathrm{cyc}}^{\mathrm{ur}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right)^{H_m} \cong \frac{H^1(k_{\mathrm{cyc}}^{\mathrm{ur}}, E_{p^\infty})^{H_m}}{\left(E^\pm(k_{\mathrm{cyc}}^{\mathrm{ur}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \right)^{H_m}} = \frac{H^1(k_{\mathrm{cyc}}^{(m)}, E_{p^\infty})}{E^\pm(k_{\mathrm{cyc}}^{(m)}) \otimes \mathbb{Q}_p/\mathbb{Z}_p},
$$

where the last equality follows from Lemma 5.1, together with the inflation-restriction exact sequence and Lemma 5.2(b). By [22, Proposition 3.32], this gives

$$
\left(\frac{H^1(k_{\mathrm{cyc}}^{\mathrm{ur}}, E_{p^\infty})}{E^\pm(k_{\mathrm{cyc}}^{\mathrm{ur}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right)^{H_m} \cong \mathbb{Z}_p[[\widehat{\mathrm{Gal}(k_{\mathrm{cyc}}/k)}]]^{\oplus [k^{(m)} : \mathbb{Q}_p]}.
$$

The result follows. $\qquad\square$

5.2. Plus and minus Selmer groups.

We work under the same setting as in §4 and further assume that p splits completely in F. Let F_∞ denote the compositum of all $\mathbb{Z}_p$-extensions of F. Note that $F_{\mathrm{cyc}} \subset F_\infty$. The Galois group $\Omega := \mathrm{Gal}(F_\infty/F)$ is an abelian torsion-free pro-p group. In particular,

$$
\Omega \cong \mathbb{Z}_p^d
$$

for some integer $d \geq 1$. Leopoldt's conjecture predicts that d is given by $r_2 + 1$, where r_2 is the number of pairs of complex embeddings of F. We write $\Lambda(\Omega)$ for its Iwasawa algebra over $\mathbb{Z}_p$, that is, $\mathbb{Z}_p[[\Omega]] = \varprojlim \mathbb{Z}_p[\Omega/U]$, where the inverse limit runs through all open subgroups U of Ω and the connecting maps are projections.

Let v be a place of F and w a place of F_∞ above v. If $v|p$, then F_v may be identified with $\mathbb{Q}_p$ and $F_{\infty,w}/F_v$ is an abelian pro-p extension. By local class field theory, its Galois group is isomorphic to either $\mathbb{Z}_p$ or $\mathbb{Z}_p^2$, depending on whether $d = 1$ or $d > 1$. In particular, $F_{\infty,w}$ coincides with either $F_{v,\mathrm{cyc}}$ or $F_{v,\mathrm{cyc}}^{\mathrm{ur}}$ under the notation introduced in §5.1. If $v \nmid p$, then $F_{\infty,w}$ is the unique unramified $\mathbb{Z}_p$-extension of F_v.

Let $v_0 \in S_p^{\mathrm{ss}}$ be a place of F'. Fix $v \in S_{p,F}^{\mathrm{ss}}$ and a place w of F_∞, both of which lying above v_0. As noted above, $F_{\infty,w}$ may be identified with either $F_{v,\mathrm{cyc}}$ or $F_{v,\mathrm{cyc}}^{\mathrm{ur}}$. In both cases, there exist the plus and minus norm groups $E^\pm(F_{\infty,w}) \subset \hat{E}(F_{\infty,w})$. Define

$$
J_v^\pm(E/F_\infty) = \bigoplus_{w|v} \frac{H^1(F_{\infty,w}, E_{p^\infty})}{E^\pm(F_{\infty,w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p},
$$

where $E^\pm(F_{\infty,w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ is identified as a subgroup of $H^1(F_{\infty,w}, E_{p^\infty})$ via the Kummer map as before. The plus and minus Selmer groups over F_∞ are given by

$$
\mathrm{Sel}_p^\pm(E/F_\infty) = \ker \left(\mathrm{Sel}_p(E/F_\infty) \to \bigoplus_{v \in S_{p,F}^{\mathrm{ss}}} J_v^\pm(E/F_\infty) \right).
$$

