Rend. Sem. Mat. Univ. Padova 149 (2023), 83–129
DOI 10.4171/RSMUP/111

Residual supersingular Iwasawa theory and signed Iwasawa invariants

Filippo A. E. Nuccio Mortarino Majno di Capriglio (*) –
Sujatha Ramdorai (**)

Abstract – For an odd prime p and a supersingular elliptic curve over a number field, this article introduces a multi-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.

Mathematics Subject Classification (2020) – Primary 11R23; Secondary 11G05.

Keywords – Iwasawa theory, elliptic curves, supersingular reduction, signed Selmer groups.

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. Iwasawa theory for ordinary elliptic curves, and more generally for ordinary Galois representations, was initiated by Mazur in [25] and Greenberg in [5]. The corresponding theory for supersingular elliptic curves is subtler and was already begun by Perrin-Riou in [27]. In the last couple of decades, supersingular Iwasawa theory has gained considerable momentum (see [11, 16–20, 30, 36] and references therein).

(*) *Indirizzo dell'A.*: Université Jean Monnet Saint-Étienne, CNRS, Institut Camille Jordan, UMR 5208, 42023 Saint-Étienne, France; filippo.nuccio@univ-st-etienne.fr

(**) *Indirizzo dell'A.*: Department of Mathematics, University of British Columbia, Vancouver, BC V6T 1Z2, Canada; sujatha@math.ubc.ca

Greenberg and Vatsal [8] investigated 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 [4], and to more general base fields and $\mathbb{Z}_p$-extensions by, among others, Hachimori in [9] and by Kidwell in [14]. A crucial input in the study of p^∞-Selmer groups in the ordinary case is a deep result of Kato (see [13]) 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 over the Iwasawa algebra. Kobayashi defined the *signed* p^∞-Selmer group in [19], 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* Iwasawa invariants $\lambda^\pm, \mu^\pm$. Results analogous to those of Greenberg–Vatsal for these signed invariants were proved by Kim in [15], again making use of the non-primitive Selmer groups. The study of signed Selmer groups for higher weight modular forms has been initiated by Lei, Loeffler and Zerbes in [20] through the theory of Wach modules, and extensions of Greenberg–Vatsal results in this setting can be found in [10] by Hatley and Lei. The definition of the signed Selmer groups has been extended to a broader class of number fields in [11, 16, 18]. 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 [15], largely because we set up a framework for multi-signed Selmer groups.

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 E_{p^∞}. In particular, we introduce a new Selmer group, attached to the Galois representation E_p of p-torsion points of E, which we call multi-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 multisigned residual Selmer group contains the residual analogue of the fine Selmer group as defined by Coates and the second author in [2]. They 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 [7, 37]) and its formulation is independent of the reduction type at p of the elliptic curve. Working directly with the multi-signed residual Selmer group provides a conceptual framework to explore the comparison of Iwasawa 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 Theorems 4.13 and 4.15. Under certain hypotheses Hyp 1 and Hyp $2_\ddagger$, and assuming Conjecture A, Theorem 4.13 provides a criterion for the μ-invariant of the multi-signed p^∞-Selmer group to vanish, purely in terms of the multi-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 4.13, our second theorem provides a criterion for the μ-invariant of the signed p^∞-Selmer group to vanish, purely in terms of the multi-signed residual Selmer group. In the following, denote by d the number of primes in L of supersingular reduction for an elliptic curve E and let $\ddagger \in \{+,-\}^d$ be a vector of signs, in other words $\ddagger$ is a d-tuple with entries either $+$ or $-$. Denote by $\mathrm{X}^\ddagger((\mathsf{E})_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$ the dual multi-signed p^∞- Selmer groups, as defined in Definition 3.6 (see also [18, Definition 2.1]):

Theorem 4.15. *Let $\mathsf{E}_1, \mathsf{E}_2$ be two elliptic curves defined over L, satisfying Hypothesis Hyp 1 and such that the residual Galois representations $(\mathsf{E}_1)_p$ and $(\mathsf{E}_2)_p$ are isomorphic. Then, the sets S_1^{ss} and S_2^{ss} of primes of supersingular reduction for E_1 and E_2 coincide. Given a vector $\ddagger \in \{+,-\}^d$, assume that both curves satisfy Hyp $2_\ddagger$ and let $\mu^\ddagger_{\mathsf{E}_j}$ be the Iwasawa μ-invariants of $\mathrm{X}^\ddagger((\mathsf{E}_j)_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$, for $j = 1, 2$. Then*

$$\mu^\ddagger_{\mathsf{E}_1} = 0 \Longleftrightarrow \mu^\ddagger_{\mathsf{E}_2} = 0.$$

