Residual supersingular Iwasawa theory and signed Iwasawa invariants

Filippo Alberto Edoardo Nuccio Mortarino Majno di Capriglio, Ramdorai Sujatha

RESIDUAL SUPERSINGULAR IWASAWA THEORY AND SIGNED IWASAWA INVARIANTS

FILIPPO A. E. NUCCIO MORTARINO MAJNO DI CAPRIGLIO AND RAMDORAI SUJATHA

Abstract. For an odd prime p and a supersingular elliptic curve over a number field, this article introduces a fine signed residual Selmer group, under certain hypotheses on the base field. This group depends purely on the residual representation at p, yet captures information about the Iwasawa theoretic invariants of the signed p^∞-Selmer group that arise in supersingular Iwasawa theory. Working in this residual setting provides a natural framework for studying congruences modulo p in Iwasawa theory.

1. Introduction

Iwasawa theory of Galois representations, especially those arising from elliptic curves and modular forms, affords deep insights into the arithmetic of these objects over number fields. The Iwasawa theoretic invariants, especially the μ and λ invariants, play a central role in this study. The Iwasawa theory for ordinary elliptic curves, and more generally for ordinary Galois representations, was initiated by Mazur in [Maz72] and Greenberg in [Gre89]. The corresponding theory for supersingular elliptic curves is subtler and was already begun by Perrin-Riou in [PR90]. In the last couple of decades, the supersingular Iwasawa theory has gained considerable momentum (see [Kob03, Pol03, IP06, LLZ10, Spr12, Kim13, Kim18, KO18] and references therein).

Greenberg and Vatsal investigated in [GV00] the behaviour of Iwasawa invariants for ordinary elliptic curves whose residual representations are congruent. The objects of study are the dual p^∞-Selmer groups of the elliptic curves over the cyclotomic $\mathbb{Z}_p$-extension of the base field, which is assumed to be a number field. Specifically, let p be an odd prime and E_i, $i = 1, 2$ be two elliptic curves over $\mathbb{Q}$ with good ordinary reduction at p. Greenberg and Vatsal prove that the vanishing of the μ-invariant for the dual p^∞-Selmer group of one of the curves implies the vanishing for the other. Their study makes crucial use of a *non-primitive* dual Selmer group, which has the same μ-invariant as the dual p^∞-Selmer group. When the μ-invariants vanish, they also prove the equality of the λ-invariants for the non-primitive dual p^∞-Selmer groups for E_1 and E_2. However, they provide examples showing that the λ-invariants for the dual p^∞-Selmer groups do not coincide. These results have been extended to the representations coming from higher weight modular forms by Emerton, Pollack and Weston in [EPW06], and to more general base fields and $\mathbb{Z}_p$-extensions by, among others, Hachimori in [Hac11] and by Kidwell in [Kid18]. A crucial input in the study of p^∞-Selmer groups in the ordinary case is a deep result of Kato (see [Kat04]) which implies that the dual p^∞-Selmer groups (and their non-primitive counterparts) are torsion modules over the Iwasawa algebra.

When $\mathsf{E}/\mathbb{Q}$ is an elliptic curve having good, supersingular reduction at p, the dual p^∞-Selmer group is no longer torsion. Kobayashi defined the *signed* p^∞-Selmer in [Kob03], making use of special subgroups of the local Mordell–Weil groups along the cyclotomic tower which were already considered by Perrin-Riou. These signed p^∞-Selmer groups are torsion over the Iwasawa algebra and display properties that are strikingly similar to those of the p^∞-Selmer group in the ordinary case and come equipped with *signed*

Date: November 24th 2019.
2010 *Mathematics Subject Classification.* 11R23, 11G05.

Iwasawa invariants $\lambda^{\pm}, \mu^{\pm}$. Analogous results to those of Greenberg–Vatsal for these signed invariants were proved by Kim in [Kim09], again making use of the notion of non-primitive Selmer groups. The study of signed Selmer groups for higher weight modular forms has been initiated by Lei, Loeffler and Zerbes in [LLZ10] through the theory of Wach modules, and extensions of Greenberg–Vatsal results in this setting can be found in [HL19] by Hatley and Lei. The definition of the signed Selmer groups has been extended to a broader class of number fields in [IP06, Kim13, KO18]. In this article we will mainly refer to Kitajima–Otsuki's paper. Our work sheds more light on the behaviour of the Iwasawa invariants for the dual signed p^{∞}-Selmer groups of elliptic curves in the supersingular case. The results proved here are more general than those in [Kim09].

The novelty in our approach is that we systematically work with the residual representation of a supersingular elliptic curve defined over a number field L satisfying certain conditions (see Section 2, in particular hypothesis **Hyp 1** therein), instead of working with $\mathsf{E}_{p^{\infty}}$. In particular, we introduce a new Selmer group, attached to the Galois representation E_p of p-torsion points of E, which we call *fine signed residual Selmer group*. It depends only on the isomorphism class of the residual Galois representation E_p, yet captures the full Iwasawa-theoretic information about the $\mu^{\pm}$- and the $\lambda^{\pm}$-invariants of the usual signed p^{∞}-Selmer group. The group that we introduce is to be viewed as the residual, signed, analogue of the fine p^{∞}-Selmer group introduced by Coates and the second author in [CS05]. In *loc. cit.* , the authors postulate a conjecture, referred to as Conjecture A, which asserts that the Iwasawa μ-invariant of the dual fine p^{∞}-Selmer group over $\mathrm{L}_{\mathrm{cyc}}$ vanishes. It is pertinent to remark here that Conjecture A depends only on the residual Galois representation (see [Gre11] and [Suj10]) and its formulation is independent of the reduction type at p of the elliptic curve. Working directly with the fine signed residual Selmer group provides a conceptual framework to explore the comparison of Iwasawa-theoretic invariants, when the residual representations are isomorphic. It also potentially provides the right context for explaining a plethora of congruences in arithmetic, such as the congruences between complex and p-adic L-values which occur when the residual representations are isomorphic. We hope to return to this subject of framing a *residual Iwasawa theory* in our future works.

The main results of this paper are Theorem 4.12 and Theorem 4.14. Under certain hypothesis **Hyp 1** and **Hyp 2**, and assuming Conjecture A, Theorem 4.12 provides a criterion for the $\mu^{\pm}$-invariant of the signed p^{∞}-Selmer group to vanish, purely in terms of the fine signed residual Selmer group. We refer to the main body of the paper for its statement, because it involves some morphism whose definition is too technical for this introduction.

As an application of Theorem 4.12, the next theorem provides a criterion for the $\mu^{\pm}$-invariant of the signed p^{∞}-Selmer group to vanish, purely in terms of the fine signed residual Selmer group. In the following, denote by $\mathrm{X}^{\pm}((\mathsf{E}_j)_{p^{\infty}}/\mathrm{L}_{\mathrm{cyc}})$ the dual signed p^{∞}- Selmer groups, as defined in [KO18, Definition 2.1] (see also Definition 3.6):

Theorem 4.14. *Let $\mathsf{E}_1, \mathsf{E}_2$ be two elliptic curves defined over* L*, satisfying hypotheses **Hyp 1** and **Hyp 2**. Suppose that the residual Galois representations $(\mathsf{E}_1)_p$ and $(\mathsf{E}_2)_p$ are isomorphic.*

Let $\mu^{\pm}_{\mathsf{E}_j}$ and $\lambda^{\pm}_{\mathsf{E}_j}$ be the Iwasawa invariants of $\mathrm{X}^{\pm}((\mathsf{E}_j)_{p^{\infty}}/\mathrm{L}_{\mathrm{cyc}})$, for $j = 1, 2$. Then, for both choices of sign,

$$\mu^{\pm}_{\mathsf{E}_1} = 0 \iff \mu^{\pm}_{\mathsf{E}_2} = 0.$$

For each sign $* \in \{+, -\}$ for which this vanishing happens, we also have

$$\lambda^{*}_{\mathsf{E}_j} = \rho^{*} + \delta_{\mathsf{E}_j}$$

where δ_{E_j} is as in Definition 4.4 and $\rho^{\pm} := \rho^{\pm}_{\mathsf{E}_1} = \rho^{\pm}_{\mathsf{E}_2}$ is as in (35).

The first term ρ^* in the above statement depends only on the residual representation and is independent of the sign. The second term δ_{E_j} depends on the structure of the local p-torsion of the elliptic curve over the first layer of the cyclotomic tower at the set of primes of bad reduction, together with the primes above p with ordinary reduction. We refer the reader to the main body of the paper for the precise definitions of these numerical invariants.

Our methods also show that the difference $\lambda^+ - \lambda^-$ depends only on the residual representation, a fact which was already observed by Kim in [Kim09, Remark 3.3] for $\mathrm{L} = \mathbb{Q}$. Proposition 3.8 and Proposition 3.9 are the key technical tools needed to show that the definition of the fine signed residual Selmer group depends only on the residual representation. They compare the reduction type at places above p of two residually isomorphic elliptic curve at primes above p, and are of independent interest. The first result relies on Honda–Tate theory and is a typical feature of supersingular reduction, while the second relies upon a result by Raynaud on finite flat group schemes killed by p.

In ongoing works we extend these results in the following different directions. First, to higher weight modular forms over the cyclotomic extension, second to multiple $\mathbb{Z}_p$-extensions, and finally to the multiply signed Selmer groups as well as non-commutative p-adic Lie extensions.

The paper consists of five sections, including this introductory section. In Section 2, we introduce notation and some preliminaries about the local structure of elliptic curves with supersingular reduction. In Section 3, we recall the main properties of plus/minus Kummer maps and Selmer groups, mainly building upon [KO18], and we introduce the fine signed residual Selmer group. In Section 4, we study the Iwasawa theory of this group and state our main results. The final section presents some numerical examples that illustrate our results.

Acknowledgement. We would like to thank Laurent Berger for inviting the second author to ENS Lyon in June 2018 which led to initiating this research. This work was continued during the visit of the first author to the Pacific Institute of Mathematical Sciences (PIMS), Vancouver benefiting of a CNRS-PIMS exchange. F. A. E. N. gratefully acknowledges the support and hospitality of PIMS and of the University of British Columbia, as well as the *acceuil en délégation à l'UMI-3069 du CNRS*. S. R. gratefully acknowledges support from NSERC Discovery grant 201903987. We would also like to thank Matthieu Romagny for helpful correspondence.

2. Preliminaries

In this paper L denotes a fixed number field of absolute degree $[\mathrm{L} : \mathbb{Q}] = N$, and E/L is an elliptic curve defined over L. Throughout, p will denote an odd prime ≥ 3, S_p denotes the set of primes above p in L and $T_p(\mathsf{E})$ will denote the Tate module of E. The following hypothesis is assumed throughout (*cf.* [KO18, Theorem 1.3 (i)–(v)]):

Hyp 1

(i) The curve E/L has good reduction at all primes in S_p;

Denote by $S^{\mathrm{ss}} \subseteq S_p$ the set of primes above p where E has supersingular reduction.

(ii) S^{ss} is non-empty;

(iii) all primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_d$ in S^{ss} split completely in $\mathrm{L}/\mathbb{Q}$, so $\mathrm{L}_{\mathfrak{p}_i} \cong \mathbb{Q}_p$ for all $1 \leq i \leq d$;

(iv) $1 + p - |\widetilde{\mathsf{E}}(\mathbb{F}_{\mathfrak{p}_i})| = 0$, where $\widetilde{\mathsf{E}}$ is the reduction of E modulo any of the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_d$ and $\mathbb{F}_{\mathfrak{p}_i}$ denotes the residue field of $\mathfrak{p}_i$.

(v) The ramification index $e(\pi)$ in the extension $\mathrm{L}/\mathbb{Q}$ of every prime $\pi \in S_p$ where E has good, ordinary reduction, is at most $p - 1$.

Remark 2.1. Kitajima and Otsuki work in a slightly greater generality, allowing the supersingular primes to be simply unramified in $\mathrm{L}/\mathbb{Q}$, provided the curve is defined over a subfield where they split completely.

Points (i)–(iv) in **Hyp 1** ensure that the signed Selmer groups are defined (see Section 3). Point (v) in **Hyp 1** ensures that the fine signed residual Selmer group depends only on the residual Galois representation E_p (*cf*. Proposition 3.8 and Proposition 3.9).

Let us set the notation that will be used in the paper.

Notation 2.2. The set S_p of primes above p is the disjoint union $S_p = S^{\mathrm{ss}} \coprod S^{\mathrm{ord}}$, where $S^{\mathrm{ord}} = \{\pi_1, \dots, \pi_s\}$ is the (possibly empty) set of primes where E has good, ordinary reduction. Consider the cyclotomic $\mathbb{Z}_p$-extension $\mathrm{L}_{\mathrm{cyc}}/\mathrm{L}$ of L, with intermediate layers L_n, for $n \geq 0$, so that $\mathrm{Gal}(\mathrm{L}_n/\mathrm{L}) \cong \mathbb{Z}/p^n\mathbb{Z}$ and $\mathrm{L}_0 = \mathrm{L}$. By **Hyp 1**, all primes $\mathfrak{p}_i \in S^{\mathrm{ss}}$ split in L, so they are all totally ramified in $\mathrm{L}_{\mathrm{cyc}}/\mathrm{L}$. Let $\mathfrak{p}_{n,i}$ denote the prime ideal of L_n above $\mathfrak{p}_i$, for $1 \leq i \leq d$ and let $\mathcal{L}_{n,i}$ be the localisation of L_n at $\mathfrak{p}_{n,i}$. For ease of notation, we often suppress the index i since these fields, for fixed n, are all isomorphic to the nth layer of the cyclotomic extension of $\mathcal{L}_0 \cong \mathbb{Q}_p$. In particular, $\mathcal{L}_{\mathrm{cyc},i} \cong (\mathbb{Q}^{\mathrm{cyc}})_{\mathfrak{p}_{\mathrm{cyc},i}}$. We also need to consider the fields obtained by adjoining p-power order roots of unity to $\mathcal{L}_{0,i} = \mathcal{L}_0$. Set $\Bbbk_n = \mathcal{L}_0(\zeta_{p^{n+1}})$, for $n \geq -1$, where $\zeta_{p^{n+1}}$ is a primitive p^{n+1}th root of unity. For all $n \geq -1$, we let $\mathfrak{m}_n$ be the maximal ideal of $\Bbbk_n$. In particular, $\Bbbk_{-1} \cong \mathbb{Q}_p$ and $\mathfrak{m}_{-1} \cong p\mathbb{Z}_p$. The Galois group $\mathrm{Gal}(\Bbbk_0/\mathcal{L}_0)$ is denoted by Δ. It is isomorphic to $\mathrm{Gal}(\Bbbk_n/\mathcal{L}_n)$ for all $n \geq 0$, and we tacitly identify these groups throughout.

Let $S = S_p \coprod S^{\mathrm{bad}}$ where $S^{\mathrm{bad}} = \{\mathfrak{l}_1, \dots, \mathfrak{l}_r\}$ is the finite set of primes of bad reduction for E/L. The maximal extension of L unramified outside of S will be denoted L^S. We usually write v or w to denote generic primes above S in an extension of L. Given an extension L'/L, we sometimes abuse notation and again denote by S the primes of L' above primes in S. When we need to specify the field, we write $S^*_{\mathrm{L}'}$ for $* \in \{\emptyset, \mathrm{ord}, \mathrm{ss}, \mathrm{bad}\}$ to denote the sets of primes of L' above primes in S^*.

Given any field $K \in \{\mathrm{L}_n, \mathrm{L}_{n,v}, \Bbbk_n\}$ (for some $0 \leq n < \infty$ and possibly some prime $v \in S$ of L_n), its ring of integers will be denoted by $\mathcal{O}_K$; when K is a local field, we further denote its residue field by $\mathbb{F}_v$. For K as above, write $\widetilde{K} = \mathrm{L}^S$ if $K = \mathrm{L}_n$, $\widetilde{K} = \overline{\Bbbk_n} = \overline{\mathbb{Q}_p}$ if $K = \Bbbk_n$ and $\widetilde{K} = (\mathrm{L}^S)_w = \overline{\mathrm{L}_{n,v}}$, for some extension $w \mid v$, when $K = \mathrm{L}_{n,v}$. The corresponding Galois groups $\mathrm{Gal}(\widetilde{K}/K)$ are denoted, respectively, by $\mathscr{G}_n^S$, $G_{\Bbbk_n}$ and $G_{\mathrm{L}_{n,v}}$; in case $v = \mathfrak{p}_i$, this will be denoted $G_{\mathcal{L}_i}$. When $K \in \{\mathrm{L}_{n,v}, \Bbbk_n\}$, and M is any Galois module, we usually write $\mathrm{H}^i(K, M)$ to denote the cohomology group $\mathrm{H}^i(\mathrm{Gal}(\widetilde{K}/K), M)$.

The Galois module of p^t-torsion points of E is denoted E_{p^t}, and more generally M_{p^t} will denote the submodule consisting of the p^t-torsion elements in M. By a slight abuse of notation, $\widetilde{\mathsf{E}}/\mathbb{F}_p$ is the reduction of E modulo any of the prime ideals $\mathfrak{p}_i$, all the reductions being isomorphic. Similarly, $\mathcal{E}$ is the formal group of E over $\mathbb{Z}_p = \mathcal{O}_{\mathcal{L}_0}$. As discussed in [Kob03, Corollary 8.5] and [KO18, § 3.1], there is a $\mathbb{Z}_p$-isomorphism $\mathcal{E} \cong \mathcal{F}_{\mathrm{ss}}$ between the formal group of $\mathsf{E}/\mathbb{Z}_p$ and the supersingular formal group $\mathcal{F}_{\mathrm{ss}}$ whose logarithm of Honda type $t^2 + p$ (the group $\mathcal{F}_{\mathrm{ss}}$ is denoted by $\mathcal{G}$ in [KO18]: in our setting the automorphism φ in *loc. cit*. is trivial).

3. Plus and minus decomposition

3.1. **The signed Kummer maps.** The aim of this section is to gather some results about the plus/minus decomposition, mainly taken from [KO18], which in turn relies on [Kob03]. Most of the results mentioned below are either well-known or easy adaptations to the finite Galois module of p-torsion points, of arguments which are normally stated for the divisible module of p^∞-torsion points.

We start with a general remark about vanishing of global torsion points for E along the cyclotomic extension.

Proposition 3.1. *For every $n \geq 0$, the torsion subgroup $\mathcal{E}(\mathfrak{m}_n)_p$ is trivial. In particular,*

$$\mathsf{E}(\Bbbk_n)_p = \mathsf{E}(\mathcal{L}_n)_p = \mathsf{E}(\mathrm{L}_n)_p = \{0\} \qquad \textit{for all } n \geq 0.$$

Proof. See [KO18, Proposition 3.1]. □

Following the pivotal works [PR90] and [Kob03] by Perrin-Riou and Kobayashi, respectively, we now define plus/minus subgroups of the local points, as follows.

Definition 3.2 ([KO18, Definitions 2.1 and 3.13])**.** With notations as above we denote, for every $n \geq 1$,

$$\mathcal{E}^+(\mathfrak{m}_n) = \{P \in \mathcal{E}(\mathfrak{m}_n) \mid \mathrm{Tr}^n_{m+1}(P) \in \mathcal{E}(\mathfrak{m}_m) \text{ for all } -1 \leq m \leq n-1, m \text{ even}\}$$

and

$$\mathcal{E}^-(\mathfrak{m}_n) = \{P \in \mathcal{E}(\mathfrak{m}_n) \mid \mathrm{Tr}^n_{m+1}(P) \in \mathcal{E}(\mathfrak{m}_m) \text{ for all } -1 \leq m \leq n-1, m \text{ odd}\}$$

Similarly, we set

$$\mathsf{E}^+(\Bbbk_n) = \{P \in \mathsf{E}(\Bbbk_n) \mid \mathrm{Tr}^n_{m+1}(P) \in \mathsf{E}(\Bbbk_m) \text{ for all } -1 \leq m \leq n-1, m \text{ evem}\}$$

and

$$\mathsf{E}^-(\Bbbk_n) = \{P \in \mathsf{E}(\Bbbk_n) \mid \mathrm{Tr}^n_{m+1}(P) \in \mathsf{E}(\Bbbk_m) \text{ for all } -1 \leq m \leq n-1, m \text{ odd}\}$$

and we let $\mathsf{E}^\pm(\mathcal{L}_n) = \mathsf{E}^\pm(\Bbbk_n)^\Delta = \mathrm{H}^0(\Delta, \mathsf{E}^\pm(\Bbbk_n))$.

The next lemma compares the formal signed subgroups of local points with the whole signed subgroups:

Lemma 3.3 (see [KO18, Lemma 3.14])**.** *Let $\mathfrak{p} = \mathfrak{p}_i \in S^{\mathrm{ss}}$ and let $\mathcal{L} = \mathcal{L}_{0,i}$. For all $n \geq 1$ there are exact sequences*

$$0 \longrightarrow \mathcal{E}^\pm(\mathfrak{m}_n) \longrightarrow \mathsf{E}^\pm(\Bbbk_n) \longrightarrow \mathcal{D}^\pm_n \longrightarrow 0 \tag{1}$$

where $\mathcal{D}^\pm_n \subseteq \widetilde{\mathsf{E}}(\mathbb{F}_p)$ is a finite group, of prime-to-p order bounded independently of n.