Remark 5.4. *In fact, it is possible to define $2^{\#S_{p,F}^{\mathrm{ss}}}$ signed Selmer groups since we may choose either the plus or minus norm subgroup as local condition for each prime $v \in S_{p,F}^{\mathrm{ss}}$. In [21], Kim studied four such Selmer groups for an elliptic curve $E/\mathbb{Q}$ when F is an imaginary quadratic field where p splits (so that $\#S_{p,F}^{\mathrm{ss}} = 2$). See also [1].*

5.3. **Euler characteristics.** Recall that if A is a discrete primary Γ-module, the Γ-Euler characteristic of A is said to be finite if $H^0(\Gamma, A)$ and $H^1(\Gamma, A)$ are both finite and it is defined to be

$$\chi(\Gamma, A) = \frac{\#H^0(\Gamma, A)}{\#H^1(\Gamma, A)}.$$

Theorem 5.5 ([20, Theorem 1.2]). *Suppose that $\mathrm{Sel}_p(E/F)$ is finite and that E has supersingular reduction at every prime above p, then the Γ-Euler characteristic of $\mathrm{Sel}_p^{\pm}(E/F_{\mathrm{cyc}})$ is finite and equals, up to a p-adic unit*

$$\#\mathrm{Sel}_p(E/F) \times \prod_v c_v,$$

where v runs through all primes of F and c_v denotes the Tamagawa number of E at v.

We now study the Ω-Euler characteristic of $\mathrm{Sel}_p^{\pm}(E/F_\infty)$, where $\Omega = \mathrm{Gal}(F_\infty/F)$ and F_∞ is the extension considered in §5.2. Let $H = \mathrm{Gal}(F_\infty/F_{\mathrm{cyc}}) \cong \mathbb{Z}_p^{d-1}$ (so that $\Gamma \cong \Omega/H$). Let w be a finite place of F_∞. Recall that the decomposition group of $w|p$ in H is either $\mathbb{Z}_p$ or 0, depending on whether $d > 1$ or $d = 1$. It is always 0 when $w \nmid p$.

Consider the following commutative diagram:

$$
\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Sel}_p^{\pm}(E/F_\infty)^H & \longrightarrow & H^1(F_S/F_\infty, E_{p^\infty})^H & \xrightarrow{\lambda_\infty^{H,\pm}} & \bigoplus_{v \in S} J_v^{\pm}(E/F_\infty)^H \\
& & \alpha_\infty^{\pm} \uparrow & & \beta_\infty \uparrow & & \gamma_\infty^{\pm} = \oplus \gamma_{v,\infty}^{\pm} \uparrow \\
0 & \longrightarrow & \mathrm{Sel}_p^{\pm}(E/F_{\mathrm{cyc}}) & \longrightarrow & H^1(F_S/F_{\mathrm{cyc}}, E_{p^\infty}) & \xrightarrow{\lambda_{\mathrm{cyc}}^{\pm}} & \bigoplus_{v \in S} J_v^{\pm}(E/F_{\mathrm{cyc}}).
\end{array}
$$

$$(5.2)$$

Lemma 5.6. *The map β_∞ in (5.2) is an isomorphism.*

Proof. Lemma 5.1 says that $E_{p^\infty}(F_{\infty,w}) = 0$ for any place w of F_∞ lying above a prime in $S_{p,F}^{\mathrm{ss}}$. In particular, it implies that $E_{p^\infty}(F_\infty) = 0$. Therefore, β_∞ is an isomorphism by the inflation-restriction exact sequence. $\square$

Corollary 5.7. *If $\lambda_{\mathrm{cyc}}^{\pm}$ is surjective, then the map $\alpha_\infty^{\pm}$ in (5.2) is injective and its cokernel is isomorphic to $\ker \gamma_\infty^{\pm}$.*

Proof. This follows from the snake lemma and Lemma 5.6. $\square$

Proposition 5.8. *The map $\gamma_{v,\infty}^{\pm}$ in (5.2) is an isomorphism for all $v \in S_{p,F}^{\mathrm{ss}}$.*