In the ordinary case, using the non-primitive Selmer groups, Greenberg and Vatsal (see [8, Theorem 1.5]) compare the λ-invariants. When the μ-invariants vanish, our approach also enables such a comparison, without the use of the imprimitive Selmer groups. These results should be compared with those by Kim (see [15, Corollary 2.13]) and Hatley–Lei (see [10, Theorem 4.6]). We need the additional assumption that the Pontryagin dual of the usual Selmer group (and hence, also of the multi-signed one by Corollary 4.18) contains no non-zero finite $\Lambda(\Gamma)$-submodule, and this is known to be true in many cases.

THEOREM 4.20. *Let $\mathsf{E}_1, \mathsf{E}_2$ be two elliptic curves defined over* L*, satisfying the hypotheses of Theorem* 4.15*. Assume that their Iwasawa $\mu^{\ddagger}$-invariants vanish and suppose further that the Pontryagin duals* $\mathrm{X}((\mathsf{E}_j)_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$ *of the usual Selmer groups do not have any non-zero finite* $\Lambda(\Gamma)$*-submodule. Then,*

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

where δ_{E_j} is as in Definition 4.5 *and $\rho^{\ddagger} := \rho^{\ddagger}_{\mathsf{E}_1} = \rho^{\ddagger}_{\mathsf{E}_2}$ is as in* (4.28).

The first term $\rho^{\ddagger}$ in the above statement depends only on the residual representation and is independent of the curve. 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: in particular, it is independent of the vector $\ddagger$. The reader is referred to the main body of the paper for the precise definitions of these numerical invariants.

Our methods also show that the difference $\lambda^{\ddagger} - \lambda^{-\ddagger}$ depends only on the residual representation, a fact which was already observed by Kim in [15, Remark 3.3] for $\mathrm{L} = \mathbb{Q}$. Propositions 3.8 and 3.9 are the key technical tools needed to show that the definition of the multi-signed residual Selmer group depends only on the residual representation. They compare the reduction type at places above p of two residually isomorphic elliptic curves at primes above p, and are of independent interest. While the first result relies on Honda–Tate theory and is a typical feature of supersingular reduction, the second relies upon a result by Raynaud on finite flat group schemes killed by p. We remark that some of the techniques used here were first developed in the setting of purely ordinary reduction in [22]. The extension to the generality considered in this paper was not obvious then.

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 multi-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 multi-signed Kummer maps and Selmer groups, mainly building upon [18], and we introduce the multi-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.

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, which will be referred to as Hyp 1, is assumed throughout (cf. [18, Theorem 1.3 (i)–(v)]):

Hypothesis Hyp 1. Denote by $S^{\mathrm{ss}} \subseteq S_p$ the set of primes above p where E has supersingular reduction.

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

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

(iii) All primes $\mathfrak{p}_1, \dots, \mathfrak{p}_d$ 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 $\mathfrak{p}_1, \dots, \mathfrak{p}_d$ 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 multi-signed residual Selmer group depends only on the residual Galois representation E_p (cf. Propositions 3.8 and 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 $S_p = S^{\mathrm{ss}} \sqcup S^{\mathrm{ord}}$, 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 $\mathscr{L}_{n,i}$ 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 n-th layer of the cyclotomic extension of $\mathscr{L}_0 \cong \mathbb{Q}_p$. In particular, $\mathscr{L}_{\mathrm{cyc},i} \cong (\mathbb{Q}^{\mathrm{cyc}})_{\mathfrak{p}_{\mathrm{cyc},i}}$. We also need to consider the fields obtained by adjoining p-power order roots of unity to $\mathscr{L}_{0,i} = \mathscr{L}_0$. Set $\Bbbk_n = \mathscr{L}_0(\zeta_{p^{n+1}})$, 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 $\mathrm{Gal}(\Bbbk_0/\mathscr{L}_0)$ is denoted by Δ. It is isomorphic to $\mathrm{Gal}(\Bbbk_n/\mathscr{L}_n)$ for all $n \geq 0$, and we tacitly identify these groups throughout.