More generally, if $K/\mathcal{L}$ is any algebraic extension and $\mathfrak{m}_K$ is the maximal ideal of its valuation ring, there is an exact sequence

$$0 \longrightarrow \mathcal{E}(\mathfrak{m}_K) \longrightarrow \mathsf{E}(K) \longrightarrow D \longrightarrow 0 \tag{2}$$

where D is a finite group of prime-to-p order, inducing an isomorphism

$$\mathcal{E}(\mathfrak{m}_{\overline{\mathbb{Q}_p}})_{p^\infty} \cong \mathsf{E}(\overline{\mathbb{Q}_p})_{p^\infty}.$$

Proof. Fix $m \geq -1$ and consider the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{E}(\mathfrak{m}_m) & \longrightarrow & \mathsf{E}(\Bbbk_m) & \longrightarrow & \widetilde{\mathsf{E}}(\mathbb{F}_p) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \| & & \\ 0 & \longrightarrow & \mathcal{E}(\mathfrak{m}_{m+1}) & \longrightarrow & \mathsf{E}(\Bbbk_{m+1}) & \longrightarrow & \widetilde{\mathsf{E}}(\mathbb{F}_p) & \longrightarrow & 0 \end{array}$$

which induces, by the snake lemma, an isomorphism

$$\mathcal{E}(\mathfrak{m}_{m+1})/\mathcal{E}(\mathfrak{m}_m) \xrightarrow{\cong} \mathsf{E}(\Bbbk_{m+1})/\mathsf{E}(\Bbbk_m).$$

Now fix $n \geq m+1$: the above sequence fits into the commutative diagram of exact sequences

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \ker \widehat{\mathrm{Tr}^n_{m+1}} & \longrightarrow & \ker \overline{\mathrm{Tr}^n_{m+1}} & \longrightarrow & \widetilde{\mathsf{E}}(\mathbb{F}_p) & & \\
 & & \downarrow & & \downarrow & & \| & & \\
0 & \longrightarrow & \mathcal{E}(\mathfrak{m}_n) & \longrightarrow & \mathsf{E}(\mathbb{k}_n) & \longrightarrow & \widetilde{\mathsf{E}}(\mathbb{F}_p) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \widehat{\mathrm{Tr}^n_{m+1}}} & & \downarrow{\scriptstyle \overline{\mathrm{Tr}^n_{m+1}}} & & \downarrow & & \\
0 & \longrightarrow & \mathcal{E}(\mathfrak{m}_{m+1})/\mathcal{E}(\mathfrak{m}_m) & \xrightarrow{\cong} & \mathsf{E}(\mathbb{k}_{m+1})/\mathsf{E}(\mathbb{k}_m) & \longrightarrow & 0 & \longrightarrow & 0
\end{array}$$

where $\widehat{\mathrm{Tr}^n_{m+1}}$ (*resp.* $\overline{\mathrm{Tr}^n_{m+1}}$) denotes the trace map followed by reduction modulo $\mathcal{E}(\mathfrak{m}_{m+1})$ (*resp.* modulo $\mathsf{E}(\mathbb{k}_{m+1})$). In particular, we deduce that $\ker \widehat{\mathrm{Tr}^n_{m+1}}$ is a subgroup of $\ker \overline{\mathrm{Tr}^n_{m+1}}$ with quotient contained inside $\widetilde{\mathsf{E}}(\mathbb{F}_p)$, for every $m \leq n-1$. Taking intersections, we find

$$\mathcal{E}^{\pm}(\mathfrak{m}_n) = \bigcap_{\substack{(-1)^m=\pm 1 \\ -1\leq m\leq n-1}} \ker \widehat{\mathrm{Tr}^n_{m+1}} \qquad \text{and} \qquad \mathsf{E}^{\pm}(\mathbb{k}_n) = \bigcap_{\substack{(-1)^m=\pm 1 \\ -1\leq m\leq n-1}} \ker \overline{\mathrm{Tr}^n_{m+1}}$$

and therefore an exact sequence

$$0 \longrightarrow \mathcal{E}^{\pm}(\mathfrak{m}_n) \longrightarrow \mathsf{E}^{\pm}(\mathbb{k}_n) \longrightarrow \mathcal{D}^{\pm}_n \longrightarrow 0$$

for some $\mathcal{D}^{\pm}_n \subseteq \widetilde{\mathsf{E}}(\mathbb{F}_p)$. Since E has supersingular reduction at $\mathfrak{p}$, the order of $\widetilde{\mathsf{E}}(\mathbb{F}_p)$ is prime-to-p.

The final isomorphism is simply a translation of the fact that $\widetilde{\mathsf{E}}(\overline{\mathbb{F}_p})$ has no p-torsion. Using the exact sequence

$$0 \longrightarrow \mathcal{E}(\mathfrak{m}_K) \longrightarrow \mathsf{E}(K) \longrightarrow \widetilde{\mathsf{E}}(\mathcal{O}_K/\mathfrak{m}_K) \longrightarrow 0,$$

one obtains

$$\mathcal{E}(\mathfrak{m}_K)_{p^\infty} \cong \mathsf{E}(K)_{p^\infty}$$

and taking direct limit over all $\mathcal{L} \subseteq K \subseteq \overline{\mathbb{Q}_p}$, we deduce the isomorphism in the statement. □

Let $K \in \{\mathrm{L}_n, \mathbb{k}_n, \mathrm{L}_{n,v}\}$ and $G \in \{\mathscr{G}^S_n, G_{\mathbb{k}_n}, G_{\mathrm{L}_{n,v}}\}$. Recall that for each integer $t \geq 0$, there exists the following functorial exact sequence for E_{p^t}/K

$$0 \longrightarrow \mathsf{E}(K)/p^t\mathsf{E}(K) \xrightarrow{\kappa_K^{p^t}} \mathrm{H}^1(G, \mathsf{E}_{p^t}) \longrightarrow \mathrm{H}^1(G, \mathsf{E})_{p^t} \longrightarrow 0$$

where $\kappa_K^{p^t}$ is the Kummer map.

Lemma 3.4 (see [Kob03, Lemma 8.17]). *For every $n \geq 1$ and every $t \geq 1$, there is an injection*

$$\mathsf{E}^{\pm}(\mathcal{L}_n)/p^t\mathsf{E}^{\pm}(\mathcal{L}_n) \hookrightarrow \mathsf{E}(\mathcal{L}_n)/p^t\mathsf{E}(\mathcal{L}_n)$$

which induces injections

$$\kappa^{\pm,p^t}_{\mathcal{L}_n} : \mathsf{E}^{\pm}(\mathcal{L}_n)/p^t\mathsf{E}^{\pm}(\mathcal{L}_n) \hookrightarrow \mathrm{H}^1(\mathcal{L}_n, \mathsf{E}_{p^t}).$$

Similarly, there are injections

$$\kappa^{\pm,p^t}_{\mathcal{L}_n} : \mathcal{E}^{\pm}(\mathfrak{m}^{\Delta}_n)/p^t\mathcal{E}^{\pm}(\mathfrak{m}^{\Delta}_n) \hookrightarrow \mathrm{H}^1(\mathcal{L}_n, \mathcal{E}_{p^t}).$$

Proof. Let us first show that

$$\mathsf{E}^{\pm}(\Bbbk_n)/p^t\mathsf{E}^{\pm}(\Bbbk_n) \hookrightarrow \mathsf{E}(\Bbbk_n)/p^t\mathsf{E}(\Bbbk_n) \tag{3}$$

is injective. An element in

$$\ker\Big(\mathsf{E}^{\pm}(\Bbbk_n)/p^t\mathsf{E}^{\pm}(\Bbbk_n) \longrightarrow \mathsf{E}(\Bbbk_n)/p^t\mathsf{E}(\Bbbk_n)\Big)$$

is represented by a point $P \in \mathsf{E}^{\pm}(\Bbbk_n)$ such that $P = p^tQ$ for some $Q \in \mathsf{E}(\Bbbk_n)$. Choose now $m \leq n-1$ such that $(-1)^m = \pm 1$. Taking the trace of P down to $\Bbbk_{m+1}$ we obtain that $\mathrm{Tr}^n_{m+1}(P) \in \mathsf{E}(\Bbbk_m)$, by definition of $\mathsf{E}^{\pm}$. On the other hand, $\mathrm{Tr}^n_{m+1}(P) = p^t\,\mathrm{Tr}^n_{m+1}(Q)$, hence for all $\sigma \in \mathrm{Gal}(\Bbbk_{m+1}/\Bbbk_m)$ we have $p^t({}^{\sigma}\mathrm{Tr}^n_{m+1}(Q) - \mathrm{Tr}^n_{m+1}(Q)) = 0$. Thus $\mathrm{Tr}^n_{m+1}(Q) \in \mathsf{E}(\Bbbk_m)$ thanks to Proposition 3.1, which implies $Q \in \mathsf{E}^{\pm}(\Bbbk_n)$ and the arrow in (3) is injective. For each $* \in \{\emptyset, +, -\}$, taking Δ-cohomology of the tautological exact sequence defining $\mathsf{E}^*(\Bbbk_n)/p^t\mathsf{E}^*(\Bbbk_n)$ gives

$$0 \longrightarrow \mathsf{E}^*(\mathcal{L}_n) \xrightarrow{\cdot p^t} \mathsf{E}^*(\mathcal{L}_n) \longrightarrow \mathrm{H}^0\big(\Delta, \mathsf{E}^*(\Bbbk_n)/p^t\mathsf{E}^*(\Bbbk_n)\big) \longrightarrow \mathrm{H}^1(\Delta, \mathsf{E}^*(\mathcal{L}_n))_{p^t} \longrightarrow 0.$$

The last module is trivial, because Δ has order prime-to-p, so

$$\mathrm{H}^0\big(\Delta, \mathsf{E}^*(\Bbbk_n)/p^t\mathsf{E}^*(\Bbbk_n)\big) = \mathsf{E}^*(\mathcal{L}_n)/p^t\mathsf{E}^*(\mathcal{L}_n). \tag{4}$$

Taking Δ-invariants of the injections in (3) establishes the first part of the lemma. The second is analogous, upon replacing $\mathsf{E}^{\pm}$ with $\mathcal{E}^{\pm}$. □

In light of the above Lemma, we can define, for all $n \geq 0$ (and all $\mathfrak{p}_i$ if we need to keep track of the local Galois groups), the *signed* Kummer sequence as the exact sequence

$$0 \longrightarrow \mathsf{E}^{\pm}(\mathcal{L}_n)/p^t\mathsf{E}^{\pm}(\mathcal{L}_n) \xrightarrow{\kappa^{\pm,p^t}_{\mathcal{L}_n}} \mathrm{H}^1(G_{\mathcal{L}_n}, \mathsf{E}_{p^t}) \longrightarrow \mathrm{H}^1(G_{\mathcal{L}_n}, \mathsf{E}_{p^t})/\operatorname{Im}\kappa^{\pm,p^t}_{\mathcal{L}_n} \longrightarrow 0 \tag{5}$$

and refer to $\kappa^{\pm,p^t}_K$ as the *signed* Kummer map. Analogous signed Kummer exact sequence can be defined for the formal group $\mathcal{E}$, as follows:

$$0 \longrightarrow \mathcal{E}^{\pm}(\mathcal{L}_n)/p^t\mathcal{E}^{\pm}(\mathfrak{m}_n^{\Delta}) \xrightarrow{\kappa^{\pm,p^t}_{\mathcal{L}_n}} \mathrm{H}^1(G_{\mathcal{L}_n}, \mathcal{E}_{p^t}) \longrightarrow \mathrm{H}^1(G_{\mathcal{L}_n}, \mathcal{E}_{p^t})/\kappa^{\pm,p^t}_{\mathcal{L}_n}\big(\mathcal{E}^{\pm}(\mathfrak{m}_n^{\Delta})\big) \longrightarrow 0 \tag{6}$$

Remark 3.5. It is perhaps interesting to stress that the signed Kummer map defined in (5) *does not arise* as a connecting homomorphism in Galois cohomology. Indeed, $\mathsf{E}^{\pm}$ is only defined at the level of points for extensions in the cyclotomic tower and it is not a sub-representation of E, since in the supersingular case the local Galois representation E_{p^∞} is irreducible.

3.2. **The signed Selmer groups.** We use the notation introduced in 2.2. For generalities regarding the classical Selmer group for $\mathsf{E}_{p^t}/\mathrm{L}_n$ (for $1 \leq t < \infty$) and for $\mathsf{E}_{p^\infty}/\mathrm{L}_n$ we refer to [CS10, Chapters 1 and 2]. They are defined as

$$\begin{aligned}
\mathrm{Sel}(\mathsf{E}_{p^t}/\mathrm{L}_n) &= \ker\Big(\mathrm{H}^1(\mathscr{G}^S_n, \mathsf{E}_{p^t}) \longrightarrow \bigoplus_{v \in S_{\mathrm{L}_n}} \mathrm{H}^1(\mathrm{L}_{n,v}, \mathsf{E})_{p^t}\Big) \\
&= \ker\Big(\mathrm{H}^1(\mathscr{G}^S_n, \mathsf{E}_{p^t}) \longrightarrow \bigoplus_{v \in S_{\mathrm{L}_n} \setminus S^{\mathrm{ss}}_{\mathrm{L}_n}} \mathrm{H}^1(\mathrm{L}_{n,v}, \mathsf{E})_{p^t} \oplus \bigoplus_{i=1}^{d} \mathrm{H}^1(\mathcal{L}_{n,i}, \mathsf{E})_{p^t}\Big) \\
&= \ker\Big(\mathrm{H}^1(\mathscr{G}^S_n, \mathsf{E}_{p^t}) \longrightarrow \bigoplus_{v \in S_{\mathrm{L}_n} \setminus S^{\mathrm{ss}}_{\mathrm{L}_n}} \mathrm{H}^1(\mathrm{L}_{n,v}, \mathsf{E}_{p^t})/\operatorname{Im}\kappa^{p^t}_{\mathcal{L}_{n,i}} \oplus \bigoplus_{i=1}^{d} \mathrm{H}^1(\mathcal{L}_{n,i}, \mathsf{E}_{p^t})/\operatorname{Im}\kappa^{p^t}_{\mathcal{L}_{n,i}}\Big)
\end{aligned}$$

where we isolate the local terms at primes in S^{ss} for future comparison with signed Selmer groups. Passing to the limit over t, one defines

$$\mathrm{Sel}(\mathsf{E}_{p^\infty}/\mathrm{L}_n) = \varinjlim_t \mathrm{Sel}(\mathsf{E}_{p^t}/\mathrm{L}_n).$$

In the supersingular reduction case, the Iwasawa theory of the signed Selmer groups as initially defined by Perrin-Riou and Kobayashi respectively in [PR90] and [Kob03] is of particular interest. The residual signed Selmer groups are defined below and we postpone a larger discussion, from the Iwasawa-theoretic point of view, to Section 4. Our main reference is the work [KO18] by Kitajima–Otsuki.

Definition 3.6. For every intermediate number field $\mathrm{L} \subseteq \mathrm{L}_n \subsetneq \mathrm{L}_{\mathrm{cyc}}$ define the *fine signed residual Selmer group* as

$$\mathcal{R}^{\pm}(\mathsf{E}_p/\mathrm{L}_n) = \ker\Big(\mathrm{H}^1(\mathscr{G}_n^S, \mathsf{E}_p) \to \bigoplus_{\mathfrak{l}\in S^{\mathrm{bad}}_{\mathrm{L}_n}} \mathrm{H}^1(\mathrm{L}_{n,\mathfrak{l}}, \mathsf{E}_p) \oplus \bigoplus_{\pi\in S^{\mathrm{ord}}_{\mathrm{L}_n}} \mathrm{H}^1(\mathrm{L}_{n,\pi}, \widetilde{\mathsf{E}}_p) \oplus \bigoplus_{i=1}^{d} \mathrm{H}^1(\mathcal{L}_{n,i}, \mathsf{E}_p)/\operatorname{Im}\kappa^{\pm,p}_{\mathcal{L}_{n,i}}\Big),$$

where, at an ordinary prime π, $\widetilde{\mathsf{E}}_p$ is seen as a $G_{\mathrm{L}_{n,\pi}}$-module through the surjection $G_{\mathrm{L}_{n,\pi}} \twoheadrightarrow G^{\mathrm{ur}}_{\mathrm{L}_{n,\pi}} = G_{\mathbb{F}_\pi}$. Similarly, the *usual signed Selmer group* is defined as

$$\mathrm{Sel}^{\pm}(\mathsf{E}_{p^\infty}/\mathrm{L}_n) = \ker\Big(\mathrm{H}^1(\mathscr{G}_n^S, \mathsf{E}_{p^\infty}) \to \bigoplus_{v\in S_{\mathrm{L}_n}\setminus S^{\mathrm{ss}}_{\mathrm{L}_n}} \mathrm{H}^1(\mathrm{L}_{n,v}, \mathsf{E})_{p^\infty} \oplus \bigoplus_{i=1}^{d} \mathrm{H}^1(\mathcal{L}_{n,i}, \mathsf{E}_{p^\infty})/\operatorname{Im}\kappa^{\pm,p^\infty}_{\mathcal{L}_{n,i}}\Big).$$

The rationale for the nomenclature in this definition is that $\mathcal{R}^{\pm}(\mathsf{E}_p/\mathrm{L}_n)$ contains the usual fine Selmer group for E_p. As the notation suggests, these fine residual signed Selmer groups only depend upon the isomorphism class of E_p rather than on the curve E itself, at least when assuming **Hyp 1**. This is the content of Corollary 4.3, which relies on Proposition 3.8 and Proposition 3.9 below.

We start with the following technical lemma:

Lemma 3.7. *Fix $n \geq 0$ and let $G \in \{\mathscr{G}_n^S, G_{\mathcal{L}_n}, G_{\mathrm{L}_{n,\mathfrak{l}}}\}$ for some $\mathfrak{l} \in S^{\mathrm{bad}}$. Denote by $\psi_{G,n} = \psi_n$ the natural surjective arrow*

$$\psi_n\colon \mathrm{H}^1(G, \mathsf{E}_p) \longrightarrow \mathrm{H}^1(G, \mathsf{E}_{p^\infty})_p.$$

For $\pi \in S^{\mathrm{ord}}$ and $G = G_{\mathrm{L}_{n,\pi}}$ let

$$\widetilde{\psi_{G,n}} = \widetilde{\psi_n}\colon \mathrm{H}^1(G, \widetilde{\mathsf{E}}_p) \longrightarrow \mathrm{H}^1(G, \widetilde{\mathsf{E}}_{p^\infty})_p$$

be the analogous surjection for the Galois representation $\widetilde{\mathsf{E}}_{p^\infty}$. Then the following assertions hold.

- *i) If $G \in \{\mathscr{G}_n^S, G_{\mathcal{L}_n}\}$, then ψ_n is an isomorphism.*
- *ii) If $G = G_{\mathrm{L}_{n,\mathfrak{l}}}$ for some $\mathfrak{l} \in S^{\mathrm{bad}}$, then $\ker\psi_n$ is an $\mathbb{F}_p$-vector space of dimension $\dim_{\mathbb{F}_p}(\ker\psi_n) = \dim_{\mathbb{F}_p}\mathsf{E}(\mathrm{L}_{n,\mathfrak{l}})_p \leq 2$.*
- *iii) If $G = G_{\mathrm{L}_{n,\pi}}$ for some $\pi \in S^{\mathrm{ord}}$, then $\ker\widetilde{\psi_n}$ is an $\mathbb{F}_p$-vector space of dimension $\dim_{\mathbb{F}_p}(\ker\widetilde{\psi_n}) = \dim_{\mathbb{F}_p}\widetilde{\mathsf{E}}(\mathrm{L}_{n,\pi})_p \leq 1$.*

Proof. Taking G-cohomology of the exact sequence

$$0 \longrightarrow \mathsf{E}_p \longrightarrow \mathsf{E}_{p^\infty} \longrightarrow \mathsf{E}_{p^\infty} \longrightarrow 0 \tag{7}$$

gives an exact sequence

$$0 \longrightarrow \ker\psi_n = \mathrm{H}^0(G, \mathsf{E}_{p^\infty})/p\,\mathrm{H}^0(G, \mathsf{E}_{p^\infty}) \longrightarrow \mathrm{H}^1(G, \mathsf{E}_p) \xrightarrow{\psi_n} \mathrm{H}^1(G, \mathsf{E}_{p^\infty})_p \longrightarrow 0. \tag{8}$$

When $G \in \{\mathscr{G}_n^S, G_{\mathcal{L}_n}\}$, the first term in (8) is trivial thanks to Proposition 3.1 and assertion ii) follows.

When $G = G_{\mathrm{L}_{n,\mathfrak{l}}}$ for some $\mathfrak{l} \in S^{\mathrm{bad}}$, the first term in (8) has $\mathbb{F}_p$-dimension equal to $\dim_{\mathbb{F}_p} \mathsf{E}(\mathrm{L}_{n,\mathfrak{l}})_p$, since $\mathsf{E}(\mathrm{L}_{n,\mathfrak{l}})_{p^\infty}$ is finite. Moreover, the group $\mathrm{H}^0(G, \mathsf{E}_p)$ is a subgroup of $\mathsf{E}(\overline{\mathrm{L}_{\mathfrak{l}}})_p \cong (\mathbb{F}_p)^2$. This shows that this dimension is bounded by 2, whence assertion ii).