18

Proof. Let w be a place of F_∞ lying above v and write H_w for the Galois group of the extension $F_{\infty,w}/F_{v,\mathrm{cyc}}$. Then, the proof of Proposition 5.3 gives

$$\left(\frac{H^1(F_{\infty,w}, E_{p^\infty})}{E^\pm(F_{\infty,w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right)^{H_w} \cong \frac{H^1(F_{v,\mathrm{cyc}}, E_{p^\infty})}{E^\pm(F_{v,\mathrm{cyc}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p},$$

which implies that $\gamma_{v,\infty}^\pm$ is the identity map. $\qquad\square$

Lemma 5.9. *Let $v \in S \setminus S_{p,F}^{\mathrm{ss}}$ such that $v|p$. Then $\gamma_{v,\infty}^\pm$ is surjective, and $\ker \gamma_{v,\infty}^\pm$ is $\Lambda(\Gamma)$-cotorsion.*

Proof. Let w be a place of F_∞ lying above v. Recall from [5, Proposition 4.8] that

$$\frac{H^1(F_{\infty,w}, E_{p^\infty})}{E(F_{\infty,w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} = H^1(F_{\infty,w}, \tilde{E}_w[p^\infty]), \quad \frac{H^1(F_{v,\mathrm{cyc}}, E_{p^\infty})}{E(F_{v,\mathrm{cyc}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} = H^1(F_{v,\mathrm{cyc}}, \tilde{E}_w[p^\infty]),$$

where $\tilde{E}_w$ denotes the reduced curve of E at w. By the inflation-restriction exact sequence, the cokernel of

$$H^1(F_{v,\mathrm{cyc}}, \tilde{E}_w[p^\infty]) \to H^1(F_{\infty,w}, \tilde{E}_w[p^\infty])^{\mathrm{Gal}(F_{\infty,w}/F_{v,\mathrm{cyc}})}$$

is given by

$$H^2\left(F_{\infty,w}/F_{v,\mathrm{cyc}}, \tilde{E}_w(\tilde{F}_{\infty,w})[p^\infty] \right),$$

where $\tilde{F}_{\infty,w}$ is the residue field of $F_{\infty,w}$. This is zero since $F_{\infty,w}/F_{v,\mathrm{cyc}}$ is either trivial or a $\mathbb{Z}_p$-extension. The kernel of this map is given by $H^1(F_{\infty,w}/F_{v,\mathrm{cyc}}, \tilde{E}_w(\tilde{F}_{\infty,w})[p^\infty])$, which is cofinitely generated over $\mathbb{Z}_p$. There are only finitely many places of F_{cyc} lying above p, so $\ker \gamma_{v,\infty}^\pm$ is also cofinitely generated over $\mathbb{Z}_p$. $\qquad\square$

Lemma 5.10. *If $v \in S$ and $v \nmid p$, then the map $\gamma_{v,\infty}^\pm$ is an isomorphism.*

Proof. Let ν be a place of F_{cyc} lying above v and let w be a place of F_∞ lying above ν. Then, $F_{\infty,w} = F_{\mathrm{cyc},\nu}$ is the unique $\mathbb{Z}_p$-extension of F_v. In particular, $\gamma_{v,\infty}^\pm$ is nothing but the identity map. $\qquad\square$

Proposition 5.11. *Assume that $\widehat{\mathrm{Sel}_p^\pm(E/F_{\mathrm{cyc}})}$ is $\Lambda(\Gamma)$-torsion. Then the map $\lambda_\infty^{H,\pm}$ in (5.2) is surjective.*

Proof. It suffices to show that $\gamma_\infty^\pm \circ \lambda_{\mathrm{cyc}}^\pm$ is surjective. Proposition 4.4 says that $\lambda_{\mathrm{cyc}}^\pm$ is surjective. On combining Proposition 5.8 with Lemmas 5.10 and 5.9, we deduce that $\gamma_\infty^\pm$ is surjective. Hence the result. $\qquad\square$

Corollary 5.12. *Assume that $\mathrm{Sel}_p(E/F)$ is finite, then*
(a) $H^1(H, \mathrm{Sel}_p^\pm(E/F_\infty)) = 0$;
(b) $H^1(\Omega, \mathrm{Sel}_p^\pm(E/F_\infty)) = H^1(\Gamma, \mathrm{Sel}_p^\pm(E/F_\infty)^H)$.

Proof. Recall from Remark 4.1 that $\mathrm{Sel}_p^\pm(E/F) = \mathrm{Sel}_p(E/F)$. Thus, by Kim's control theorem (see Theorem 1.1 of [21]; we remark that the hypothesis on $4 \nmid [F_v : \mathbb{Q}_p]$ in loc. cit. can be removed thanks to the work of Kitajima-Otsuki [22]),

$\mathrm{Sel}_p^{\pm}(E/F_\infty)^\Omega$ is finite. By Nakayama's lemma (see [2]), $\widehat{\mathrm{Sel}_p^{\pm}(E/F_\infty)}$ is a torsion $\Lambda(\Omega)$-module. Thus, the same proof of Proposition 4.4 shows that the map

$$\lambda_\infty^{\pm} : H^1(F_S/F_\infty, E_{p^\infty}) \to \bigoplus_{v \in S} J_v^{\pm}(E/F_\infty)$$

is surjective and $H^2(F_S/F_\infty, E_{p^\infty}) = 0$.

Similarly, Kobayashi's control theorem [23, Theorem 9.3] tells us that $\widehat{\mathrm{Sel}_p^{\pm}(E/F_{\mathrm{cyc}})}$ is $\Lambda(\Gamma)$-torsion. Thus, it follows from Proposition 5.11 that $\lambda_\infty^{H,\pm}$ in (5.2) is surjective. Therefore, the proof of Proposition 2.6 gives

$$H^1(H, \mathrm{Sel}_p^{\pm}(E/F_\infty)) = 0.$$

The result now follows from the Hochschild-Serre spectral sequence

$$H^m(\Gamma, H^n(H, \mathrm{Sel}_p^{\pm}(E/F_\infty)) \Rightarrow H^{m+n}(\Omega, \mathrm{Sel}_p^{\pm}(E/F_\infty)).$$

$\square$

Corollary 5.13. *Assume that E has supersingular reduction at every prime above p and that $\mathrm{Sel}_p(E/F)$ is finite. Then*

$$H^1(\Omega, \mathrm{Sel}_p^{\pm}(E/F_\infty)) = 0.$$

Proof. It follows from Lemma 5.6, Proposition 5.8 and Lemma 5.10 that the map $\alpha_\infty^{\pm}$ in (5.2) is an isomorphism. Therefore, Corollary 5.12(b) says that

$$H^1(\Omega, \mathrm{Sel}_p^{\pm}(E/F_\infty)) = H^1(\Gamma, \mathrm{Sel}_p^{\pm}(E/F_{\mathrm{cyc}})).$$

This is zero by Proposition 4.2. $\square$

Proposition 5.14. *Assume that E has supersingular reduction at every prime above p and that $\mathrm{Sel}_p(E/F)$ is finite. Then for $i \geq 2$,*

$$H^i(\Omega, \mathrm{Sel}_p^{\pm}(E/F_\infty)) = 0.$$

Proof. It is enough to show that

(a) $H^i(\Omega, H_S^1(F_\infty, E_{p^\infty})) = 0$ for $i \geq 2$;
(b) $H^i(\Omega, J_v^{\pm}(E/F_\infty)) = 0$ for $i \geq 1$ and $v \in S$.

Since p is odd, the cohomological dimension of $\mathrm{Gal}(F_S/F)$ is 2. Therefore, (a) follows from $H^2(F_S/F_{\mathrm{cyc}}, E_{p^\infty}) = 0$ (which is a consequence of Proposition 4.4) and the spectral sequence

$$H^i\left(\Omega, H^j(F_S/F_\infty, E_{p^\infty})\right) \Rightarrow H^{i+j}(F_S/F, E_{p^\infty}).$$

For (b), consider the following two cases:

(b1) $v \nmid p$;
(b2) $v \in S_{p,F}^{\mathrm{ss}}$.