Finally, when $G = G_{\mathrm{L}_{n,\pi}}$ for some $\pi \in S^{\mathrm{ord}}$, replace (7) by

$$0 \longrightarrow \widetilde{\mathsf{E}}_p \longrightarrow \widetilde{\mathsf{E}}_{p^\infty} \longrightarrow \widetilde{\mathsf{E}}_{p^\infty} \longrightarrow 0$$

to obtain an exact sequence

$$0 \longrightarrow \ker \widetilde{\psi_n} = \mathrm{H}^0(G, \widetilde{\mathsf{E}}_{p^\infty})/p\,\mathrm{H}^0(G, \widetilde{\mathsf{E}}_{p^\infty}) \longrightarrow \mathrm{H}^1(G, \widetilde{\mathsf{E}}_p) \xrightarrow{\widetilde{\psi_n}} \mathrm{H}^1(G, \widetilde{\mathsf{E}}_{p^\infty})_p \longrightarrow 0. \tag{9}$$

The first term in (9) is a $\mathbb{F}_p$-vector space of dimension bounded by $\dim_{\mathbb{F}_p} \widetilde{\mathsf{E}}(\overline{\mathbb{F}_\pi})_{p^\infty}/p\widetilde{\mathsf{E}}(\overline{\mathbb{F}_\pi})_{p^\infty} \cong \mathbb{F}_p$. This finishes the proof. □

Let us now move to the proof that the local conditions in the definition of the fine residual signed Selmer group depend only on the residual representation also for primes above p, beginning with supersingular primes. Under our standing assumption **Hyp 1**, E is supersingular at all primes $\mathfrak{p}_1, \dots, \mathfrak{p}_d$ and the exact sequence (2) induces an isomorphism $\mathrm{H}^1(\mathcal{L}_{n,i}, \mathsf{E}_{p^\infty}) \cong \mathrm{H}^1(\mathcal{L}_{n,i}, \mathcal{E}_{p^\infty})$, for all $n \geq 0$. On the other hand, the exact sequence (1) shows that the images of the signed Kummer maps $\kappa_{\mathcal{L}_{n,i}}^{\pm,p^\infty}\big(\mathsf{E}^\pm(\mathcal{L}_{i,n})\big)$ and $\kappa_{\mathcal{L}_{n,i}}^{\pm,p^\infty}\big(\mathcal{E}^\pm(\mathfrak{m}_n^\Delta)\big)$ are isomorphic. It is straightforward to check that these isomorphisms are compatible, and in turn induce isomorphisms

$$\mathrm{H}^1(\mathcal{L}_{n,i}, \mathsf{E}_{p^\infty})/\operatorname{Im}(\kappa_{\mathcal{L}_{n,i}}^{\pm,p^\infty}) \cong \mathrm{H}^1(\mathcal{L}_{n,i}, \mathcal{E}_{p^\infty})/\kappa_{\mathcal{L}_{n,i}}^{\pm,p^\infty}\big(\mathcal{E}^\pm(\mathfrak{m}_n^\Delta)\big). \tag{10}$$

As discussed in [Kob03, Corollary 8.5] and [KO18, § 3.1], there is a $\mathcal{O}_{\mathcal{L}_0} = \mathbb{Z}_p$-isomorphism

$$\log_{\mathcal{F}_{\mathrm{ss}}} \circ \exp_{\mathcal{E}} : \mathcal{E} \xrightarrow{\cong} \mathcal{F}_{\mathrm{ss}} \tag{11}$$

where $\mathcal{F}_{\mathrm{ss}}$ is the supersingular formal group whose logarithm $\log_{\mathcal{F}_{\mathrm{ss}}}$ is of Honda type $t^2 + p$. In particular, the isomorphism class of the formal group $\mathcal{E}$ is independent of the curve E, whenever the curve satisfies **Hyp 1**. Moreover, for every n there are two subgroups $\mathcal{F}_{\mathrm{ss}}^\pm(\mathfrak{m}_n) \subseteq \mathcal{F}_{\mathrm{ss}}(\mathfrak{m}_n)$ defined by the same norm relations defining $\mathcal{E}^\pm$ (see Definition 3.2), but for points on the formal group $\mathcal{F}_{\mathrm{ss}}$ rather than $\mathcal{E}$. Equivalently, they are defined as

$$\mathcal{F}_{\mathrm{ss}}^\pm(\mathfrak{m}_n) = (\log_{\mathcal{F}_{\mathrm{ss}}} \circ \exp_{\mathcal{E}})\big(\mathcal{E}^\pm(\mathfrak{m}_n)\big).$$

Therefore, as subgroups of $\mathcal{F}_{\mathrm{ss}}(\mathfrak{m}_n)$, they are independent of E for all $n \geq 0$. Moreover, there is an evident definition of the analogues of the signed Kummer sequence (6) for $\mathcal{F}_{\mathrm{ss}}$ and $\mathcal{F}_{\mathrm{ss}}^\pm$ instead of $\mathcal{E}$. Combining (10) with (11) gives

$$\mathrm{H}^1(\mathcal{L}_{n,i}, \mathsf{E}_{p^\infty})/\operatorname{Im}(\kappa_{\mathcal{L}_{n,i}}^{\pm,p^\infty}) \cong \mathrm{H}^1(\mathcal{L}_{n,i}, (\mathcal{F}_{\mathrm{ss}})_{p^\infty})/\kappa_{\mathcal{L}_{n,i}}^{\pm,p^\infty}\big(\mathcal{F}_{\mathrm{ss}}^\pm(\mathfrak{m}_n^\Delta)\big),$$

where the right-hand side does not depend on E. We summarise the above discussion in the following

Proposition 3.8. *Let E/L be an elliptic curve satisfying hypothesis **Hyp 1**. For all $1 \leq i \leq d$ and all $n \geq 0$, there are functorial isomorphisms*

$$\mathrm{H}^1(\mathcal{L}_{n,i}, \mathsf{E}_{p^\infty})/\operatorname{Im}(\kappa_{\mathcal{L}_{n,i}}^{\pm,p^\infty}) \cong \mathrm{H}^1(\mathcal{L}_{n,i}, (\mathcal{F}_{\mathrm{ss}})_{p^\infty})/\kappa_{\mathcal{L}_{n,i}}^{\pm,p^\infty}\big(\mathcal{F}_{\mathrm{ss}}^\pm(\mathfrak{m}_n^\Delta)\big)$$

In particular, the modules $\mathrm{H}^1(\mathcal{L}_{n,i}, \mathsf{E}_{p^\infty})/\operatorname{Im}(\kappa_{\mathcal{L}_{n,i}}^{\pm,p^\infty})$ are independent of E, since the right-hand sides are.

Proof. The fact that the first isomorphism is functorial follows from Honda theory, which shows that the isomorphism between $\mathcal{F}_{\mathrm{ss}}$ and $\mathcal{E}$ is given by $\log_{\mathcal{E}} \circ \exp_{\mathcal{F}_{\mathrm{ss}}}$ (see [Kob03, Theorem 8.3 (ii)]). □

What remains to be proven is the analogue of the above result when replacing E_{p^∞} by E_p, which is the module we are ultimately interested in. This is done in Proposition 4.1-d), as we move up the cyclotomic tower. Concerning ordinary primes, we have the following result.

Proposition 3.9. *Let $\mathsf{E}_1, \mathsf{E}_2$ be two elliptic curves defined over L satisfying hypothesis **Hyp 1**. Let S_j^{ss}* (resp. S_j^{ord}) *denote the set of primes where E_j has supersingular* (resp. *ordinary*) *reduction, for $j = 1, 2$. Then*

i) $S_1^{\mathrm{ss}} = S_2^{\mathrm{ss}}$ and $S_1^{\mathrm{ord}} = S_2^{\mathrm{ord}}$. Denote these sets simply by S^{ss} and S^{ord}, respectively.

ii) Every isomorphism $(\mathsf{E}_1)_p \cong (\mathsf{E}_2)_p$ induces an isomorphism $(\widetilde{\mathsf{E}}_1)_p \cong (\widetilde{\mathsf{E}}_2)_p$ and, in particular, an isomorphism

$$\mathrm{H}^1(\mathrm{L}_{n,\pi}, (\widetilde{\mathsf{E}}_1)_p) \cong \mathrm{H}^1(\mathrm{L}_{n,\pi}, (\widetilde{\mathsf{E}}_2)_p) \qquad \text{for all } n \geq 0.$$

Proof. Starting with i), observe that an equality $S_1^{\mathrm{ss}} = S_2^{\mathrm{ss}}$ will imply $S_1^{\mathrm{ord}} = S_2^{\mathrm{ord}}$ because $S_j^{\mathrm{ord}} = S_p \setminus S_j^{\mathrm{ss}}$ (by **Hyp 1**, both curves have good reduction at all primes in S_p). To show the claimed equality, pick a prime $\mathfrak{p} \in S_1^{\mathrm{ss}}$. By **Hyp 1**, $\mathrm{L}_{\mathfrak{p}} \cong \mathbb{Q}_p$ is absolutely unramified. Denote by $\mathscr{E}_j$ the Néron model of E_j. (see [Sil94, IV, Corollary 6.3] for the existence of this model). Note that the operations of passing to the generic (*resp.* special) fibre and of computing the kernel of multiplication by p are fibre products. Thus these two operations commute and, in particular, the generic (*resp.* special) fibre of the finite, flat $\mathcal{O}_{\mathrm{L}_{\mathfrak{p}}}$-group scheme $(\mathscr{E}_j)_p$ is isomorphic to $(\mathsf{E}_j)_p$ (*resp.* to $(\widetilde{\mathsf{E}}_j)_p$), for $j = 1, 2$. Applying [Ray74, Corollaire 3.3.6], we see that the hypothesis $(\mathsf{E}_1)_p \cong (\mathsf{E}_2)_p$ (as Galois modules or, what amounts to the same, as finite, flat $\mathrm{L}_{\mathfrak{p}}$-group schemes) grants the existence of an isomorphism

$$(\mathscr{E}_1)_p \cong (\mathscr{E}_2)_p \tag{12}$$

of finite, flat $\mathcal{O}_{\mathrm{L}_{\mathfrak{p}}}$-group schemes. By taking closed fibres, this yields an isomorphism

$$(\widetilde{\mathsf{E}}_1)_p \cong (\mathscr{E}_1)_{p/\mathbb{F}_{\mathfrak{p}}} \cong (\mathscr{E}_2)_{p/\mathbb{F}_{\mathfrak{p}}} \cong (\widetilde{\mathsf{E}}_2)_p$$

as finite flat $\mathbb{F}_{\mathfrak{p}}$-group schemes. This shows that the elliptic cuve $\widetilde{\mathsf{E}}_2$ has supersingular reduction at $\mathfrak{p}$ and $S_1^{\mathrm{ss}} \subseteq S_2^{\mathrm{ss}}$. By reversing the role of E_1 and E_2, this yields $S_1^{\mathrm{ss}} = S_2^{\mathrm{ss}}$, as claimed.

Passing to ii), let π be a prime where one, and hence both curves, have ordinary reduction. The assumption $e(\pi) < p - 1$ allows us to again apply [Ray74, Corollaire 3.3.6] and the isomorphism (12) holds again, where now $\mathscr{E}_j$ denotes the Néron model of $\mathsf{E}_j/\mathrm{L}_\pi$. Taking closed fibres, we obtain

$$(\widetilde{\mathsf{E}}_1)_p \cong (\mathscr{E}_1)_{p/\mathbb{F}_\pi} \cong (\mathscr{E}_2)_{p/\mathbb{F}_\pi} \cong (\widetilde{\mathsf{E}}_2)_p$$

finishing the proof of the proposition. □

4. Iwasawa theory for the signed Selmer groups

4.1. **Cyclotomic fine signed residual Selmer groups.** In this section we focus on the Iwasawa theory for the fine signed residual Selmer group introduced in Definition 3.6. Retaining the notation introduced in 2.2, set $\mathscr{G}_{\mathrm{cyc}}^S = \mathrm{Gal}(\mathrm{L}^S/\mathrm{L}_{\mathrm{cyc}})$. Denote by Γ the Galois group $\mathrm{Gal}(\mathrm{L}_{\mathrm{cyc}}/\mathrm{L}) \cong \mathrm{Gal}(\mathcal{L}_{\mathrm{cyc}}/\mathbb{Q}_p)$, let $\Lambda(\Gamma) = \mathbb{Z}_p[\![\Gamma]\!]$ be its Iwasawa algebra, and set $\Omega(\Gamma) = \mathbb{F}_p[\![\Gamma]\!]$. For any module M over an Iwasawa algebra, its Pontryagin dual $\mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p)$ is denoted by $M^\vee$. When M is discrete, we say that it is cofinitely generated (*resp.* cofree, cotorsion, of corank equal to $m \in \mathbb{N}$) to mean that $M^\vee$ is finitely generated (*resp.* free, torsion,

of rank equal to m) over the Iwasawa algebra. Observe that, given any co-finitely generated $\Lambda(\Gamma)$-module M, there is an equality $M^\wedge/pM^\wedge = (M_p)^\wedge$, inducing the inequality

$$\operatorname{corank}_{\Lambda(\Gamma)} M \leq \operatorname{corank}_{\Omega(\Gamma)} M_p$$

which is an equality if and only if the μ invariant of $M^\wedge$ vanishes.

Thanks to Lemma 3.4, there is an inclusion of subgroups in $\mathrm{H}^1(\mathcal{L}_n, \mathsf{E}_p)$

$$\operatorname{Im}(\kappa^{\pm,p}_{\mathcal{L}_n}) \hookrightarrow \operatorname{Im}(\kappa^{p}_{\mathcal{L}_n}),$$

which will play a role in defining the Selmer groups. We display the subscript $1 \leq i \leq d$ to keep track of the local Galois cohomology groups, writing $\operatorname{Im}(\kappa^{\pm,p}_{\mathcal{L}_{n,i}}) \hookrightarrow \operatorname{Im}(\kappa^{p}_{\mathcal{L}_{n,i}}) \subseteq \mathrm{H}^1(\mathcal{L}_{n,i}, \mathsf{E}_p)$.

By taking the direct limit of the exact sequence (5) over the subextensions inside $\mathcal{L}_{\mathrm{cyc}}/\mathcal{L}$ gives the exact sequences, for all $1 \leq t \leq \infty$,

$$0 \longrightarrow \mathsf{E}^{\pm}(\mathcal{L}_{\mathrm{cyc}})/p^t\mathsf{E}^{\pm}(\mathcal{L}_{\mathrm{cyc}}) \xrightarrow{\kappa^{\pm,p^t}_{\mathcal{L}_{\mathrm{cyc}}}} \mathrm{H}^1(\mathcal{L}_{\mathrm{cyc}}, \mathsf{E}_{p^t}) \longrightarrow \mathrm{H}^1(\mathcal{L}_{\mathrm{cyc}}, \mathsf{E})/\operatorname{Im}(\kappa^{\pm,p^t}_{\mathcal{L}_{\mathrm{cyc},i}}) \longrightarrow 0, \tag{13}$$

The following proposition is the main technical tool needed to compare local and global cohomology groups of the residual representation E_p along the cyclotomic tower, with those of the representation E_{p^∞}. We refer to Lemma 3.7 for the definition of the arrows ψ in the statement below.

Proposition 4.1. *Let $G \in \{\mathscr{G}^S_{\mathrm{cyc}}, G_{\mathcal{L}_{\mathrm{cyc}}}, G_{\mathrm{L}_{\mathrm{cyc},w}}\}$ where $w \mid v \in S^{\mathrm{bad}} \cup S^{\mathrm{ord}}$. Write $\kappa^{\pm,p^\infty}_{\mathrm{L}_{\mathrm{cyc},w}}$ to denote $\kappa^{p^\infty}_{\mathrm{L}_{\mathrm{cyc},w}}$ when $w \mid v \in S^{\mathrm{bad}} \cup S^{\mathrm{ord}}$ (in particular, these maps are independent of the sign $\pm$).*

a) If $G \in \{\mathscr{G}^S_{\mathrm{cyc}}, G_{\mathcal{L}_{\mathrm{cyc}}}\}$, the map $\psi_{G,\mathrm{cyc}}$ is an isomorphism $\mathrm{H}^1(G, \mathsf{E}_p) \xrightarrow{\cong} \mathrm{H}^1(G, \mathsf{E}_{p^\infty})_p$.

b) If $G = G_{\mathrm{L}_{\mathrm{cyc},w}}$ for some $w \mid \mathfrak{l} \in S^{\mathrm{bad}}$, the kernel of $\psi_{w,\mathrm{cyc}}\colon \mathrm{H}^1(G, \mathsf{E}_p) \twoheadrightarrow \mathrm{H}^1(G, \mathsf{E}_{p^\infty})_p$ is finite, of dimension $\dim_{\mathbb{F}_p}(\ker \psi_{w,\mathrm{cyc}}) = \dim_{\mathbb{F}_p} \mathsf{E}(\mathrm{L}_{\mathrm{cyc},w})_p \leq 2$, and

$$\operatorname{corank}_{\Omega(\Gamma)} \mathrm{H}^1(G, \mathsf{E}_p) = \operatorname{corank}_{\Omega(\Gamma)} \mathrm{H}^1(G, \mathsf{E}_{p^\infty})_p.$$

c) If $G = G_{\mathrm{L}_{\mathrm{cyc},w}}$ for some $w \mid \pi \in S^{\mathrm{ord}}$, $\widetilde{\psi_{w,\mathrm{cyc}}}$ extends to a surjective map

$$\widetilde{\psi_{w,\mathrm{cyc}}}\colon \mathrm{H}^1(G, \widetilde{\mathsf{E}}_p) \twoheadrightarrow \mathrm{H}^1(G, \mathsf{E})_p = \left(\mathrm{H}^1(G, \mathsf{E}_{p^\infty})/\operatorname{Im}(\kappa^{\pm,p^\infty}_{\mathrm{L}_{w,\mathrm{cyc}}})\right)_p$$

whose kernel is finite, of dimension $\dim_{\mathbb{F}_p}(\ker \widetilde{\psi_{w,\mathrm{cyc}}}) = \dim_{\mathbb{F}_p} \widetilde{\mathsf{E}}(\mathbb{F}_w)_p \leq 1$, and

$$\operatorname{corank}_{\Omega(\Gamma)} \mathrm{H}^1(G, \widetilde{\mathsf{E}}_p) = \operatorname{corank}_{\Omega(\Gamma)} \left(\mathrm{H}^1(G, \mathsf{E}_{p^\infty})/\operatorname{Im}(\kappa^{\pm,p^\infty}_{\mathrm{L}_{w,\mathrm{cyc}}})\right)_p.$$

d) If $G = G_{\mathcal{L}_{\mathrm{cyc}}}$, the morphism $\psi_{\mathfrak{p},\mathrm{cyc}}$ induces an isomorphism

$$\psi^{\pm}_{\mathfrak{p},\mathrm{cyc}}\colon \mathrm{H}^1(G, \mathsf{E}_p)/\operatorname{Im}(\kappa^{\pm,p}_{\mathcal{L}_{\mathrm{cyc}}}) \xrightarrow{\cong} \left(\mathrm{H}^1(G, \mathsf{E}_{p^\infty})/\operatorname{Im}(\kappa^{\pm,p^\infty}_{\mathcal{L}_{\mathrm{cyc}}})\right)_p$$

giving

$$\operatorname{corank}_{\Omega(\Gamma)} \left(\mathrm{H}^1(G, \mathsf{E}_p)/\operatorname{Im}(\kappa^{\pm,p}_{\mathcal{L}_{\mathrm{cyc}}})\right) = \operatorname{corank}_{\Omega(\Gamma)} \left(\mathrm{H}^1(G, \mathsf{E}_{p^\infty})/\operatorname{Im}(\kappa^{\pm,p^\infty}_{\mathcal{L}_{\mathrm{cyc}}})\right)_p.$$

Proof. The isomorphism in a) follows immediately from passing to the direct limit of the isomorphisms at finite levels, proven in Lemma 3.7-i). Similarly, the description of the kernels in b) follows from passing to the direct limit in Lemma 3.7-ii).

The proof of c) relies on the theory of *deeply ramified extensions* as defined by Coates and Greenberg (see [CG96], in particular Theorem 2.13 *ibid.*, noting that the cyclotomic $\mathbb{Z}_p$-extension is deeply ramified). Consider the exact sequence

$$0 \longrightarrow \mathcal{A}_{p^\infty} \longrightarrow \mathsf{E}_{p^\infty} \longrightarrow \widetilde{\mathsf{E}}_{p^\infty} \longrightarrow 0,$$

where $\mathcal{A}$ is the formal group of $\mathsf{E}/\mathcal{O}_{\mathrm{L}_{\mathrm{cyc},\pi}}$. Then the long exact G-cohomology sequence gives

$$0 \longrightarrow \mathrm{H}^1(G,\mathsf{E}_{p^\infty})/\operatorname{Im}(\mathrm{H}^1(G,\mathcal{A}_{p^\infty})) \longrightarrow \mathrm{H}^1(G,\widetilde{\mathsf{E}}_{p^\infty}) \longrightarrow \mathrm{H}^2(G,\mathcal{A}_{p^\infty}). \tag{14}$$

We claim that $\mathrm{H}^2(G,\mathcal{A}_{p^\infty}) = 0$. Indeed, $\mathrm{H}^2(G,\mathcal{A}_{p^\infty}) = \varinjlim \mathrm{H}^2(G,\mathcal{A}_{p^t})$ and it will be enough to show that $\mathrm{H}^2(G,\mathcal{A}_{p^t}) = 0$ for all $t \geq 0$. This follows from the fact that G has p-cohomological dimension 1 (see [Ser94, proof of Proposition 9, Chapitre II, §3.3]).

Thus we obtain from (14) an isomorphism

$$\mathrm{H}^1(G,\mathsf{E}_{p^\infty})/\operatorname{Im}(\mathrm{H}^1(G,\mathcal{A}_{p^\infty})) \cong \mathrm{H}^1(G,\widetilde{\mathsf{E}}_{p^\infty}).$$

By [CG96, Proposition 4.3 and diagram (4.8)], we further have

$$\mathrm{H}^1(G,\mathsf{E})_{p^\infty} = \mathrm{H}^1(G,\mathsf{E}_{p^\infty})/\operatorname{Im}(\kappa^{\pm,p^\infty}_{\mathrm{L}_{\mathrm{cyc},w}}) = \mathrm{H}^1(G,\mathsf{E}_{p^\infty})/\operatorname{Im}(\mathrm{H}^1(G,\mathcal{A}_{p^\infty})).$$

Hence $\mathrm{H}^1(G,\mathsf{E})_{p^\infty} \cong \mathrm{H}^1(G,\widetilde{\mathsf{E}}_{p^\infty})$ and, in particular,

$$\mathrm{H}^1(G,\mathsf{E})_p \cong \mathrm{H}^1(G,\widetilde{\mathsf{E}}_{p^\infty})_p. \tag{15}$$

It follows that the surjective arrow $\widetilde{\psi_{w,\mathrm{cyc}}}\colon \mathrm{H}^1(G,\widetilde{\mathsf{E}}_p) \twoheadrightarrow \mathrm{H}^1(G,\widetilde{\mathsf{E}}_{p^\infty})_p$ takes values in $\mathrm{H}^1(G,\mathsf{E})_p$ and its kernel is finite, of $\mathbb{F}_p$-dimension less or equal to 1, by Lemma 3.7-iii).

The equality of $\Omega(\Gamma)$-coranks in b) and c) follows from the fact that a finite module has trivial $\Omega(\Gamma)$-rank.

To prove assertion d), note that $\mathsf{E}^\pm(\mathcal{L}_{\mathrm{cyc}})$ is p-torsion free. Indeed, $\mathsf{E}^\pm(\mathcal{L}_{\mathrm{cyc}})_p = \mathcal{E}^\pm(\mathfrak{m}^\Delta_\infty)_p$ by Lemma 3.3. But $\mathcal{E}^\pm(\mathfrak{m}_{\mathrm{cyc}})_p \subseteq \mathcal{E}(\mathfrak{m}_{\mathrm{cyc}})_p = 0$, by Proposition 3.1, hence $\mathsf{E}^\pm(\mathcal{L}_{\mathrm{cyc}})_p = 0$. In particular, $\mathsf{E}^\pm(\mathcal{L}_{\mathrm{cyc}})$ is a direct limit of free $\mathbb{Z}_p$-modules of finite rank, hence $\operatorname{Tor}^1_{\mathbb{Z}_p}(\mathsf{E}^\pm(\mathcal{L}_{\mathrm{cyc}}),\mathbb{Q}_p/\mathbb{Z}_p) = 0$. Consider the exact sequence

$$0 \longrightarrow \mathbb{Z}/p \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 0.$$

Tensoring it with $\mathsf{E}^\pm(\mathcal{L}_{\mathrm{cyc}})$ over $\mathbb{Z}_p$ yields

$$\mathsf{E}^\pm(\mathcal{L}_{\mathrm{cyc}}) \otimes \mathbb{Z}/p \cong (\mathsf{E}^\pm(\mathcal{L}_{\mathrm{cyc}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)_p. \tag{16}$$

Now, the map $\psi^\pm_{\mathfrak{p},\mathrm{cyc}}$, defined as the composition of $\psi_{\mathfrak{p},\mathrm{cyc}}$ with reduction modulo $\operatorname{Im}\kappa^{\pm,p^\infty}_{\mathcal{L}_{\mathrm{cyc}}}$, appears in the following diagram of exact sequences:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathsf{E}^\pm(\mathcal{L}_{\mathrm{cyc}}) \otimes \mathbb{Z}/p & \xrightarrow{\kappa^{\pm,p}_{\mathcal{L}_{\mathrm{cyc}}}} & \mathrm{H}^1(\mathcal{L}_{\mathrm{cyc}},\mathsf{E}_p) & \longrightarrow & \mathrm{H}^1(\mathcal{L}_{\mathrm{cyc}},\mathsf{E}_p)/\operatorname{Im}\kappa^{\pm,p}_{\mathcal{L}_{\mathrm{cyc}}} & \longrightarrow & 0 \\
 & & \wr\downarrow & & \wr\downarrow \psi_{\mathscr{G}^S_{\mathrm{cyc}}} & & \downarrow \psi^\pm_{\mathfrak{p},\mathrm{cyc}} & & \\
0 & \longrightarrow & \left(\mathsf{E}^\pm(\mathcal{L}_{\mathrm{cyc}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p\right)_p & \xrightarrow{\kappa^{\pm,p^\infty}_{\mathcal{L}_{\mathrm{cyc}}}} & \mathrm{H}^1(\mathcal{L}_{\mathrm{cyc}},\mathsf{E}_{p^\infty})_p & \xrightarrow{\alpha} & \left(\mathrm{H}^1(\mathcal{L}_{\mathrm{cyc}},\mathsf{E}_{p^\infty})/\operatorname{Im}\kappa^{\pm,p^\infty}_{\mathcal{L}_{\mathrm{cyc}}}\right)_p & &
\end{array} \tag{17}$$

The first vertical arrow is an isomorphism in light of (16), and the second vertical arrow is an isomorphism thanks to a). The snake lemma implies that $\psi^\pm_{\mathfrak{p},\mathrm{cyc}}$ is injective and $\operatorname{coker}(\psi^\pm_{\mathfrak{p},\mathrm{cyc}}) = \operatorname{coker}(\alpha)$. To show that

α is surjective observe that the bottom row in (17) is the beginning of the $\mathrm{Tor}^i_{\mathbb{Z}_p}(-,\mathbb{Z}/p)$-sequence of the tautological exact sequence

$$0 \longrightarrow \mathsf{E}^{\pm}(\mathcal{L}_{\mathrm{cyc}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{\kappa^{\pm,p^\infty}_{\mathcal{L}_{\mathrm{cyc}}}} \mathrm{H}^1(\mathcal{L}_{\mathrm{cyc}}, \mathsf{E}_{p^\infty}) \longrightarrow \mathrm{H}^1(\mathcal{L}_{\mathrm{cyc}}, \mathsf{E}_{p^\infty})/\operatorname{Im}\kappa^{\pm,p^\infty}_{\mathcal{L}_{\mathrm{cyc}}} \longrightarrow 0$$

and therefore $\mathrm{coker}(\alpha)$ is contained in

$$\Big(\mathsf{E}^{\pm}(\mathcal{L}_{\mathrm{cyc}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p\Big)\otimes\mathbb{Z}/p = \Big(\mathsf{E}^{\pm}(\mathcal{L}_{\mathrm{cyc}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p\Big)/p\Big(\mathsf{E}^{\pm}(\mathcal{L}_{\mathrm{cyc}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p\Big).$$

Since $\mathsf{E}^{\pm}(\mathcal{L}_{\mathrm{cyc}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ is divisible, the above module is trivial, establishing the surjectivity of α and thus of $\psi^{\pm}_{\mathfrak{p},\mathrm{cyc}}$. This finishes the proof of the proposition. □

Let us now pass to Selmer groups. We refer to [CS10, Chapter 2] for generalities on Iwasawa theory for elliptic curves over cyclotomic extensions and, in particular, for the definitions of the groups $\mathrm{Sel}(\mathrm{L}_{\mathrm{cyc}}/\mathsf{E}_{p^\infty})$ in the ordinary case.

Definition 4.2. The fine signed residual Selmer group $\mathcal{R}^{\pm}(\mathsf{E}_{p^t}/\mathrm{L}_{\mathrm{cyc}})$ is defined as

$$\mathcal{R}^{\pm}\big(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}\big) = \varinjlim_{\mathrm{res}} \mathcal{R}^{\pm}\big(\mathsf{E}_p/\mathrm{L}_n\big)$$

and the usual signed Selmer group is defined as

$$\mathrm{Sel}^{\pm}\big(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}}\big) = \varinjlim_{\mathrm{res}} \mathrm{Sel}^{\pm}\big(\mathsf{E}_{p^\infty}/\mathrm{L}_n\big).$$

The groups $\mathcal{R}^{\pm}\big(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}\big)$ are discrete $\Omega(\Gamma)$-modules, whose Pontryagin duals are compact, finitely generated over $\Omega(\Gamma)$. Similarly, the groups $\mathrm{Sel}^{\pm}\big(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}}\big)$ are discrete, cofinitely generated $\Lambda(\Gamma)$-modules. For $v \in S$, denote by ${}^{\pm}\widetilde{K}_v(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})$ the $\Omega(\Gamma)$-module

$${}^{\pm}\widetilde{K}_v(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) = \begin{cases} \displaystyle\bigoplus_{w|\mathfrak{l}} \mathrm{H}^1(\mathrm{L}_{w,\mathrm{cyc}}, \mathsf{E}_p) & \text{if } v = \mathfrak{l} \in S^{\mathrm{bad}} \\ \displaystyle\bigoplus_{w|\pi} \mathrm{H}^1(\mathrm{L}_{w,\mathrm{cyc}}, \widetilde{\mathsf{E}}_p) & \text{if } v = \pi \in S^{\mathrm{ord}} \\ \mathrm{H}^1(\mathcal{L}_{\mathrm{cyc},i}, \mathsf{E}_p)/\operatorname{Im}(\kappa^{\pm,p}_{\mathcal{L}_{\mathrm{cyc},i}}) & \text{if } v = \mathfrak{p}_i \in S^{\mathrm{ss}}. \end{cases}$$

Similarly, define $J^{\pm}_v(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$ as the $\Lambda(\Gamma)$-module

$$J^{\pm}_v(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}}) = \bigoplus_{w|v} \mathrm{H}^1(\mathrm{L}_{w,\mathrm{cyc}}, \mathsf{E}_{p^\infty})/\operatorname{Im}(\kappa^{\pm,p^\infty}_{\mathrm{L}_{w,\mathrm{cyc}}})$$

where, as in Proposition 4.1, we set $\kappa^{\pm,p^\infty}_{\mathrm{L}_{w,\mathrm{cyc}}} = \kappa^{p^\infty}_{\mathrm{L}_{w,\mathrm{cyc}}}$ for all $w \mid v \in S \setminus S^{\mathrm{ss}}$. By definition, the fine signed residual Selmer group (*resp.* the usual signed Selmer group) give the following exact sequences:

$$0 \longrightarrow \mathcal{R}^{\pm}\big(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}\big) \longrightarrow \mathrm{H}^1(\mathscr{G}^S_{\mathrm{cyc}}, \mathsf{E}_p) \xrightarrow{\zeta^{\pm}_p} \bigoplus_{v\in S} {}^{\pm}\widetilde{K}_v(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) \tag{18}$$

resp.

$$0 \longrightarrow \mathrm{Sel}^{\pm}\big(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}}\big) \longrightarrow \mathrm{H}^1\big(\mathscr{G}^S_{\mathrm{cyc}}, \mathsf{E}_{p^\infty}\big) \xrightarrow{\xi^{\pm}_{p^\infty}} \bigoplus_{v\in S}\big(J_v^{\pm}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})\big). \tag{19}$$

As a consequence of the results in Section 3, we can now check that the local conditions ${}^{\pm}\widetilde{K}_v(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})$ depend only on the residual representation E_p. This is immediate at all $\mathfrak{l} \in S^{\mathrm{bad}}$, and follows from Proposition 3.9 at all primes $\pi \in S^{\mathrm{ord}}$ by taking inductive limit along the cyclotomic tower. Concerning primes $\mathfrak{p} \in S^{\mathrm{ss}}$, this independence follows from combining Proposition 3.8 with the isomorphism in Proposition 4.1-d). The fact that the local conditions depend only on the residual representation implies that the same holds for the fine residual signed Selmer group. We record this as

Corollary 4.3. *Let* $\mathsf{E}_1, \mathsf{E}_2$ *be two elliptic curves over* L *satisfying* ***Hyp 1*** *such that* $(\mathsf{E}_1)_p \cong (\mathsf{E}_2)_p$. *Then*

$$\mathcal{R}^{\pm}\big((\mathsf{E}_1)_p/\mathrm{L}_{\mathrm{cyc}}\big) \cong \mathcal{R}^{\pm}\big((\mathsf{E}_2)_p/\mathrm{L}_{\mathrm{cyc}}\big).$$

Kim considers in [Kim09] the primitive and non-primitive Selmer groups along the lines of [GreVat00]. Corollary 4.5 below is the analogue of [Kim09, Proposition 2.10] for the fine signed residual Selmer groups. In order to state it, let us introduce a final notation. For all $w \mid v \in S^{\mathrm{bad}} \cup S^{\mathrm{ord}}$, let g_v be the number of primes w lying above v in $\mathrm{L}_{\mathrm{cyc}}$. Further, for $v = \mathfrak{l} \in S^{\mathrm{bad}}$ and $\mathfrak{q} \mid \mathfrak{l}$ in $\mathrm{L}_{\mathrm{cyc}}$, denote by $\mathrm{L}^1_{\mathfrak{q}}$ the first layer of the cyclotomic extension $\mathrm{L}_{\mathrm{cyc},\mathfrak{q}}/\mathrm{L}_{\mathfrak{l}}$. Note that $\mathrm{L}^1_{\mathfrak{q}}$ is also the unique unramified extension of degree p of $\mathrm{L}_{\mathfrak{l}}$.

Recall that, for any place v, the residue field at that place is denoted by $\mathbb{F}_v$.

Definition 4.4. For all $\mathfrak{l} \in S^{\mathrm{bad}}$, choose a place $\mathfrak{q}$ of $\mathrm{L}_{\mathrm{cyc}}$ above $\mathfrak{l}$. We define the defect of E as

$$\delta_{\mathsf{E}} := \sum_{\mathfrak{l}\in S^{\mathrm{bad}}} g_{\mathfrak{l}} \cdot \dim_{\mathbb{F}_p} \mathsf{E}(\mathrm{L}^1_{\mathfrak{q}})_p + \sum_{\pi\in S^{\mathrm{ord}}} g_\pi \dim_{\mathbb{F}_p} \widetilde{\mathsf{E}}(\mathbb{F}_\pi)_p \leq 2\sum_{\mathfrak{l}\in S^{\mathrm{bad}}} g_{\mathfrak{l}} + \sum_{\pi\in S^{\mathrm{ord}}} g_\pi.$$

The fact that $\dim_{\mathbb{F}_p} \mathsf{E}(\mathrm{L}^1_{\mathfrak{q}})_p$ is independent of $\mathfrak{q} \mid \mathfrak{l}$ follows from $\mathrm{L}_{\mathrm{cyc}}/\mathrm{L}$ being Galois, since E is defined over L.

Corollary 4.5. *There are injections*

$$\varphi^{\pm}\colon \mathcal{R}^{\pm}\big(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}\big) \hookrightarrow \mathrm{Sel}^{\pm}\big(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}}\big)_p$$

whose cokernel is finite, of dimension $\dim_{\mathbb{F}_p} \mathrm{coker}(\varphi^{\pm}) \leq \delta_{\mathsf{E}}$. *In particular,*

$$\mathrm{corank}_{\Omega(\Gamma)}\, \mathcal{R}^{\pm}\big(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}\big) = \mathrm{corank}_{\Omega(\Gamma)}\, \mathrm{Sel}^{\pm}\big(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}}\big)_p.$$

Moreover, when $\xi^{\pm}_p$ *is surjective,* $\dim_{\mathbb{F}_p} \mathrm{coker}(\varphi^{\pm}) = \delta_{\mathsf{E}}$, *independently of the sign* $\pm$.

Proof. Consider the commutative diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathcal{R}^{\pm}\big(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}\big) & \longrightarrow & \mathrm{H}^1\big(\mathscr{G}^S_{\mathrm{cyc}}, \mathsf{E}_p\big) & \xrightarrow{\xi^{\pm}_p} & \displaystyle\bigoplus_{v\in S} {}^{\pm}\widetilde{K}_v(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) \\
 & & \downarrow{\scriptstyle \varphi^{\pm}} & & \downarrow{\scriptstyle \wr} & & \downarrow{\scriptstyle \oplus\varphi_v^{\pm}} \\
0 & \longrightarrow & \mathrm{Sel}^{\pm}\big(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}}\big)_p & \longrightarrow & \mathrm{H}^1\big(\mathscr{G}^S_{\mathrm{cyc}}, \mathsf{E}_{p^\infty}\big)_p & \xrightarrow{\xi^{\pm}_{p^\infty}} & \displaystyle\bigoplus_{v\in S}\big(J_v^{\pm}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})\big)_p
\end{array} \tag{20}$$

The central vertical arrow is an isomorphism thanks to Proposition 4.1-a). The local arrows $\varphi_v^{\pm}$ can be decomposed as

$$\varphi_v^{\pm} = \bigoplus_{w|v} \varphi_w^{\pm}$$

and each $\varphi_w^{\pm}$ is induced by the corresponding arrow $\psi_{w,\mathrm{cyc}}$ of Proposition 4.1. More precisely,

$$\varphi_w^{\pm} = \begin{cases} \psi_{w,\mathrm{cyc}} \colon \mathrm{H}^1(\mathrm{L}_{w,\mathrm{cyc}}, \mathsf{E}_p) \longrightarrow \mathrm{H}^1(\mathrm{L}_{w,\mathrm{cyc}}, \mathsf{E}_{p^\infty})_p = \Big(\mathrm{H}^1(\mathrm{L}_{w,\mathrm{cyc}}, \mathsf{E}_{p^\infty}) / \operatorname{Im}(\kappa^{\pm,p^\infty}_{\mathrm{L}_{w,\mathrm{cyc}}})\Big)_p & \text{if} \quad v = \mathfrak{l} \in S^{\mathrm{bad}} \\ \widetilde{\psi_{w,\mathrm{cyc}}} \colon \mathrm{H}^1(\mathrm{L}_{w,\mathrm{cyc}}, \widetilde{\mathsf{E}}_p) \longrightarrow \mathrm{H}^1(\mathrm{L}_{w,\mathrm{cyc}}, \widetilde{\mathsf{E}}_{p^\infty})_p = \Big(\mathrm{H}^1(\mathrm{L}_{w,\mathrm{cyc}}, \mathsf{E}_{p^\infty}) / \operatorname{Im}(\kappa^{\pm,p^\infty}_{\mathrm{L}_{w,\mathrm{cyc}}})\Big)_p & \text{if} \quad v = \pi \in S^{\mathrm{ord}} \\ \psi^{\pm}_{\mathfrak{p},\mathrm{cyc}} \colon \mathrm{H}^1(\mathcal{L}_{\mathrm{cyc}}, \mathsf{E}_p) / \operatorname{Im}(\kappa^{\pm,p}_{\mathcal{L}_{\mathrm{cyc}}}) \xrightarrow{\cong} \Big(\mathrm{H}^1(\mathcal{L}_{\mathrm{cyc}}, \mathsf{E}_{p^\infty}) / \operatorname{Im}(\kappa^{\pm,p^\infty}_{\mathcal{L}_{\mathrm{cyc}}})\Big)_p & \text{if} \quad v = \mathfrak{p} \in S^{\mathrm{ss}} \end{cases}$$

Indeed, the first equality

$$\mathrm{H}^1(\mathrm{L}_{w,\mathrm{cyc}}, \mathsf{E}_{p^\infty})_p = \Big(\mathrm{H}^1(\mathrm{L}_{w,\mathrm{cyc}}, \mathsf{E}_{p^\infty}) / \operatorname{Im}(\kappa^{\pm,p^\infty}_{\mathrm{L}_{w,\mathrm{cyc}}})\Big)_p$$

follows from the fact that $\operatorname{Im}(\kappa^{\pm,p^\infty}_{\mathrm{L}_{w,\mathrm{cyc}}}) = 0$, since $\mathsf{E}(\mathrm{L}_{w,\mathrm{cyc}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$ when $v \notin S_p$. The second equality

$$\mathrm{H}^1(\mathrm{L}_{w,\mathrm{cyc}}, \widetilde{\mathsf{E}}_{p^\infty})_p = \Big(\mathrm{H}^1(\mathrm{L}_{w,\mathrm{cyc}}, \mathsf{E}_{p^\infty}) / \operatorname{Im}(\kappa^{\pm,p^\infty}_{\mathrm{L}_{w,\mathrm{cyc}}})\Big)_p$$

follows from (15), because

$$\mathrm{H}^1(\mathrm{L}_{w,\mathrm{cyc}}, \mathsf{E})_p = \Big(\mathrm{H}^1(\mathrm{L}_{w,\mathrm{cyc}}, \mathsf{E}_{p^\infty}) / \operatorname{Im}(\kappa^{\pm,p^\infty}_{\mathrm{L}_{w,\mathrm{cyc}}})\Big)_p .$$

Similarly, the fact that $\psi^{\pm}_{\mathfrak{p},\mathrm{cyc}}$ takes values in $\Big(\mathrm{H}^1(\mathcal{L}_{\mathrm{cyc}}, \mathsf{E}_{p^\infty}) / \operatorname{Im}(\kappa^{\pm,p^\infty}_{\mathcal{L}_{\mathrm{cyc}}})\Big)_p$ and is an isomorphism follows from Proposition 4.1-d).