For (b1), recall from the proof of Lemma 5.10 that the decomposition group of any place not dividing p inside H is trivial. Hence,

$$H^1(\Omega, J_v^{\pm}(E/F_\infty)) = H^1(\Gamma, J_v^{\pm}(E/F_{\mathrm{cyc}})) = \bigoplus_{w|v} H^1(\Gamma, H^1(F_{\mathrm{cyc},w}, E_{p^\infty})) = 0$$

20

by the Hochschild-Serre spectral sequence. For (b2), the result follows from the co-freeness of $J_v^\pm(E/F_\infty)$ as given by Proposition 5.3. $\qquad\square$

Theorem 5.15. *Suppose that E has supersingular reduction at every prime above p and that $\mathrm{Sel}_p(E/F)$ is finite. Then $\chi(\Omega, \mathrm{Sel}_p^\pm(E/F_\infty))$ is well-defined and equals*

$$\chi(\Gamma, \mathrm{Sel}_p^\pm(E/F_{\mathrm{cyc}})) = \#\mathrm{Sel}_p(E/F) \times \prod_v c_v.$$

Proof. By Corollary 5.12 and Proposition 5.14, $H^i(\Omega, \mathrm{Sel}_p^\pm(E/F_{\mathrm{cyc}})) = 0$ for all $i \geq 1$. The finiteness of $\mathrm{Sel}_p(E/F)$, together with Kim's control theorem imply that $H^0(\Omega, \mathrm{Sel}_p^\pm(E/F_{\mathrm{cyc}}))$ is finite. In particular,

$$\chi(\Omega, \mathrm{Sel}_p^\pm(E/F_\infty)) = \#H^0(\Omega, \mathrm{Sel}_p^\pm(E/F_\infty)).$$

Since all primes above p are supersingular primes for E, Proposition 5.8, Lemmas 5.10 and 5.6 imply that $\alpha_\infty^\pm$ in (5.2) is an isomorphism. Therefore,

$$H^0(\Omega, \mathrm{Sel}_p^\pm(E/F_\infty)) = H^0(\Gamma, \mathrm{Sel}_p^\pm(E/F_{\mathrm{cyc}}))$$

as required. $\qquad\square$

References

[1] S. Ahmed, M. F. Lim, *On the Euler characteristics of signed Selmer groups*, (2019), to appear in B. Aust. Math. Soc.

[2] P. N. Balister, S. Howson, *Note on Nakayama's lemma for compact Λ-modules*, Asian J. Math. **1** (1997), no. 2, 224–229.

[3] L. Berger, *Représentations de de Rham et normes universelles*, Bull. Soc. Math. France **133** (2005), no. 4, 601–618.

[4] S. Bloch, K. Kato, *L-functions and Tamagawa numbers of motives*, The Grothendieck Festschrift, Vol. I, 333–400, Progr. Math., **86**, Birkhäuser Boston, Boston, MA, 1990.

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

[6] J. Coates, G. McConnell, *Iwasawa theory of modular elliptic curves of analytic rank at most 1*, J. London Math. Soc. **50** (1994), no. 2, 243–264.

[7] J. Coates, P. Schneider, R. Sujatha, *Links between cyclotomic and GL2 Iwasawa theory.* Kazuya Kato's fiftieth birthday. Doc. Math. 2003, Extra Vol., 187–215.

[8] J. Coates, R. Sujatha, *Fine Selmer groups of elliptic curves over p-adic Lie extensions*, Math. Ann. **331** (2005), no. 4, 809–839.

[9] J. Coates, R. Sujatha, *Galois Cohomology of Elliptic Curves*, 2nd Ed., Tata Institute of Fundamental Research Lectures on Mathematics, 88. Published by Narosa Publishing House, New Delhi; for the Tata Institute of Fundamental Research, Mumbai, 2010.

[10] J. Coates, R. Sujatha, J.-P. Wintenberger, *On the Euler-Poincaré characteristics of finite dimensional p-adic Galois representations*, Publ. Math. Inst. Hautes Études Sci. No. **93** (2001), 107–143

[11] P. Deligne, *Formes modulaires et représentations l-adiques*. Séminaire Bourbaki. Vol. 1968/69: Exposés 347–363, Exp. No. 355, 139–172, Lecture Notes in Math., 175, Springer, Berlin, 1971.

[12] R. Greenberg, *Iwasawa theory for p-adic representations*, Algebraic number theory, 97–137, Adv. Stud. Pure Math., **17**, Academic Press, Boston, MA, 1989.

[13] R. Greenberg, *On the structure of Selmer groups*, Elliptic curves, modular forms and Iwasawa theory, 225–252, Springer Proc. Math. Stat., 188, Springer, Cham, 2016.

[14] Y. Hachimori, *Euler characteristics of fine Selmer groups*, J. Ramanujan Math. Soc. **25** (2010), no. 3, 285–293.