By applying the snake lemma to (20) we see that

$$\operatorname{coker}(\varphi^{\pm}) \subseteq \bigoplus_{\mathfrak{q}|\mathfrak{l} \in S^{\mathrm{bad}}} \ker\big(\psi_{\mathfrak{q},\mathrm{cyc}}\big) \oplus \bigoplus_{w|\pi \in S^{\mathrm{ord}}} \ker\big(\widetilde{\psi_{w,\mathrm{cyc}}}\big) \tag{21}$$

and the inclusion in (21) is an equality when $\xi_p^{\pm}$ is surjective.

It follows from (21) and Proposition 4.1-b)–c) that

$$\dim_{\mathbb{F}_p} \operatorname{coker}(\varphi^{\pm}) \leq \dim_{\mathbb{F}_p} \bigoplus_{\mathfrak{q}|\mathfrak{l} \in S^{\mathrm{bad}}} \dim_{\mathbb{F}_p} \mathsf{E}(\mathrm{L}_{\mathrm{cyc},w})_p + \dim_{\mathbb{F}_p} \bigoplus_{w|\pi \in S^{\mathrm{ord}}} \dim_{\mathbb{F}_p} \widetilde{\mathsf{E}}(\mathbb{F}_w)_p$$

which is an equality if $\xi_p^{\pm}$ is surjective. To prove the statement of the corollary, we need to show that

$$\dim_{\mathbb{F}_p} \mathsf{E}(\mathrm{L}_{\mathrm{cyc},\mathfrak{q}})_p = \mathsf{E}(\mathrm{L}^1_{\mathfrak{q}})_p \qquad \text{if } \mathfrak{q} \mid \mathfrak{l} \in S^{\mathrm{bad}} \tag{22}$$

and

$$\dim_{\mathbb{F}_p} \widetilde{\mathsf{E}}(\mathbb{F}_w)_p = \dim_{\mathbb{F}_p} \widetilde{\mathsf{E}}(\mathbb{F}_\pi)_p \qquad \text{for all } w \mid \pi \in S^{\mathrm{ord}}. \tag{23}$$

The equality in (23) simply follows from the fact that the inertia degree of every p-adic prime is 1 along the $\mathbb{Z}_p$-cyclotomic $\mathrm{L}_{\mathrm{cyc}}/\mathrm{L}$, whence $\mathbb{F}_w = \mathbb{F}_\pi$.

Concerning (22), we argue as follows. If $\dim_{\mathbb{F}_p} \mathsf{E}(\mathrm{L}_\mathfrak{l})_p = 2$, then the full torsion of $\mathsf{E}(\overline{\mathrm{L}_\mathfrak{l}})$ is already defined over $\mathrm{L}_\mathfrak{l}$, hence $\mathsf{E}(\mathrm{L}_\mathfrak{l})_p = \mathsf{E}(\mathrm{L}_\mathfrak{q}^1)_p = \mathsf{E}(\mathrm{L}_{\mathrm{cyc},\mathfrak{q}})_p$. If $\dim_{\mathbb{F}_p} \mathsf{E}(\mathrm{L}_\mathfrak{l})_p = 0$, then the p-group $\mathsf{E}(\mathrm{L}_{\mathrm{cyc},\mathfrak{q}})_p$ has no non-zero fixed point under the action of the pro-p-group $\Gamma = \mathrm{Gal}(\mathrm{L}_{\mathrm{cyc},\mathfrak{q}}/\mathrm{L}_\mathfrak{l})$, and must be trivial. Hence $\mathsf{E}(\mathrm{L}_{\mathrm{cyc},\mathfrak{q}})_p = 0 = \mathsf{E}(\mathrm{L}_\mathfrak{q}^1)_p$. Finally, if $\dim_{\mathbb{F}_p} \mathsf{E}(\mathrm{L}_\mathfrak{l})_p = 1$ but $\dim_{\mathbb{F}_p} \mathsf{E}(\mathrm{L}_{\mathrm{cyc},\mathfrak{q}})_p = 2$, we need to show that $\dim_{\mathbb{F}_p} \mathsf{E}(\mathrm{L}_\mathfrak{q}^1)_p = 2$. The assumption that $\dim_{\mathbb{F}_p} \mathsf{E}(\mathrm{L}_{\mathrm{cyc},\mathfrak{q}})_p = 2$ implies that the action of Γ in $\mathrm{Aut}\big(\mathsf{E}(\mathrm{L}_{\mathrm{cyc},w})_p\big)$ induces, upon fixing a basis, a 2-dimensional linear representation

$$\varrho\colon \Gamma \longrightarrow \mathrm{GL}_2(\mathbb{F}_p).$$

As $\mathrm{GL}_2(\mathbb{F}_p)$ contains no element of order p^2, ϱ factors through $\Gamma/\Gamma^p = \mathrm{Gal}(\mathrm{L}_\mathfrak{q}^1/\mathrm{L}_\mathfrak{l})$, so Γ^p acts trivially on $\mathsf{E}(\mathrm{L}_{\mathrm{cyc},\mathfrak{q}})_p$. This implies that $\mathsf{E}(\mathrm{L}_{\mathrm{cyc},\mathfrak{q}})_p = \mathsf{E}(\mathrm{L}_\mathfrak{q}^1)_p$ also in this case, and concludes the proof of the corollary. □

4.2. **Cassels–Poiutou–Tate exact sequence and Iwasawa cohomology.** For $n \in \mathbb{N} \cup \{\mathrm{cyc}\}$, let $\mathrm{X}(\mathsf{E}_{p^\infty}/\mathrm{L}_n)$ denote the Pontryagin duals

$$\mathrm{X}(\mathsf{E}_{p^\infty}/\mathrm{L}_n) = \mathrm{Hom}_{\mathbb{Z}_p}\big(\mathrm{Sel}(\mathsf{E}_{p^\infty}/\mathrm{L}_n), \mathbb{Q}_p/\mathbb{Z}_p\big).$$

These modules clearly admit signed versions, defined as

$$\mathrm{X}^\pm(\mathsf{E}_{p^\infty}/\mathrm{L}_n) = \mathrm{Hom}_{\mathbb{Z}_p}\big(\mathrm{Sel}^\pm\big(\mathsf{E}_{p^\infty}/\mathrm{L}_n\big), \mathbb{Q}_p/\mathbb{Z}_p\big).$$

Similarly, the duals of the fine signed residual Selmer groups are defined as

$$\mathrm{Y}^\pm(\mathsf{E}_p/\mathrm{L}_n) = \mathrm{Hom}_{\mathbb{Z}_p}\big(\mathcal{R}^\pm\big(\mathsf{E}_p/\mathrm{L}_n\big), \mathbb{Q}_p/\mathbb{Z}_p\big).$$

Both $\mathrm{X}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$ and $\mathrm{X}^\pm(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$ are finitely generated compact $\Lambda(\Gamma)$-modules and it follows from Corollary 4.5 that the $\Omega(\Gamma)$-modules $\mathrm{Y}^\pm(\mathsf{E}_p/\mathrm{L}_n)$ are finitely generated. Further, Corollary 4.3 implies that they only depend upon the isomorphism class of E_p. As a last piece of notation, suppose that $K \in \{\mathcal{L}_n, \mathrm{L}_v, \mathrm{L}_n\}$ for some $0 \leq n < \infty$, and retain notation from (2.2): in particular, $\widetilde{K} = \overline{\mathbb{Q}_p}$ if $K = \mathcal{L}_n$, $\widetilde{K} = \overline{\mathrm{L}_v}$ if $K = \mathrm{L}_v$ and $\widetilde{K} = \mathrm{L}^S$ if $K = \mathrm{L}$. Let M be a compact $\mathbb{Z}_p$-module with a continuous $\mathrm{Gal}(\widetilde{K}/K)$-action. The *Iwasawa cohomology* modules $\mathrm{H}^i_{\mathrm{Iw}}(K, M)$ (for all $i \geq 1$) are defined as the projective limit, with respect to corestriction maps

$$\mathrm{H}^i_{\mathrm{Iw}}(K, M) = \varprojlim_{K \subseteq K' \subseteq K_{\mathrm{cyc}}} \mathrm{H}^i(\widetilde{K}/K', M).$$

For consistency with the notation for usual cohomology, when $K = \mathrm{L}_n$ we write $\mathrm{H}^i_{\mathrm{Iw}}(\mathscr{G}_n^S, M)$ rather than $\mathrm{H}^i_{\mathrm{Iw}}(\mathrm{L}_n, M)$. The reader is referred to [PR92, §3.1] for generalities about Iwasawa cohomology. In particular, the above $\Lambda(\Gamma)$-modules are known to be trivial for $i \neq 1, 2$.

A fundamental tool for the study of the Iwasawa theory of Selmer groups is the Cassels–Poitou–Tate exact sequence, for which we refer to [CS10, Theorem 1.5] and which we now briefly recall. Fix $n \in \mathbb{N}$ and consider the self-dual module $M = \mathsf{E}_p$. Put

$$W_v = \begin{cases} 0 & \text{if } v = \mathfrak{l} \in S^{\mathrm{bad}} \\ \mathrm{Im}(\kappa^{\pm,p}_{\mathcal{L}_{n,i}}) & \text{if } v = \mathfrak{p}_i \in S^{\mathrm{ss}} \quad (1 \leq i \leq d) \\ \mathrm{H}^1(\mathcal{L}_{n,\pi_i}, (\mathcal{A}_\pi)_p) & \text{if } v = \pi_i \in S^{\mathrm{ord}} \quad (1 \leq i \leq s) \end{cases}$$

where $\mathcal{A}_\pi$ denotes the formal group of $\mathsf{E}/\mathcal{O}_{\mathrm{L}_\pi}$. These coincide with the local conditions in Definition 3.6, so that $\mathcal{R}^{\pm}\big(\mathsf{E}_p/\mathrm{L}_n\big)$ sit in the exact sequences (one for each sign $\pm$)

$$0 \longrightarrow \mathcal{R}^{\pm}\big(\mathsf{E}_p/\mathrm{L}_n\big) \longrightarrow \mathrm{H}^1(\mathscr{G}_n^S, \mathsf{E}_p) \longrightarrow \bigoplus_{v\in S} \mathrm{H}^1(\mathrm{L}_{v,n}, \mathsf{E}_p)/W_v.$$

For all $v \in S$, let $W_v^\perp$ denote the orthogonal complement of W_v in the Tate pairing

$$\mathrm{H}^1(\mathrm{L}_{v,n}, \mathsf{E}_p) \times \mathrm{H}^1(\mathrm{L}_{v,n}, \mathsf{E}_p) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

and define $\mathcal{R}^{\perp,\pm}\big(\mathsf{E}_p/\mathrm{L}\big)$ as the kernel

$$0 \longrightarrow \mathcal{R}^{\perp,\pm}\big(\mathsf{E}_p/\mathrm{L}_n\big) \longrightarrow \mathrm{H}^1(\mathscr{G}_n^S, \mathsf{E}_p) \longrightarrow \bigoplus_{v\in S} \mathrm{H}^1(\mathrm{L}_{v,n}, \mathsf{E}_p)/W_v^\perp.$$

This gives two Cassels–Poitou–Tate exact sequences

$$\begin{aligned} 0 \longrightarrow \mathcal{R}^{\pm}\big(\mathsf{E}_p/\mathrm{L}_n\big) \longrightarrow \mathrm{H}^1(\mathscr{G}_n^S, \mathsf{E}_p) \longrightarrow \bigoplus_{v\in S} \mathrm{H}^1(\mathrm{L}_{v,n}, \mathsf{E}_p)/W_v \longrightarrow \Big(\mathcal{R}^{\perp,\pm}\big(\mathsf{E}_p/\mathrm{L}_n\big)\Big)^\wedge \longrightarrow \\ \longrightarrow \mathrm{H}^2(\mathscr{G}_n^S, \mathsf{E}_p) \longrightarrow \bigoplus_{w|v\in S} \mathrm{H}^2(\mathrm{L}_{n,v}, \mathsf{E}_p) \longrightarrow 0 \end{aligned} \tag{24}$$

where the final 0 comes from Proposition 3.1.

In order to study to the limit, as $n \to \infty$ along the cyclotomic tower, of the Cassels–Poitou–Tate sequences, consider the group

$$\mathscr{S}^{\pm}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) = \varprojlim_{\mathrm{cores}} \mathcal{R}^{\perp,\pm}\big(\mathsf{E}_p/\mathrm{L}_n\big) \subseteq \mathrm{H}^1_{\mathrm{Iw}}(\mathscr{G}_n^S, \mathsf{E}_p).$$

This is a $\Omega(\Gamma)$-module whose relevance for our study comes from the following observation (*cf.* [LS18, Lemma 2.6 and Remark 2.7], where the case of an elliptic curve with ordinary reduction at p is considered):

Lemma 4.6. *There is an isomorphism*

$$\mathscr{S}^{\pm}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})^\wedge \cong \varinjlim_{(\mathrm{cores})^\wedge} \Big(\mathcal{R}^{\perp,\pm}\big(\mathsf{E}_p/\mathrm{L}_n\big)\Big)^\wedge.$$

Moreover, the group $\mathscr{S}^{\pm}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})$ is free as $\Omega(\Gamma)$-module.

Proof. The displayed isomorphism simply follows from the definition, since

$$\begin{aligned} \mathscr{S}^{\pm}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})^\wedge &= \mathrm{Hom}\Big(\varprojlim_{\mathrm{cores}} \mathcal{R}^{\perp,\pm}(\mathsf{E}_p/\mathrm{L}_n), \mathbb{Q}_p/\mathbb{Z}_p\Big) \\ &= \varinjlim_{(\mathrm{cores})^\wedge} \mathrm{Hom}\Big(\mathcal{R}^{\perp,\pm}(\mathsf{E}_p/\mathrm{L}_n), \mathbb{Q}_p/\mathbb{Z}_p\Big) \\ &= \varinjlim_{(\mathrm{cores})^\wedge} \Big(\mathcal{R}^{\perp,\pm}\big(\mathsf{E}_p/\mathrm{L}_n\big)\Big)^\wedge. \end{aligned}$$

To show that $\mathscr{S}^{\pm}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})$ is a free $\Omega(\Gamma)$-module, note that Jannsen's spectral sequence [Jan14, Corollary 13] takes the form

$$E_2^{p,q} = \mathrm{Ext}^p_{\Omega(\Gamma)}\big(\mathrm{Hom}\big(\mathrm{H}^q(\mathscr{G}^S_{\mathrm{cyc}}, \mathsf{E}_p), \mathbb{F}_p\big), \Omega(\Gamma)\big) \Longrightarrow \mathrm{H}^{p+q}_{\mathrm{Iw}}(\mathscr{G}^S, \mathsf{E}_p).$$

By Proposition 3.1, $E_2^{p,0} = 0$ for all $p \geq 1$. Hence, $E_2^{1,0} = E_\infty^{1,0} = 0$ and $E_2^{0,1} = E_\infty^{0,1}$. It follows that

$$E_2^{0,1} = \mathrm{Hom}_{\Omega(\Gamma)}\big(\mathrm{Hom}_{\mathbb{F}_p}(\mathrm{H}^1(\mathscr{G}_{\mathrm{cyc}}^S, \mathsf{E}_p), \mathbb{F}_p), \Omega(\Gamma)\big) \cong \mathrm{H}^1_{\mathrm{Iw}}(\mathscr{G}^S, \mathsf{E}_p).$$

In particular, the first Iwasawa cohomology group of E_p is torsion-free over $\Omega(\Gamma)$, and hence free since $\Omega(\Gamma)$ is a PID. By taking projective limit, with respect to corestriction, of the inclusions $\mathcal{R}^{\perp,\pm}\big(\mathsf{E}_p/\mathrm{L}_n\big) \hookrightarrow \mathrm{H}^1(\mathscr{G}_n^S, \mathsf{E}_p)$, we obtain an injection

$$\mathscr{S}^{\pm}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) \lhook\joinrel\longrightarrow \mathrm{H}^1_{\mathrm{Iw}}(\mathscr{G}^S, \mathsf{E}_p).$$

Since $\Omega(\Gamma)$ is a principal ideal domain, a submodule of a free module is itself free, finishing the proof. □

Given two subextensions $\mathrm{L} \subseteq \mathrm{L}_n \subseteq \mathrm{L}_m \subseteq \mathrm{L}_{\mathrm{cyc}}$, consider the corresponding exact sequences (24) . The restriction map on cohomology induces morphisms between the first three (*resp.* the last two) terms. A standard argument in local Tate duality shows that connecting the fourth terms via the Pontryagin dual of corestriction

$$(\mathrm{cores})^\wedge\colon \Big(\mathcal{R}^{\perp,\pm}\big(\mathsf{E}_p/\mathrm{L}_n\big)\Big)^\wedge \longrightarrow \Big(\mathcal{R}^{\perp,\pm}\big(\mathsf{E}_p/\mathrm{L}_m\big)\Big)^\wedge \qquad (m \geq n \geq 0)$$

of (24), gives commutative diagrams of exact sequences. By taking the direct limit over n, Lemma 4.6 gives exact sequences

$$\begin{aligned} 0 \longrightarrow \mathcal{R}^{\pm}\big(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}\big) \longrightarrow \mathrm{H}^1(\mathscr{G}_{\mathrm{cyc}}^S, \mathsf{E}_p) \xrightarrow{\xi_p^{\pm}} \bigoplus_{v\in S}{}^{\pm}\widetilde{K}_v(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) \longrightarrow \mathscr{S}^{\pm}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})^\wedge \longrightarrow \\ \longrightarrow \mathrm{H}^2(\mathscr{G}_{\mathrm{cyc}}^S, \mathsf{E}_p) \longrightarrow \bigoplus_{w|v\in S} \mathrm{H}^2(\mathrm{L}_{\mathrm{cyc},w}, \mathsf{E}_p) \longrightarrow 0 \end{aligned} \tag{25}$$

where the morphism $\xi_p^{\pm}$ and the $\Omega(\Gamma)$-modules ${}^{\pm}\widetilde{K}_v(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})$ where introduced in (18).

We go back to the study of $\mathcal{R}^{\pm}\big(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}\big)$. Unlike the ordinary case, the full Selmer group

$$\begin{aligned} \mathrm{Sel}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}}) &= \ker\Big(\mathrm{H}^1(\mathscr{G}_\infty^S, \mathsf{E}_{p^\infty}) \longrightarrow \bigoplus_{w|v\in S} \mathrm{H}^1(\mathrm{L}_{\mathrm{cyc},w}, \mathsf{E})_{p^\infty}\Big) \\ &= \ker\Big(\mathrm{H}^1(\mathscr{G}_\infty^S, \mathsf{E}_{p^\infty}) \longrightarrow \bigoplus_{w|v\in S\setminus S^{\mathrm{ss}}} \mathrm{H}^1(\mathrm{L}_{\mathrm{cyc},w}, \mathsf{E})_{p^\infty} \oplus \bigoplus_{i=1}^{d} \mathrm{H}^1(\mathcal{L}_{\mathrm{cyc},i}, \mathsf{E}_{p^\infty})/\,\mathrm{Im}(\kappa_{\mathcal{L}_{\mathrm{cyc},i}}^{p^\infty})\Big) \end{aligned} \tag{26}$$

is not $\Lambda(\Gamma)$-cotorsion, in general. Indeed, as is discussed in the proof of [CS10, Theorem 2.6], each local term $\mathrm{H}^1(\mathcal{L}_{\mathrm{cyc},i}, \mathsf{E})_{p^\infty}$ has $\Lambda(\Gamma)$-corank equal to 0 or 1 depending on the reduction type of $\widetilde{\mathsf{E}}/\mathbb{F}_p$ and this implies that $\mathrm{Sel}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$ is not $\Lambda(\Gamma)$-cotorsion in the supersingular case. In the ordinary reduction case, Mazur asked in [Maz72, §6] whether $\mathrm{Sel}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$ is co-torsion. This is known to be true if $\mathrm{Sel}(\mathsf{E}_{p^\infty}/\mathrm{L})$ is finite or if $\mathrm{L} = \mathbb{Q}$ (see [CS10, Theorem 2.8 and Theorem 2.18]).

In the supersingular setting, both Perrin-Riou and Kobayashi reduce the size of the kernels in (26) by replacing $\mathrm{Im}(\kappa_{\mathcal{L}_{\mathrm{cyc}}}^{p^\infty})$ with the smaller subgroup $\mathrm{Im}(\kappa_{\mathcal{L}_{\mathrm{cyc}}}^{\pm,p^\infty})$, at supersingular primes. This has the effect that the corresponding *signed* Selmer group is potentially a cotorsion module over the Iwasawa algebra. We follow the same strategy, replacing E_{p^∞} by E_p, and replacing signed Selmer groups by their *fine* residual versions.

4.3. **Rank computation.** To approach $\mathcal{R}^{\pm}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})$, the main objects of study will be the maps $\xi_p^{\pm}$ appearing in the exact sequence (25). We will ultimately relate the surjectivity of $\xi_p^{\pm}$ to the structure of $\mathrm{X}^{\pm}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$ as a $\Lambda(\Gamma)$-module (see Theorem 4.12). In this direction, the following hypothesis (which is condition (vi) in [KO18, Theorem 1.3]) is crucial:

Hyp 2 The $\Lambda(\Gamma)$-modules $\mathrm{X}^{\pm}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$ are torsion and hence each admits two structural Iwasawa invariants, which we denote by $\lambda^{\pm}$ and $\mu^{\pm}$.

The exact sequence which is crucial in our approach is (25). Concerning the term $\mathrm{H}^2(\mathscr{G}_{\mathrm{cyc}}^S, \mathsf{E}_p)$ in it, Coates and the second author have proposed in [CS05] the following

Conjecture A. $\mathrm{H}^2(\mathscr{G}_{\mathrm{cyc}}^S, \mathsf{E}_p) = 0$.

The original formulation of Conjecture A in *loc. cit*. is that the dual fine Selmer group $\mathcal{Y}(\mathsf{E}/\mathrm{L}_{\mathrm{cyc}})$ over $\mathrm{L}_{\mathrm{cyc}}$ (see [CS05, §3] for its definition) is a finitely generated $\mathbb{Z}_p$-module. Note that this is equivalent to $\mathcal{Y}(\mathsf{E}/\mathrm{L}_{\mathrm{cyc}})$ being $\Lambda(\Gamma)$-torsion, and having μ-invariant equal to 0. The next proposition relates the two formulations, and shows that Conjecture A implies the Weak Leopoldt Conjecture (see Remark 4.8 below).

Proposition 4.7. *Conjecture A implies that* $\mathrm{H}^2(\mathscr{G}_{\mathrm{cyc}}^S, \mathsf{E}_{p^\infty}) = 0$. *Moreover, if* E *satisfies* ***Hyp 2****, and if* $\mu^* = 0$ *for at least one sign* $* \in \{+, -\}$, *then Conjecture A holds.*

Proof. Taking $\mathscr{G}_{\mathrm{cyc}}^S$-cohomology of the exact sequence (7) yields

$$\mathrm{H}^2(\mathscr{G}_{\mathrm{cyc}}^S, \mathsf{E}_p) \longrightarrow \mathrm{H}^2(\mathscr{G}_{\mathrm{cyc}}^S, \mathsf{E}_{p^\infty}) \xrightarrow{\cdot p} \mathrm{H}^2(\mathscr{G}_{\mathrm{cyc}}^S, \mathsf{E}_{p^\infty}) \longrightarrow 0$$

where the surjection comes from the fact that $\mathrm{Gal}(\overline{\mathrm{L}}/\mathrm{L}_{\mathrm{cyc}})$ has cohomological dimension 2 (see [NSW08, Theorem 10.11.3 and Proposition 3.3.5]). Therefore, if $\mathrm{H}^2(\mathscr{G}_{\mathrm{cyc}}^S, \mathsf{E}_p) = 0$ then multiplication by p is injective on $\mathrm{H}^2(\mathscr{G}_{\mathrm{cyc}}^S, \mathsf{E}_{p^\infty})$. On the other hand, every class in $\mathrm{H}^2(\mathscr{G}_{\mathrm{cyc}}^S, \mathsf{E}_{p^\infty})$ has finite p-power order, hence multiplication by p is injective if and only if $\mathrm{H}^2(\mathscr{G}_{\mathrm{cyc}}^S, \mathsf{E}_{p^\infty}) = 0$.

Suppose now that $\mathrm{X}^*(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$ is $\Lambda(\Gamma)$-torsion and $\mu^* = 0$. The dual fine Selmer group $\mathcal{Y}(\mathsf{E}/\mathrm{L}_{\mathrm{cyc}})$ is defined in [CS05, (42)] as the Pontryagin dual of

$$\ker\Big(\mathrm{H}^1(\mathscr{G}_{\mathrm{cyc}}^S, \mathsf{E}_{p^\infty}) \longrightarrow \bigoplus_{w|v\in S} \mathrm{H}^1(\mathrm{L}_{\mathrm{cyc},w}, \mathsf{E}_{p^\infty})\Big).$$

Since the above kernel injects into $\mathrm{Sel}^*(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$ by (19), we obtain a surjection

$$\mathrm{X}^*(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}}) \twoheadrightarrow \mathcal{Y}(\mathsf{E}/\mathrm{L}_{\mathrm{cyc}}).$$

Our assumptions imply then that $\mathcal{Y}(\mathsf{E}/\mathrm{L}_{\mathrm{cyc}})$ is a torsion $\Lambda(\Gamma)$-module with trivial μ-invariant, which is the formulation of [CS05, Conjecture A]. We are thus left to show that if $\mathcal{Y}(\mathsf{E}/\mathrm{L}_{\mathrm{cyc}})$ is $\Lambda(\Gamma)$-torsion and has trivial μ-invariant, then $\mathrm{H}^2(\mathscr{G}_{\mathrm{cyc}}^S, \mathsf{E}_p) = 0$. But Greenberg shows in [Gre11, Proposition 4.1.6] that the vanishing of $\mathrm{H}^2(\mathscr{G}_{\mathrm{cyc}}^S, \mathsf{E}_p)$ is equivalent to the p-torsion subgroup $\mathcal{Y}(\mathsf{E}/\mathrm{L}_{\mathrm{cyc}})_p$ being finite, and this is certainly the case when $\mathcal{Y}(\mathsf{E}/\mathrm{L}_{\mathrm{cyc}})$ is $\Lambda(\Gamma)$-torsion and has trivial μ-invariant. □

Remark 4.8.

1. As is evident from the proof, only the torsionness of one of the two signed dual Selmer groups $\mathrm{X}^*(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$ is needed, provided its μ-invariant vanishes.

2. The vanishing of $\mathrm{H}^2(\mathscr{G}^S_{\mathrm{cyc}}, \mathsf{E}_{p^\infty})$ is known as the *Weak Leopoldt Conjecture* (see [Sch85, p. 348] and [Gre89, Conjecture 3]). If $\mathrm{L} = \mathbb{Q}$, it holds by [Kat04, Theorem 12.4], at least for $S = \{p\}$; the case for general $S = S^{\mathrm{bad}} \cup \{p\}$ can be deduced from Kato's result by combining the exact sequence of [PR95, p. 33, (1.4.3)] with Jannsen's spectral sequence from [Jan14, Theorem 1]. Over an arbitrary base L, if $\mathrm{Sel}(\mathsf{E}/\mathrm{L})$ is finite, the vanishing can be proven by combining [CS10, Proposition 1.9] with the Hochschild–Serre spectral sequence.
3. It is clear that the validity of Conjecture A depends only upon the isomorphism class of the Galois representation E_p.

Let us now pass to the study of $\Omega(\Gamma)$-coranks of some cohomology groups, which will turn out to be a key step in the proof of our main result. In Lemma 4.9, global cohomology and local cohomology at primes where E does not have supersingular reduction are considered. Then, in Lemma 4.10, supersingular primes are treated.

Lemma 4.9. *Let $v \in S \setminus S^{\mathrm{ss}}$ and let $w \mid v$ be a place in $\mathrm{L}_{\mathrm{cyc}}$ that lies above v. Then,*

i) If $v = \mathfrak{l} \in S^{\mathrm{bad}}$, the Pontryagin duals $\mathrm{H}^1(\mathrm{L}_{\mathrm{cyc},w}, \mathsf{E}_{p^\infty})$ have μ invariant equal to 0.

ii) If $v = \pi \in S^{\mathrm{ord}}$, the Pontryagin duals of $\mathrm{H}^1(\mathrm{L}_{\mathrm{cyc},w}, \mathsf{E}_{p^\infty})/\operatorname{Im}(\kappa^{p^\infty}_{\mathrm{L}_{\mathrm{cyc},w}})$ have μ invariant equal to 0.

iii) Assuming Conjecture A, the Pontryagin dual of $\mathrm{H}^1(\mathscr{G}^S_{\mathrm{cyc}}, \mathsf{E}_{p^\infty})$ has trivial μ invariant as well.

As a consequence,

$$\operatorname{corank}_{\Omega(\Gamma)} \mathrm{H}^1(\mathrm{L}_{\mathrm{cyc},w}, \mathsf{E}_p) = \operatorname{corank}_{\Lambda(\Gamma)} \mathrm{H}^1(\mathrm{L}_{\mathrm{cyc},w}, \mathsf{E}_{p^\infty}), \qquad w \mid \mathfrak{l} \in S^{\mathrm{bad}} \tag{27}$$

$$\operatorname{corank}_{\Omega(\Gamma)} \mathrm{H}^1(\mathrm{L}_{\mathrm{cyc},w}, \widetilde{\mathsf{E}}_p) = \operatorname{corank}_{\Lambda(\Gamma)} \left(\mathrm{H}^1(\mathrm{L}_{\mathrm{cyc},w}, \mathsf{E}_{p^\infty})/\operatorname{Im}(\kappa^{p^\infty}_{\mathrm{L}_{\mathrm{cyc},w}}) \right) \qquad w \mid \pi \in S^{\mathrm{ord}} \tag{28}$$

and, assuming Conjecture A,

$$\operatorname{corank}_{\Omega(\Gamma)} \mathrm{H}^1(\mathscr{G}^S_{\mathrm{cyc}}, \mathsf{E}_p) = \operatorname{corank}_{\Lambda(\Gamma)} \mathrm{H}^1(\mathscr{G}^S_{\mathrm{cyc}}, \mathsf{E}_{p^\infty}). \tag{29}$$

Proof. We start with local cohomology, and let $v \in S \setminus S^{\mathrm{ss}}$ be any prime. Greenberg proves in [Gre89, Propositions 1 and 2] that the groups $\mathrm{H}^1(\mathrm{L}_{\mathrm{cyc},w}, \mathsf{E}_{p^\infty})$ are cofinitely generated: this implies, in particular, that their quotients $\mathrm{H}^1(\mathrm{L}_{\mathrm{cyc},w}, \mathsf{E}_{p^\infty})/\operatorname{Im}(\kappa^{p^\infty}_{\mathrm{L}_{\mathrm{cyc},w}})$ are cofinitely generated as well. Moreover, we claim that the exact sequence (7) induces

$$\mathrm{H}^1(\mathrm{L}_{\mathrm{cyc},w}, \mathsf{E}_{p^\infty}) \xrightarrow{\cdot p} \mathrm{H}^1(\mathrm{L}_{\mathrm{cyc},w}, \mathsf{E}_{p^\infty}) \longrightarrow \mathrm{H}^2(\mathrm{L}_{\mathrm{cyc},w}, \mathsf{E}_p) = 0.$$

The H^2-term in the above sequence vanishes because $G_{\mathrm{L}_{\mathrm{cyc},w}}$ has p-cohomological dimension 1, as observed in the proof of Proposition 4.1.

The fact that multiplication by p is surjective on $\mathrm{H}^1(\mathrm{L}_{\mathrm{cyc},w}, \mathsf{E}_{p^\infty})$ shows that this module is p-divisible, and thus the same holds for the quotient $\mathrm{H}^1(\mathrm{L}_{\mathrm{cyc},w}, \mathsf{E}_{p^\infty})/\operatorname{Im}(\kappa^{p^\infty}_{\mathrm{L}_{\mathrm{cyc},w}})$. Observe now that this divisibility is equivalent to their Pontryagin duals having no p-torsion and, in particular, to having trivial μ invariant. This establishes points i) and ii).

When Conjecture A holds, the same argument as above shows that multiplication by p is surjective on $\mathrm{H}^1(\mathscr{G}^S_{\mathrm{cyc}}, \mathsf{E}_{p^\infty})$, whence iii).

By Proposition 4.1-a) (*resp.* Proposition 4.1-b)), the Pontryagin duals of the $\Omega(\Gamma)$-modules $\mathrm{H}^1(\mathscr{G}^S_{\mathrm{cyc}}, \mathsf{E}_p)$ and $\mathrm{H}^1(\mathscr{G}^S_{\mathrm{cyc}}, \mathsf{E}_{p^\infty})_p$ (*resp.* $\mathrm{H}^1(\mathrm{L}_{\mathrm{cyc},w}, \mathsf{E}_p)$ and $\mathrm{H}^1(\mathrm{L}_{\mathrm{cyc},w}, \mathsf{E}_{p^\infty})_p$ for some $w \mid \mathfrak{l} \in S^{\mathrm{bad}}$) have the same rank. Now equations (27) and (29) follow from assertions i) and iii), respectively, along with the structure theorem for finitely generated $\Lambda(\Gamma)$-modules. Similarly, combining Proposition 4.1-c) with ii) yields (28). □

We finish the study of $\Omega(\Gamma)$-coranks of cohomology groups by analysing what happens at supersingular primes. Our argument is the analogue, modulo p, of [KO18, Proposition 3.32].

Lemma 4.10. *For each choice of sign $\pm$, the $\Omega(\Gamma)$-module*

$$\left(\mathrm{H}^1(\mathcal{L}_{\mathrm{cyc}}, \mathsf{E}_p)/\operatorname{Im}(\kappa^{\pm,p}_{\mathcal{L}_{\mathrm{cyc}}})\right)^\wedge$$

is finitely generated and free of rank 1.

Proof. The statement will follow once we prove that

$$\left(\mathrm{H}^1(\mathcal{L}_{\mathrm{cyc}}, \mathsf{E}_{p^\infty})/\operatorname{Im}(\kappa^{\pm,p^\infty}_{\mathcal{L}_{\mathrm{cyc}}})\right)^\wedge \tag{30}$$

is free of rank 1 as $\Lambda(\Gamma)$-module, thanks to Proposition 4.1-d).

The freeness claimed in (30) follows from [KO18, Lemma 3.31]. Indeed,

$$\left(\mathrm{H}^1(\mathcal{L}_{\mathrm{cyc}}, \mathsf{E}_{p^\infty})/\operatorname{Im}(\kappa^{\pm,p^\infty}_{\mathcal{L}_{\mathrm{cyc}}})\right)^\wedge = \ker\left(\mathrm{H}^1(\mathcal{L}_{\mathrm{cyc}}, \mathsf{E}_{p^\infty})^\wedge \longrightarrow\!\!\!\!\rightarrow \operatorname{Im}(\kappa^{\pm,p^\infty}_{\mathcal{L}_{\mathrm{cyc}}})^\wedge\right)$$

where $\mathrm{H}^1(\mathcal{L}_{\mathrm{cyc}}, \mathsf{E}_{p^\infty})^\wedge$ is $\Lambda(\Gamma)$-free of rank 2, as proven in [Gre89, Corollary 1], and $\operatorname{Im}(\kappa^{\pm,p^\infty}_{\mathcal{L}_{\mathrm{cyc}}})^\wedge$ is of $\Lambda(\Gamma)$-rank equal to 1 and has no non-trivial finite $\Lambda(\Gamma)$-submodules, as follows from [KO18, Proposition 3.28 (for $\chi = 1$)]. □

The following Proposition is essentially well-known in the ordinary case, and it has already been proven by Iovita–Pollack in the supersingular case under the assumption that E is defined over $\mathbb{Q}$, and p splits completely in $\mathrm{L}/\mathbb{Q}$ (see [IP06, Proposition 6.1]).

Proposition 4.11. *Suppose that Conjecture A holds for E/L. Then*

$$\operatorname{corank}_{\Omega(\Gamma)} \mathrm{H}^1(\mathscr{G}^S_{\mathrm{cyc}}, \mathsf{E}_p) = \sum_{\pi \in S^{\mathrm{ord}}} \operatorname{corank}_{\Omega(\Gamma)} {}^{\pm}\widetilde{K}_\pi(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) + \sum_{i=1}^{d} \operatorname{corank}_{\Omega(\Gamma)} {}^{\pm}\widetilde{K}_{\mathfrak{p}_i}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})$$

and

$$\sum_{\mathfrak{l} \in S^{\mathrm{bad}}} \operatorname{corank}_{\Omega(\Gamma)} {}^{\pm}\widetilde{K}_{\mathfrak{l}}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) = 0.$$

Proof. The proof is an adaptation of [CS10, Proof of Theorem 2.6]. We first compute the left-hand side of the first equality. In [Gre89, Proposition 3] Greenberg proves that both $\mathrm{H}^1(\mathscr{G}^S_{\mathrm{cyc}}, \mathsf{E}_{p^\infty})$ and $\mathrm{H}^2(\mathscr{G}^S_{\mathrm{cyc}}, \mathsf{E}_{p^\infty})$ are co-finitely generated over $\Lambda(\Gamma)$ and further

$$\operatorname{corank}_{\Lambda(\Gamma)} \mathrm{H}^1(\mathscr{G}^S_{\mathrm{cyc}}, \mathsf{E}_{p^\infty}) - \operatorname{corank}_{\Lambda(\Gamma)} \mathrm{H}^2(\mathscr{G}^S_{\mathrm{cyc}}, \mathsf{E}_{p^\infty}) = 2r_2 + \sum_{v \text{ real place}} d_v^-.$$

Here r_2 is the number of complex places of L and, for each real place v of L, we denote by d_v^- the dimension of the (-1)-eigenspace for a complex conjugation above v acting on $T_p(\mathsf{E}) \otimes \mathbb{Q}_p$. By Proposition 4.7, the H^2-term vanishes and, by the Galois invariance of the Weil pairing, we know that $d_v^- = 1$ for all real v. Hence,

$$\operatorname{corank}_{\Lambda(\Gamma)} \mathrm{H}^1(\mathscr{G}^S_{\mathrm{cyc}}, \mathsf{E}_{p^\infty}) = [\mathrm{L} : \mathbb{Q}] = N.$$

Now (29) of Lemma 4.9 implies

$$\operatorname{corank}_{\Omega(\Gamma)} \mathrm{H}^1(\mathscr{G}^S_{\mathrm{cyc}}, \mathsf{E}_p) = \operatorname{corank}_{\Lambda(\Gamma)} \mathrm{H}^1(\mathscr{G}^S_{\mathrm{cyc}}, \mathsf{E}_{p^\infty}) = N.$$

Passing to the computation of the local coranks, let first $\pi \in S^{\mathrm{ord}}$. By [CS10, §2.13] (which applies here, thanks to our convention that $\kappa^{\pm,p^\infty}_{\mathrm{L}_{\mathrm{cyc},w}} = \kappa^{p^\infty}_{\mathrm{L}_{\mathrm{cyc},w}}$ when $\pi \in S^{\mathrm{ord}}$) we know

$$\mathrm{corank}_{\Lambda(\Gamma)} \bigoplus_{w|\pi} \Big(\mathrm{H}^1(\mathrm{L}_{\mathrm{cyc},w}, \mathsf{E}_{p^\infty}) / \operatorname{Im}(\kappa^{\pm,p^\infty}_{\mathrm{L}_{\mathrm{cyc},w}}) \Big) = [\mathrm{L}_\pi : \mathbb{Q}_p].$$

Hence equation (28) of Lemma 4.9 yields

$$\mathrm{corank}_{\Omega(\Gamma)} \bigoplus_{w|\pi} \mathrm{H}^1(\mathrm{L}_{\mathrm{cyc},w}, \widetilde{\mathsf{E}}_p) = \mathrm{corank}_{\Omega(\Gamma)} {}^{\pm}\widetilde{K}_\pi(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) = [\mathrm{L}_\pi : \mathbb{Q}_p]. \tag{31}$$

Consider now a prime $\mathfrak{p}_i \in S^{\mathrm{ss}}$. Lemma 4.10 implies that

$$\mathrm{corank}_{\Omega(\Gamma)} \big(\mathrm{H}^1(\mathcal{L}_{\mathrm{cyc},i}, \mathsf{E}_p) / \operatorname{Im}(\kappa^{\pm,p}_{\mathcal{L}_{\mathrm{cyc}}}) \big) = \mathrm{corank}_{\Omega(\Gamma)} {}^{\pm}\widetilde{K}_{\mathfrak{p}_i}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) = 1. \tag{32}$$

Combining (31) and (32), we find

$$\sum_{\pi \in S^{\mathrm{ord}}} \mathrm{corank}_{\Omega(\Gamma)} {}^{\pm}\widetilde{K}_\pi(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) + \sum_{i=1}^{d} \mathrm{corank}_{\Omega(\Gamma)} {}^{\pm}\widetilde{K}_{\mathfrak{p}_i}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) = N$$

Now suppose that $\mathfrak{l}$ is a prime in S^{bad} and let $\mathfrak{q}$ be an extension of $\mathfrak{l}$ to $\mathrm{L}_{\mathrm{cyc}}$. Greenberg proves in [Gre89, Proposition 2] that the $\Lambda(\Gamma)$-module $\mathrm{H}^1(\mathrm{L}_{\mathrm{cyc},\mathfrak{q}}, \mathsf{E}_{p^\infty})$ is cotorsion. Hence (27) of Lemma 4.9 implies

$$\mathrm{corank}_{\Omega(\Gamma)} {}^{\pm}\widetilde{K}_{\mathfrak{l}}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) = \sum_{\mathfrak{q}|\mathfrak{l}} \mathrm{corank}_{\Omega(\Gamma)} \mathrm{H}^1(\mathrm{L}_{\mathrm{cyc},\mathfrak{q}}, \mathsf{E}_p) = \sum_{\mathfrak{q}|\mathfrak{l}} \mathrm{corank}_{\Lambda(\Gamma)} \mathrm{H}^1(\mathrm{L}_{\mathrm{cyc},\mathfrak{q}}, \mathsf{E}_{p^\infty}) = 0.$$

This completes the proof of the proposition. □

4.4. **Main results.** We are now in a position to state and prove our main result. Recall the exact sequence (25)

$$\begin{aligned} 0 \longrightarrow \mathcal{R}^{\pm}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) \longrightarrow \mathrm{H}^1(\mathscr{G}^S_{\mathrm{cyc}}, \mathsf{E}_p) \xrightarrow{\xi^{\pm}_p} \bigoplus_{v\in S} {}^{\pm}\widetilde{K}_v(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) \longrightarrow \mathscr{S}^{\pm}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})^{\wedge} \longrightarrow \\ \longrightarrow \mathrm{H}^2(\mathscr{G}^S_{\mathrm{cyc}}, \mathsf{E}_p) \longrightarrow \bigoplus_{w|v\in S} \mathrm{H}^2(\mathrm{L}_{\mathrm{cyc},w}, \mathsf{E}_p) \longrightarrow 0 \end{aligned} \tag{25}$$

and consider the projection

$$\mathrm{pr}_{S_p} : \bigoplus_{v\in S} {}^{\pm}\widetilde{K}_v(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) \to \bigoplus_{v\in S_p} {}^{\pm}\widetilde{K}_v(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}).$$

Define $\vartheta^{\pm}_{\mathsf{E}_p,S_p}$, or simply $\vartheta^{\pm}_{p,S_p}$, as the composition $\mathrm{pr}_{S_p} \circ \xi^{\pm}_p$.