[15] Y. Hachimori, K. Matsuno, *An analogue of Kida's formula for the Selmer groups of elliptic curves*, J. Algebraic Geom. **8** (1999), no. 3, 581–601.

[16] J. Hatley, A. Lei, *Arithmetic properties of signed Selmer groups at nonordinary primes*, Ann. Inst. Fourier. **69** (2019), no. 3, 1259–1294

[17] H. Imai, *A remark on the rational points of abelian varieties with values in cyclotomic $\mathbb{Z}_l$-extensions*, Proc. Japan. Acad. Math. Sci. **51** (1975), 12–16.

[18] A. Iovita, R. Pollack, *Iwasawa theory of elliptic curves at supersingular primes over $\mathbb{Z}_p$-extensions of number fields*, J. Reine Angew. Math. **598** (2006), 71–103.

[19] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Cohomologies p-adiques et applications arithmétiques. III. Astérisque No. **295** (2004), ix, 117–290.

[20] B.D. Kim, *The plus/minus Selmer groups for supersingular primes*, J. Aust. Math. Soc. **95** (2013), no. 2, 189–200.

[21] B.D. Kim, *Signed-Selmer groups over the $\mathbb{Z}_p^2$-extension of an imaginary quadratic field*, Canad. J. Math., **66** (2014), no. 4, 826–843.

[22] T. Kitajima and R. Otsuki, *On the plus and minus Selmer groups for elliptic curves at supersingular primes*, Tokyo J. Math., **41** (2018), no. 1, 273–303.

[23] S. Kobayashi, *Iwasawa theory for elliptic curves at supersingular primes*, Invent. Math. **152** (2003), no. 1, 1–36.

[24] A. Lei, *Iwasawa theory for modular forms at supersingular primes*, Compos. Math. **147** (2011), no. 3, 803–838.

[25] A. Lei, B. Palvannan, *Codimension two cycles in Iwasawa theory and elliptic curves with supersingular reduction*, Forum Math. Sigma **7** (2019), e25.

[26] A. Lei, S. Zerbes, *Signed Selmer groups over p-adic Lie extensions*, J. Théor. Nombres Bordeaux **24** (2012), no. 2, 377–403.

[27] M. F. Lim, *Notes on the fine Selmer groups*, Asian J. Math. **21** (2017), no. 2, 337–361.

[28] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266.

[29] B. Perrin-Riou, *Fonctions L p-adiques des représentations p-adiques*, Astérisque **229** (1995), 198 pp.

[30] B. Perrin-Riou, *Représentations p-adiques et normes universelles. I. Le cas cristallin*, J. Amer. Math. Soc. **13** (2000), no. 3, 533–551.

[31] K. Ribet, *On l-adic representations attached to modular forms. II*, Glasgow Math. J. **27** (1985), 185–194.

[32] P. Schneider, *Arithmetic of formal groups and applications. I. Universal norm subgroups*, Invent. Math. **87** (1987), no. 3, 587–602.

[33] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.

[34] R. Sujatha, *Iwasawa theory and modular forms*, Pure Appl. Math. Q. **2** (2006), no. 2, Special Issue: In honor of John H. Coates. Part 2, 519–538.

[35] F. SPRUNG, *Iwasawa theory for elliptic curves at supersingular primes: a pair of main conjectures*, J. Number Theory **132** (2012), no. 7, 1483–1506.

[36] F. SPRUNG, *A formulation of p-adic versions of the Birch and Swinnerton-Dyer conjectures in the supersingular case*, Res. Number Theory **1** (2015), Art. 17, 13 pp.

(A. LEI) DÉPARTEMENT DE MATHÉMATIQUES ET DE STATISTIQUES, UNIVERSITÉ LAVAL, PAVILLON ALEXANDRE-VACHON, 1045 AVENUE DE LA MÉDECINE, QUÉBEC, QC, CANADA G1V 0A6

Email address: antonio.lei@mat.ulaval.ca

(R. SUJATHA) MATHEMATICS DEPARTMENT, 1984, MATHEMATICS ROAD, UNIVERSITY OF BRITISH COLUMBIA, VANCOUVER, CANADA V6T 1Z2

Email address: sujatha@math.ubc.ca