Theorem 4.12. *Under our standing assumptions* ***Hyp 1*** *and* ***Hyp 2****, the following assertions are equivalent:*

a) $\xi^{\pm}_p$ *is surjective and Conjecture A holds;*
b) $\vartheta^{\pm}_{p,S_p}$ *is surjective and Conjecture A holds;*
c) $\mathcal{R}^{\pm}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})$ *is* $\Omega(\Gamma)$*-cotorsion;*
d) $\mathrm{X}^{\pm}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$ *has trivial* μ*-invariant.*

Proof. To show that a) $\Rightarrow$ c), take Pontryagin duals of the short exact sequence

$$0 \longrightarrow \mathcal{R}^{\pm}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) \longrightarrow \mathrm{H}^1(\mathscr{G}^S_{\mathrm{cyc}},\mathsf{E}_p) \xrightarrow{\xi_p^{\pm}} \bigoplus_{v\in S} {}^{\pm}\widetilde{K}_v(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) \longrightarrow 0$$

to obtain

$$0 \longrightarrow \bigoplus_{v\in S} {}^{\pm}\widetilde{K}_v(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})^{\wedge} \xrightarrow{\xi_p^{\pm\wedge}} \mathrm{H}^1(\mathscr{G}^S_{\mathrm{cyc}},\mathsf{E}_p)^{\wedge} \longrightarrow \mathrm{Y}^{\pm}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) \longrightarrow 0. \tag{33}$$

By Proposition 4.11, the first two terms have the same $\Omega(\Gamma)$-rank, so the third is $\Omega(\Gamma)$-torsion and c) follows. Also, when a) holds, the composition $\vartheta^{\pm}_{p,S_p} = \mathrm{pr}_{S_p}\circ\xi_p^{\pm}$ is surjective, yielding a) $\Rightarrow$ b).

To show that c) and d) are equivalent, we first observe that a finitely generated torsion $\Lambda(\Gamma)$-module M has trivial μ-invariant if and only if M/pM is a torsion $\Omega(\Gamma)$-module. On the other hand, taking Pontryagin duals of the injection of Corollary 4.5 shows that the kernel of

$$\Big(\mathrm{Sel}^{\pm}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})\Big)_p^{\wedge} = \mathrm{X}^{\pm}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})/p\,\mathrm{X}^{\pm}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}}) \twoheadrightarrow \mathrm{Y}^{\pm}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})$$

is finite, showing the equivalence between c) and d). Therefore, b) $\Leftarrow$ a) $\Rightarrow$ c) $\Leftrightarrow$ d).

We are left with the implications c) $\Rightarrow$ a) and b) $\Rightarrow$ a). Since c) $\Rightarrow$ d) $\Rightarrow$ Conjecture A, and b) contains Conjecture A, we can assume from now on that $\mathrm{H}^2(\mathscr{G}^S_{cyc},\mathsf{E}_p) = 0$. In particular, the sequence (25) becomes

$$0 \longrightarrow \mathcal{R}^{\pm}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) \longrightarrow \mathrm{H}^1(\mathscr{G}^S_{\mathrm{cyc}},\mathsf{E}_p) \xrightarrow{\xi_p^{\pm}} \bigoplus_{v\in S} {}^{\pm}\widetilde{K}_v(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) \longrightarrow \mathscr{S}^{\pm}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})^{\wedge} = \mathrm{coker}(\xi_p^{\pm}) \longrightarrow 0 \tag{34}$$

and Proposition 4.11 yields

$$\mathrm{corank}_{\Omega(\Gamma)}\big(\mathcal{R}^{\pm}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})\big) = \mathrm{corank}_{\Omega(\Gamma)}\big(\mathscr{S}^{\pm}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})\big).$$

Assuming c), it follows that $\mathscr{S}^{\pm}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})$ is $\Omega(\Gamma)$-torsion. On the other $\mathscr{S}^{\pm}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})$ is $\Omega(\Gamma)$-free, in light of Lemma 4.6, and to be $\Omega(\Gamma)$-torsion it must be trivial, establishing c) $\Rightarrow$ a).

Finally, assume that $\vartheta^{\pm}_{p,S_p}$ is surjective and consider the commutative triangle

$$\begin{array}{ccc} \mathrm{H}^1(\mathscr{G}^S_{\mathrm{cyc}},\mathsf{E}_p) & \xrightarrow{\xi_p^{\pm}} & \displaystyle\bigoplus_{\mathfrak{l}\in S^{\mathrm{bad}}} {}^{\pm}\widetilde{K}_{\mathfrak{l}}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) \oplus \bigoplus_{v\in S_p} {}^{\pm}\widetilde{K}_v(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) \\ & \searrow^{\vartheta^{\pm}_{p,S_p}} & \downarrow{\scriptstyle \mathrm{pr}_{S_p}} \\ & & \displaystyle\bigoplus_{v\in S_p} {}^{\pm}\widetilde{K}_v(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}). \end{array}$$

It induces an exact sequence

$$\ker(\mathrm{pr}_{S_p}) = \bigoplus_{\mathfrak{l}\in S^{\mathrm{bad}}} {}^{\pm}\widetilde{K}_{\mathfrak{l}}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) \longrightarrow \mathrm{coker}(\xi_p^{\pm}) \longrightarrow \mathrm{coker}(\vartheta^{\pm}_{p,S_p}) = 0$$

which implies that $\mathrm{coker}(\xi_p^{\pm})$ is cotorsion, thanks to Proposition 4.11. Since $\mathrm{coker}(\xi_p^{\pm})$ is isomorphic to $\mathscr{S}^{\pm}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})^{\wedge}$ by (34), and $\mathscr{S}^{\pm}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})$ is free by Lemma 4.6, this forces $\mathrm{coker}(\xi_p^{\pm}) = 0$, establishing the final implication b) $\Rightarrow$ a). $\square$

Remark 4.13. Note that Conjecture A is pivotal to the proof and plays the role of the Weak Leopoldt Conjecture for the residual representation E_p.

As an application of Theorem 4.12, we obtain a result along the lines of Greenberg–Vatsal's work [GV00, Theorem 1.4] in the supersingular setting. Results somewhat similar to Theorem 4.14 below, again in the supersingular setting, have been obtained by Kim in [Kim09, Corollary 2.13] and by Hatley–Lei in [HL19, Theorem 4.6], by different methods.

We denote by

$$\rho_{\mathsf{E}}^{\pm} = \dim_{\mathbb{F}_p} \mathrm{Y}^{\pm}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) \tag{35}$$

the $\mathbb{F}_p$-dimension of $\mathrm{Y}^{\pm}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})$. It clearly depends only upon the isomorphism class of E_p and not on E itself.

Theorem 4.14. *Let $\mathsf{E}_1, \mathsf{E}_2$ be two elliptic curves defined over L, satisfying hypotheses **Hyp 1** and **Hyp 2**. Suppose that the residual Galois representations $(\mathsf{E}_1)_p$ and $(\mathsf{E}_2)_p$ are isomorphic.*

Let $\mu_{\mathsf{E}_j}^{\pm}$ and $\lambda_{\mathsf{E}_j}^{\pm}$ be the Iwasawa invariants of $\mathrm{X}^{\pm}((\mathsf{E}_j)_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$, for $j = 1, 2$. Then, for both choices of sign,

$$\mu_{\mathsf{E}_1}^{\pm} = 0 \Longleftrightarrow \mu_{\mathsf{E}_2}^{\pm} = 0. \tag{36}$$

For each sign $* \in \{+, -\}$ for which this vanishing happens, we also have

$$\lambda_{\mathsf{E}_j}^{*} = \rho^{*} + \delta_{\mathsf{E}_j} \tag{37}$$

where δ_{E_j} is as in Definition 4.4 and $\rho^{\pm} := \rho_{\mathsf{E}_1}^{\pm} = \rho_{\mathsf{E}_2}^{\pm}$ is as in (35).

Remark 4.15. As already observed in Corollary 4.5, the quantity δ_{E} is independent of the choice of sign in $\{+, -\}$. In particular, for elliptic curves satisfying **Hyp 1** and **Hyp 2** and such that both their signed μ-invariants are 0, the difference of the signed $\lambda^{\pm}$-invariants depends only on the isomorphism class of the residual representation.

The concrete way in which this result will be applied later, is the following. Suppose we are given a family of elliptic curves (satisfying **Hyp 1** and **Hyp 2**) with the property that their residual representations are isomorphic. If one member A in the family satisfies $\mu_{\mathsf{A}}^{+} = \mu_{\mathsf{A}}^{-} = 0$, then for all other members E in the family, we obtain $\mu_{\mathsf{E}}^{\pm} = 0$ and the difference of signed Iwasawa invariants

$$\lambda_{\mathsf{E}}^{+} - \lambda_{\mathsf{E}}^{-} = \rho_{\mathsf{A}}^{+} - \rho_{\mathsf{A}}^{-}$$

is constant. In particular, if $\rho_{\mathsf{A}}^{+} = \rho_{\mathsf{A}}^{-}$, then $\lambda_{\mathsf{E}}^{+} = \lambda_{\mathsf{E}}^{-}$ for all curves E in the family.

Proof. Observe first that if $\mu_{\mathsf{E}_j}^{*} = 0$ for one sign $* \in \{+, -\}$ and one curve E_j, then Conjecture A holds for both curves, thanks to Proposition 4.7. Moreover, Proposition 3.9-i) shows that the sets S^{ss} and S^{ord} consisting of primes of supersingular (*resp.* ordinary) reduction for E_1 and E_2 coincide.

Fix an isomorphism $(\mathsf{E}_1)_p \cong (\mathsf{E}_2)_p$ and consider the maps

$$\vartheta^{\pm}_{(\mathsf{E}_j)_p, S_p} \colon \mathrm{H}^1(\mathscr{G}^S_{\mathrm{cyc}}, (\mathsf{E}_j)_p) \longrightarrow \bigoplus_{v \in S_p} {}^{\pm}\widetilde{K}_v(\mathsf{E}_j/\mathrm{L}_{\mathrm{cyc}}) = \bigoplus_{\pi \in S^{\mathrm{ord}}} \bigoplus_{w \mid \pi} \mathrm{H}^1(\mathrm{L}_{\mathrm{cyc},w}, (\widetilde{\mathsf{E}}_j)_p) \oplus \bigoplus_{i=1}^{d} \mathrm{H}^1\big(\mathcal{L}_{n,i}, (\mathsf{E}_j)_p\big) / \operatorname{Im} \kappa^{\pm,p}_{\mathcal{L}_{n,i}}$$

defined before Theorem 4.12. For all $w \mid \pi \in S^{\mathrm{ord}}$, the chosen isomorphism induces an isomorphism between the $\mathrm{H}^1(\mathrm{L}_{\mathrm{cyc},w}, (\widetilde{\mathsf{E}}_j)_p)$ (for $j = 1, 2$) by to Proposition 3.9-ii). Similarly, at every prime in S^{ss}, Proposition 3.8 gives an isomorphism between the groups

$$\mathrm{H}^1\big(\mathcal{L}_{n,}, (\mathsf{E}_j)_p\big) / \operatorname{Im} \kappa^{\pm,p}_{\mathcal{L}_{n,}},$$

for $j = 1, 2$. It follows that $\vartheta^{\pm}_{(\mathsf{E}_1)_p, S_p}$ is surjective if and only if $\vartheta^{\pm}_{(\mathsf{E}_2)_p, S_p}$ is surjective. Theorem 4.12 now yields (36).

Suppose now that $* \in \{+, -\}$ is such that $\mu^*_{\mathsf{E}_1} = \mu^*_{\mathsf{E}_2} = 0$. By [KO18, Theorem 4.8], the Pontryagin duals of the signed Selmer groups $\mathrm{X}^*((\mathsf{E}_j)_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$ do not have any non-zero finite $\Lambda(\Gamma)$-submodule. Further, they are $\Lambda(\Gamma)$-torsion thanks to hypothesis **Hyp 2**. Therefore, for $j = 1, 2$,

$$\lambda^*_{\mathsf{E}_j} = \mathrm{length}\Big(\mathrm{X}^*((\mathsf{E}_j)_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})/p\,\mathrm{X}^*((\mathsf{E}_j)_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})\Big).$$

On the other hand, taking Pontryagin duals in Corollary 4.5 gives an exact sequence

$$V_j \hookrightarrow \Big(\mathrm{Sel}^*\big((\mathsf{E}_j)_{p^\infty}/\mathrm{L}_{\mathrm{cyc}}\big)_p\Big)^\wedge = \mathrm{X}^*((\mathsf{E}_j)_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})/p\,\mathrm{X}^*((\mathsf{E}_j)_{p^\infty}/\mathrm{L}_{\mathrm{cyc}}) \twoheadrightarrow \mathrm{Y}^*((\mathsf{E}_j)_p/\mathrm{L}_{\mathrm{cyc}}) \tag{38}$$

where V_j is an $\mathbb{F}_p$-vector space of finite dimension. Since we are assuming $\mu^*_{\mathsf{E}_j} = 0$, Theorem 4.12 implies that $\xi^*_{(\mathsf{E}_j)_p}$ is surjective and therefore, again by Corollary 4.5, we have $\dim_{\mathbb{F}_p} V_j = \delta_{\mathsf{E}_j}$. Taking lengths in (38) gives

$$\lambda^*_{\mathsf{E}_j} = \rho^* + \delta_{\mathsf{E}_j}.$$

and this finishes the proof. □

In the next two corollaries, we consider the main setting of Theorem 4.14. Thus, let $\mathsf{E}_1, \mathsf{E}_2$ be two elliptic curves defined over L satisfying hypotheses **Hyp 1** and **Hyp 2**, and such that the residual Galois representations $(\mathsf{E}_1)_p$ and $(\mathsf{E}_2)_p$ are isomorphic, so $\rho^{\pm}_{\mathsf{E}_1} = \rho^{\pm}_{\mathsf{E}_2} := \rho^{\pm}$. By Proposition 3.9-i), the set S^{ord} of p-adic primes where the curves have good, ordinary reduction, coincide. Further, we assume that $\mu^*_{\mathsf{E}_1} = 0$ for one symbol $* \in \{+, -\}$, which is equivalent to assuming $\mu^*_{\mathsf{E}_2} = 0$ by Theorem 4.14. Moreover, either implies that Conjecture A holds for both curves, again by Theorem 4.14.

Corollary 4.16. *Let S_1^{bad} and S_2^{bad}, be the sets of primes of bad reduction for E_1 and E_2, respectively. If, for both indices $j \in \{1, 2\}$, we have $\mathsf{E}_j(\mathrm{L}_v)_p = 0$ for all $v \in S^{\mathrm{ord}} \cup S_j^{\mathrm{bad}}$, then*

$$\lambda^*_{\mathsf{E}_1} = \lambda^*_{\mathsf{E}_2} = \rho^*.$$

Proof. Recall from Definition 4.4 that

$$\delta_{\mathsf{E}_j} = \sum_{\mathfrak{l} \in S_j^{\mathrm{bad}}} g_{\mathfrak{l}} \cdot \dim_{\mathbb{F}_p} \mathsf{E}_j(\mathrm{L}^1_{\mathfrak{q}})_p + \sum_{\pi \in S^{\mathrm{ord}}} g_\pi \dim_{\mathbb{F}_p} \widetilde{\mathsf{E}}_j(\mathbb{F}_\pi)_p \tag{39}$$

where $\mathfrak{q}$ is a prime in $\mathrm{L}_{\mathrm{cyc}}$ above $\mathfrak{l}$.

The same argument as in the proof of Corollary 4.5 shows that the condition $\mathsf{E}_j(\mathrm{L}_{\mathfrak{l}})_p = 0$ is equivalent to $\mathsf{E}_j(\mathrm{L}_{\mathrm{cyc},\mathfrak{q}})_p = 0$ for all $\mathfrak{q} \mid \mathfrak{l}$. In particular, the hypothesis of the corollary imply $\mathsf{E}_j(\mathrm{L}^1_{\mathfrak{q}})_p$ for all $\mathfrak{q} \mid \mathfrak{l}$. Similarly, there are surjections

$$\mathsf{E}_j(\mathrm{L}_\pi)_p \twoheadrightarrow \widetilde{\mathsf{E}}_j(\mathbb{F}_\pi)_p$$

so $\mathsf{E}_j(\mathrm{L}_\pi)_p = 0$ implies $\widetilde{\mathsf{E}}_j(\mathbb{F}_\pi)_p = 0$.

Hence all terms in (39) vanish and $\delta_{\mathsf{E}_1} = \delta_{\mathsf{E}_2} = 0$. The corollary follows from (37). □

Recall that, given a prime $v \in S$, we denote by g_v the number of primes $w \mid v$ in $\mathrm{L}_{\mathrm{cyc}}$.

Corollary 4.17. *Suppose that E_1 is a CM curve. Then*

$$\lambda^*_{\mathsf{E}_2} = \left(\rho^* + \sum_{\pi \in S^{\mathrm{ord}}} g_\pi \dim_{\mathbb{F}_p} \widetilde{\mathsf{E}}_1(\mathbb{F}_\pi)_p \right) + \sum_{\mathfrak{l} \in S_2^{\mathrm{bad}}} g_\mathfrak{l} \cdot \dim_{\mathbb{F}_p} \mathsf{E}_2(\mathrm{L}_\mathfrak{l})_p$$

Remark 4.18. The interest of Corollary 4.17 lies in the fact that the quantity in parenthesis is constant along families with isomorphic residual representation at p. Moreover, the final sum in the right-hand side only depends on the groups $\mathsf{E}_2(\mathrm{L}_\mathfrak{l})_p$ (for $\mathfrak{l} \in S_2^{\mathrm{bad}}$) and not on the behaviour of p-torsion along the local cyclotomic towers. As we shall see in the proof, the corollary still holds only assuming that the image of $\mathrm{Gal}(\overline{\mathrm{L}}/\mathrm{L})$ inside $\mathrm{Aut}\big((\mathsf{E}_1)_p\big) \subseteq \mathrm{GL}_2(\mathbb{F}_p)$ is contained in the normalizer of a Cartan subroup, which is certainly the case when E_1 is CM.

Proof. Since E_1 is CM and $p \geq 3$, the image of $\mathrm{Gal}(\overline{\mathrm{L}}/\mathrm{L})$ inside $\mathrm{Aut}\big((\mathsf{E}_1)_p\big) \subseteq \mathrm{GL}_2(\mathbb{F}_p)$ is contained in the normalizer of a Cartan subroup. In particular, it contains no element of order p, and the same holds for the image of $\mathrm{Gal}(\overline{\mathrm{L}}/\mathrm{L})$ inside $\mathrm{Aut}\big((\mathsf{E}_2)_p\big)$ because the representations are isomorphic. It follows that, for all $\mathfrak{q} \mid \mathfrak{l}$, the pro-$p$-group $\Gamma = \mathrm{Gal}(\mathrm{L}_{\mathrm{cyc},\mathfrak{q}}/\mathrm{L}_\mathfrak{l})$ acts trivially on $\mathsf{E}_2(\mathrm{L}_{\mathrm{cyc},\mathfrak{q}})_p$, and $\dim_{\mathbb{F}_p} \mathsf{E}_2(\mathrm{L}_\mathfrak{l})_p = \dim_{\mathbb{F}_p} \mathsf{E}_2(\mathrm{L}^1_\mathfrak{q})_p$. The corollary follows from (37), combined with Definition 4.4. □

5. Numerical Examples

Our class of examples comes from the work [RS95]. Both for $p = 3$ and $p = 5$, Rubin and Silverberg define, for each $D \not\equiv 0 \pmod{p}$, a family parametrised by[1] $t \in \mathbb{Z}$. All curves in the families have good, supersingular reduction at p and isomorphic residual Galois representations. In particular, the reduction type is constant along families and, since all curves are defined over $\mathbb{Q}$, in all cases $S^{\mathrm{ord}} = \emptyset$. Finally, observe that Rubin–Silverberg's construction shows that all family contain a CM member, and so Corollary 4.17 applies. For all choices of (p, D), the strategy will be to

1. Find one curve A in the family for which the Iwasawa invariants $\mu^\pm_\mathsf{A}$ and $\lambda^\pm_\mathsf{A}$ have been computed in [LMF13] and such that $\mu^\pm_\mathsf{A} = 0$. In practice, we take for A the CM curve corresponding to the parameter $t = 0$.
2. Apply Theorem 4.14 (see in particular Remark 4.15) to deduce that $\mu^\pm = 0$ for all other members in the family. In particular, Conjecture A holds for the whole family, by Proposition 4.7.
3. Deduce from formula (37) for $\lambda^\pm$-invariants that $\rho^\pm_\mathsf{A} = \lambda^\pm_\mathsf{A} - \delta_\mathsf{A}$ for A, and set $\rho^\pm := \rho^\pm_\mathsf{A}$.
4. By Corollary 4.17, we obtain
$$\lambda^\pm_\mathsf{E} = \rho^\pm + \delta_\mathsf{E} = \sum_{\ell \in S^{\mathrm{bad}}} g_\ell \dim_{\mathbb{F}_p} \mathsf{E}(\mathbb{Q}_\ell)_p$$
for all E in the family.
5. The key step is to find elliptic curves E in the family satisfying $a_p(\mathsf{E}) = 0$, to ensure that **Hyp 1** holds. Note that this is only needed when $p = 3$, because when $p = 5$ the condition $a_5(\mathsf{E}) = 0$ is automatically satisfied by the Hasse bound. Since all our examples are defined over $\mathbb{Q}$, **Hyp 2** is always satisfied by [Kob03, Theorem 1.2].
6. Choosing any curve as in (5.), we compute the $\mathbb{F}_p$-dimension of $\mathsf{E}(\mathbb{Q}_\ell)_p$ at all primes $\ell \in S^{\mathrm{bad}}$, together with the number of primes in $\mathbb{Q}^{\mathrm{cyc}}$ above ℓ, to find the numerical value of δ_E and hence of $\lambda^\pm_\mathsf{E}$.

[1] Actually, the parameters in the families can vary in $\mathbb{Q}$, but are required to be p-integral to define curves with good reduction at p. In our examples, we will restrict to $t \in \mathbb{Z}$

We will consider the families attached to $D = 1, -1$ for $p = 3$, and the families attached to $D = 3$ and $D = 14$ for $p = 5$. Our source of numerical data is [LMF13]. Labels of elliptic curves follow Cremona's tables as in [LMF13], when available (*i. e.* for discriminant less than 500.000 as per October 2019). The computations have been made in SAGE[2].

5.1. $p = 3$.

5.1.1. $D = 1$. Setting $t = 0$ we obtain the CM curve $\mathsf{A} = 32a2$ given by $y^2 = x^3 - x$. It satisfies $\mu_{\mathsf{A}}^{\pm} = \lambda_{\mathsf{A}}^{\pm} = 0$ and this is in accordance with the fact that we found $\delta_{\mathsf{A}} = 0$: indeed, $S_{\mathsf{A}}^{\mathrm{bad}} = \{2\}$ and $\mathsf{A}(\mathbb{Q}_2)_3 = 0$. Moreover, $a_3(\mathsf{A}) = 0$, and we obtain $\rho^{\pm} = 0$. The curves corresponding to $t = 1$ and $t = 2$ are, respectively, $\mathsf{E}_1 = 352f1$ and $\mathsf{E}_2 = 16096h1$: since $a_3(\mathsf{E}_1) = -3$ and $a_3(\mathsf{E}_2) = 3$, we discard them.

The curve corresponding to $t = 3$ is $\mathsf{E}_3 = 18784b1$, and $a_3(\mathsf{E}_3) = 0$. Its Iwasawa invariants are available on [LMF13], and indeed $\mu_{\mathsf{E}_3}^{\pm} = 0$. The primes of bad reduction are $S^{\mathrm{bad}} = \{2, 587\}$. We found $\mathsf{E}_3(\mathbb{Q}_2)_3 = 0$ and $\mathsf{E}_3(\mathbb{Q}_{587})_3 = \mathbb{Z}/3\mathbb{Z}$; since 587 is a generator of $\mathbb{Z}/9\mathbb{Z}$, it is totally inert in $\mathbb{Q}^{\mathrm{cyc}}/\mathbb{Q}$, so $g_{357} = 1$. Formula (37) gives $\lambda_{\mathsf{E}_3}^{\pm} = 1$, in accordance with the numerical value found in [LMF13].

To show a somehow extreme example, consider $t = 18$. It satisfies $a_3(\mathsf{E}_{18}) = 0$ and its conductor is $90.885.856 = 2^5 \cdot 2840183$. The dimensions of its local 3-torsion are

$$\dim_{\mathbb{F}_3}\left(\mathsf{E}_{18}(\mathbb{Q}_\ell)_3\right) = \begin{cases} 0 & \text{for } \ell = 2 \\ 1 & \text{for } \ell = 2840183 \end{cases}$$

The multiplicative order of 2840183 modulo 3^7 being 6, we deduce $g_{2840183} = 3^6$, whence $\lambda_{\mathsf{E}_{18}}^{\pm} = 729$, and $\mu_{\mathsf{E}_{18}}^{\pm} = 0$ by Theorem 4.14. It is relevant here to note Kim's observation that under these assumptions the Iwasawa $\lambda^{\pm}$-invariants can be arbitrarily large in the family (see [Kim09, p. 190]), although he does not produce explicit examples. Note also that these Iwasawa invariants are not available on [LMF13].

5.1.2. $D = -1$. In this case, the CM curve for $t = 0$ is $\mathsf{A} = 64a4$ given by $y^2 = x^3 + x$. Again, $\mu_{\mathsf{A}}^{\pm} = \lambda_{\mathsf{A}}^{\pm} = 0 = a_3(\mathsf{A})$. We computed the defect and found $\delta_{\mathsf{A}} = 0$, since $S_{\mathsf{A}}^{\mathrm{bad}} = \{2\}$ and $\mathsf{A}(\mathbb{Q}_2)_3 = 0$. We obtain $\rho^{\pm} = 0$. The curves corresponding to the parameters $t = 2, 4, 5$ are, respectively, $\mathsf{E}_2 = 22976p1$, $\mathsf{E}_4 = 423872t1$ and $\mathsf{E}_5 = 131392f1$. They all exist in [LMF13], and have $a_3(\mathsf{E}_i) = 0$, but the Iwasawa invariants are available only for E_2 and E_5: they read $\lambda_{\mathsf{E}_2}^{\pm} = 3, \lambda_{\mathsf{E}_5}^{\pm} = 0$. This is in accordance with formula (37): indeed, $S_{\mathsf{E}_2}^{\mathrm{bad}} = \{2, 359\}$, $S_{\mathsf{E}_5}^{\mathrm{bad}} = \{2, 2053\}$ and

$$\dim_{\mathbb{F}_3}\left(\mathsf{E}_2(\mathbb{Q}_\ell)_3\right) = \begin{cases} 0 & \text{for } \ell = 2 \\ 1 & \text{for } \ell = 359 \end{cases} \qquad \dim_{\mathbb{F}_3}\left(\mathsf{E}_5(\mathbb{Q}_\ell)_3\right) = \begin{cases} 0 & \text{for } \ell = 2 \\ 0 & \text{for } \ell = 2053 \end{cases}$$

This immediately implies $\delta_{\mathsf{E}_5} = 0$, so $\lambda_{\mathsf{E}_5}^{\pm} = 0$. As 359 has order 6 modulo 27, we obtain $g_{359} = 3$, whence $\delta_{\mathsf{E}_2} = \lambda_{\mathsf{E}_5}^{\pm} = 3$. The curve E_4 can be treated analogously, since $S_{\mathsf{E}_4}^{\mathrm{bad}} = \{2, 37, 179\}$ and

$$\dim_{\mathbb{F}_3}\left(\mathsf{E}_4(\mathbb{Q}_\ell)_3\right) = \begin{cases} 0 & \text{for } \ell = 2 \\ 2 & \text{for } \ell = 37 \\ 1 & \text{for } \ell = 179 \end{cases}$$

Further, $g_{37} = g_{179} = 3$, whence $\lambda_{\mathsf{E}_4}^{\pm} = 9$, a value which is not available on [LMF13]. Also, all curves satisfy $\mu^{\pm} = 0$ by Theorem 4.14.

[2] We used commands `E.q_expansion(4)` to compute a_3 and `E(0).division_points(p)` to compute torsion points.

We finish this series of examples with the curve E_{149} for $t = 149$. Its conductor is $106.459.833.664 = 2 \cdot 1663434901$, so it has no label in Cremona's tables, but we can compute $a_3(\mathsf{E}_{149}) = 0$. We found $\mathsf{E}_{149}(\mathbb{Q}_2)_3 = \mathsf{E}_{149}(\mathbb{Q}_{1663434901})_3 = 0$, whence $\mu^{\pm}_{\mathsf{E}_{149}} = \lambda^{\pm}_{\mathsf{E}_{149}} = 0$.

5.2. $p = 5$.

5.2.1. $D = 3$. The CM curve corresponding to $t = 0$ is $\mathsf{A} = 3888s1$, given by $y^2 = x^3 + 48$. Its Iwasawa invariants are computed in [LMF13] and $\mu^{\pm}_{\mathsf{A}} = 0, \lambda^{\pm}_{\mathsf{A}} = 1$. To find $\rho^{\pm} = \rho^{\pm}_{\mathsf{A}}$, we need to compute δ_{A}. The primes of bad reduction are $S^{\mathrm{bad}}_{\mathsf{A}} = \{2, 3\}$ and $\mathsf{A}(\mathbb{Q}_\ell)_3 = 0$ for both $\ell \in S^{\mathrm{bad}}_{\mathsf{A}}$, so $\delta_{\mathsf{A}} = 0$ and $\rho^{\pm} = 1$. The conductors of E_t for $t \in [-5, 15]$ have orders of magnitude between 10^7 and 10^{20} (except for $\mathsf{E}_0 = \mathsf{A}$), so these curves are not implemented in [LMF13]. Computing Iwasawa invariants through formula (37) is almost immediate. As an example, we compute them for the curves E_6 and E_{14} corresponding to $t = 6$ and $t = 14$, respectively. First, we immediately obtain from Theorem 4.14 that $\mu^{\pm}_{\mathsf{E}_6} = \mu^{\pm}_{\mathsf{E}_{14}} = 0$.

The conductor of E_6 is $16.847.046.490.346.928 = 2^4 \cdot 3^5 \cdot 4333088089081$. The curve has no $\mathbb{Q}_\ell$-rational 5-torsion points for any of the primes $\ell \in \{2, 3, 4333088089081\}$, so $\delta_{\mathsf{E}_6} = 0$. It follows that $\lambda^{\pm}_{\mathsf{E}_6} = \rho^{\pm} = 1$. The conductor of E_{14} is $445.766.016.078.830.163.888 = 2^4 \cdot 3^5 \cdot 29 \cdot 602279 \cdot 6564248011$ and E_{14} does not have neither $\mathbb{Q}_2$-rational nor $\mathbb{Q}_3$-rational 5-torsion points. On the other hand,

$$\dim_{\mathbb{F}_5}\Big(\mathsf{E}_{14}(\mathbb{Q}_\ell)_5\Big) = \begin{cases} 1 & \text{for } \ell = 29 \\ 1 & \text{for } \ell = 602279 \\ 2 & \text{for } \ell = 6564248011 \end{cases}$$

Further, computing multiplicative orders modulo 25, we find $g_\ell = 1$ for all $\ell \in \{29, 602279, 6564248011\}$. It follows that $\delta_{\mathsf{E}_{14}} = 4$ and $\lambda^{\pm}_{\mathsf{E}_{14}} = \delta_{\mathsf{E}_{14}} + \rho^{\pm} = 5$.

5.2.2. $D = 14$. We finish with an example where $\lambda^+ \neq \lambda^-$. Take $D = 14$, so that the CM member for $t = 0$ is $\mathsf{A} = 28224dj1$, given by $y^2 = x^2 + 224$. Its Iwasawa invariants are $\mu^{\pm}_{\mathsf{A}} = 0$, and $\lambda^{+}_{\mathsf{A}} = 3, \lambda^{-}_{\mathsf{A}} = 1$. The conductor of A is $28224 = 2^6 \cdot 3^2 \cdot 7^2$ and we compute as above that $\delta_{\mathsf{A}} = 0$, so $\rho^{+}_{\mathsf{A}} = \rho^{+} = 3, \rho^{-}_{\mathsf{A}} = \rho^{-} = 1$. As observed in Remark 4.15, all members E_t in this family satisfy $\lambda^{+}_{\mathsf{E}} - \lambda^{-}_{\mathsf{E}} = 2$, together with $\mu^{\pm} = 0$. Again, the conductors grow very fast with t and we could not find any curve in the family for which data are available on [LMF13]. As examples, we consider the curves for $t = 6$ and $t = 8$. The first has $S^{\mathrm{bad}}_{\mathsf{E}_6} = \{2, 3, 7, 22621, 92081500261\}$ and there are no $\mathbb{Q}_\ell$-rational 5-torsion points at $\ell \in S^{\mathrm{bad}}_{\mathsf{E}_6}$ except for $\ell = 92081500261$, where $\dim_{\mathbb{F}_5}\big(\mathsf{E}_6(\mathbb{Q}_\ell)_5\big) = 2$. Since $g_{92081500261} = 1$, we find $\delta_{\mathsf{E}_6} = 2$ and

$$\lambda^{+}_{\mathsf{E}_6} = 5 \qquad \text{and} \qquad \lambda^{-}_{\mathsf{E}_6} = 3.$$

Finally, we consider the curve for $t = 8$, which has no $\mathbb{Q}_\ell$-rational 5-torsion point at any of the primes $\ell \in S^{\mathrm{bad}}_{\mathsf{E}_8} = \{2, 3, 7, 10861, 642211, 9447511\}$. It follows that $\delta_{\mathsf{E}_8} = 0$ and

$$\lambda^{+}_{\mathsf{E}_6} = 3 \qquad \text{and} \qquad \lambda^{-}_{\mathsf{E}_6} = 1.$$

References

[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

[CS05] John Coates and Ramdorai Sujatha, *Fine Selmer groups of elliptic curves over p-adic Lie extensions*, Math. Ann. **331** (2005), no. 4, 809–839.

[CS10] John Coates and Ramdorai Sujatha, *Galois cohomology of elliptic curves*, second ed., Published by Narosa Publishing House, New Delhi; for the Tata Institute of Fundamental Research, Mumbai, 2010. MR 3060733

[EPW06] Matthew Emerton, Robert Pollack, and Tom Weston, *Variation of iwasawa invariants in hida families*, Invent. Math. **163** (2006), no. 3, 523–580.

[Gre89] Ralph Greenberg, *Iwasawa theory for p-adic representations*, Algebraic number theory, Adv. Stud. Pure Math., vol. 17, Academic Press, Boston, MA, 1989, pp. 97–137. MR 1097613

[Gre11] ———, *Iwasawa theory, projective modules, and modular representations*, Mem. Amer. Math. Soc. **211** (2011), no. 992, vi+185. MR 2807791

[GV00] Ralph Greenberg and Vinayak Vatsal, *On the iwasawa invariants of elliptic curves*, Invent. Math. **142** (2000), no. 1, 17–63.

[Hac11] Yoshitaka Hachimori, *Iwasawa λ-invariants and congruence of Galois representations*, J. Ramanujan Math. Soc. **26** (2011), no. 2, 203–217. MR 2816789

[HL19] Jeffrey Hatley and Antonio Lei, *Arithmetic properties of signed selmer groups at non-ordinary primes*, Annales de l'Institut Fourier **69** (2019), no. 3, 1259–1294 (en).

[IP06] Adrian Iovita and Robert 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. MR 2270567

[Jan14] Uwe Jannsen, *A spectral sequence for Iwasawa adjoints*, Münster J. Math. **7** (2014), no. 1, 135–148. MR 3271243

[Kat04] Kazuya Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Asterisque (2004), no. 295, ix, 117–290.

[Kid18] Keenan Kidwell, *On the structure of Selmer groups of p-ordinary modular forms over $\mathbf{Z}_p$-extensions*, J. Number Theory **187** (2018), 296–331. MR 3766913

[Kim09] Byoung Du Kim, *The Iwasawa invariants of the plus/minus Selmer groups*, Asian J. Math. **13** (2009), no. 2, 181–190. MR 2559107

[Kim13] ———, *The plus/minus Selmer groups for supersingular primes*, J. Aust. Math. Soc. **95** (2013), no. 2, 189–200. MR 3142355

[Kim18] ———, *Ranks of the rational points of abelian varieties over ramified fields, and Iwasawa theory for primes with non-ordinary reduction*, J. Number Theory **183** (2018), 352–387. MR 3715241

[KO18] Takahiro Kitajima and Rei Otsuki, *On the plus and the minus selmer groups for elliptic curves at supersingular primes*, Tokyo J. Math. **41** (2018), no. 1, 273–303.

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

[LLZ10] Antonio Lei, David Loeffler, and Sarah Livia Zerbes, *Wach modules and Iwasawa theory for modular forms*, Asian J. Math. **14** (2010), no. 4, 475–528. MR 2774276

[LMF13] The LMFDB Collaboration, *The L-functions and modular forms database*, http://www.lmfdb.org, 2013, [Online; accessed November 26, 2019].

[LS18] Meng Fai Lim and Ramdorai Sujatha, *On the structure of fine Selmer groups and Selmer groups of CM elliptic curves*, in preparation, 2018.

[Maz72] Barry Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, second ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, New York, 2008.

[Pol03] Robert Pollack, *On the p-adic l-function of a modular form at a supersingular prime*, Duke Math. J. **118** (2003), no. 3, 523–558.

[PR90] Bernadette Perrin-Riou, *Théorie d'Iwasawa p-adique locale et globale*, Invent. Math. **99** (1990), no. 2, 247–292.

[PR92] ———, *Théorie d'iwasawa et hauteurs p-adiques*, Invent. Math. **109** (1992), no. 1, 137–185.

[PR95] Bernadette Perrin-Riou, *Fonctions L p-adiques des représentations p-adiques*, Astérisque (1995), no. 229, 198. MR 1327803

[Ray74] Michel Raynaud, *Schémas en groupes de type $(p,\dots,p)$*, Bull. Soc. Math. France **102** (1974), 241–280. MR 419467

[RS95] K. Rubin and A. Silverberg, *Families of elliptic curves with constant mod p representations*, Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993), Ser. Number Theory, I, Int. Press, Cambridge, MA, 1995, pp. 148–161. MR 1363500

[Sch85] Peter Schneider, *p-adic height pairings. ii*, Invent. Math. **79** (1985), no. 2, 329–374.

[Ser94] Jean-Pierre Serre, *Cohomologie galoisienne*, fifth ed., Lecture Notes in Mathematics, vol. 5, Springer-Verlag, Berlin, 1994. MR 1324577

[Sil94] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. MR 1312368

[Spr12] Florian E. Ito Sprung, *Iwasawa theory for elliptic curves at supersingular primes: a pair of main conjectures*, J. Number Theory **132** (2012), no. 7, 1483–1506. MR 2903167

[Suj10] R. Sujatha, *Elliptic curves and Iwasawa's $\mu = 0$ conjecture*, Quadratic forms, linear algebraic groups, and cohomology, Dev. Math., vol. 18, Springer, New York, 2010, pp. 125–135. MR 2648723

Univ Lyon, Université Jean Monnet Saint-Étienne, CNRS UMR 5208, Institut Camille Jordan, F-42023 Saint-Étienne, France
E-mail address: filippo.nuccio@univ.st-etienne.fr

Department of Mathematics, University of British Columbia, Vancouver, BC V6T 1Z2, Canada
E-mail address: sujatha@math.ubc.ca