Let $S = S_p \sqcup S^{\mathrm{bad}}$ 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 by 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' that lie 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 $\mathfrak{G}^S_n$, $G_{\Bbbk_n}$ and $G_{\mathrm{L}_{n,v}}$; in case $v = \mathfrak{p}_i$, this will be denoted by $G_{\mathscr{L}_i}$. 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 by E_{p^t}, and more generally M_{p^t} will denote the submodule of a Galois module M 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, $\mathscr{E}$ is the formal group of E over $\mathbb{Z}_p = \mathcal{O}_{\mathscr{L}_0}$. As discussed in [19, Corollary 8.5] and [18, §3.1], there is a $\mathbb{Z}_p$-isomorphism $\mathscr{E} \cong \mathscr{F}_{\mathrm{ss}}$ between the formal group of $\mathsf{E}/\mathbb{Z}_p$ and the supersingular formal group $\mathscr{F}_{\mathrm{ss}}$ whose logarithm is of Honda type $t^2 + p$ (the group $\mathscr{F}_{\mathrm{ss}}$ is denoted by $\mathscr{G}$ in [18, §3.1]: observe that in our setting the automorphism φ in [18, §3.1] 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 of *local* Mordell–Weil and formal groups, mainly taken from [18], which in turn relies on [19]. 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,*

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

Proof. See [18, Proposition 3.1]. ■

Following the pivotal works by Perrin-Riou [27] and Kobayashi [19], we now define plus/minus subgroups of the local points, as follows.

Definition 3.2 ([18, Definitions 2.1 and 3.13]). With notations as above we denote, for every $n \geq 1$,

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

Similarly, we set

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

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

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

Lemma 3.3 ([18, 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*

$$0 \to \mathcal{E}^\pm(\mathfrak{m}_n) \to \mathsf{E}^\pm(\mathbb{k}_n) \to \mathcal{D}^\pm_n \to 0, \tag{3.1}$$

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

$$0 \to \mathcal{E}(\mathfrak{m}_K) \to \mathsf{E}(K) \to D \to 0, \tag{3.2}$$

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

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{E}(\mathfrak{m}_m) \arrow[r] \arrow[d, hook] & \mathsf{E}(\mathbb{k}_m) \arrow[r] \arrow[d, hook] & \widetilde{\mathsf{E}}(\mathbb{F}_p) \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & \mathcal{E}(\mathfrak{m}_{m+1}) \arrow[r] & \mathsf{E}(\mathbb{k}_{m+1}) \arrow[r] & \widetilde{\mathsf{E}}(\mathbb{F}_p) \arrow[r] & 0
\end{tikzcd}$$

which induces, by the snake lemma, an isomorphism

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

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

$$\begin{tikzcd}
0 \arrow[r] & \ker \widehat{\mathrm{Tr}^n_{m+1}} \arrow[r] \arrow[d, hook] & \ker \overline{\mathrm{Tr}^n_{m+1}} \arrow[r] \arrow[d, hook] & \widetilde{\mathsf{E}}(\mathbb{F}_p) \arrow[d, equal] & \\
0 \arrow[r] & \mathcal{E}(\mathfrak{m}_n) \arrow[r] \arrow[d, "\widehat{\mathrm{Tr}^n_{m+1}}"] & \mathsf{E}(\mathbb{k}_n) \arrow[r] \arrow[d, "\overline{\mathrm{Tr}^n_{m+1}}"] & \widetilde{\mathsf{E}}(\mathbb{F}_p) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathcal{E}(\mathfrak{m}_{m+1})/\mathcal{E}(\mathfrak{m}_m) \arrow[r, "\cong"] & \mathsf{E}(\mathbb{k}_{m+1})/\mathsf{E}(\mathbb{k}_m) \arrow[r] & 0 \arrow[r] & 0,
\end{tikzcd}$$

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

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

and therefore an exact sequence

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

for some $\mathcal{D}_n^{\pm} \subseteq \widetilde{\mathsf{E}}(\mathbb{F}_p)$. 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

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

we obtain

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

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

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

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

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

Lemma 3.4 ([19, 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

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

Similarly, there are injections

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

Proof. Let us first show that

$$\mathsf{E}^{\pm}(\Bbbk_n)/p^t\mathsf{E}^{\pm}(\Bbbk_n) \hookrightarrow \mathsf{E}(\Bbbk_n)/p^t\mathsf{E}(\Bbbk_n) \tag{3.3}$$

is injective. An element in

$$\ker\big(\mathsf{E}^{\pm}(\Bbbk_n)/p^t\mathsf{E}^{\pm}(\Bbbk_n) \to \mathsf{E}(\Bbbk_n)/p^t\mathsf{E}(\Bbbk_n)\big)$$

is represented by a point $P \in \mathsf{E}^{\pm}(\Bbbk_n)$ such that $P = p^t Q$ 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, $\mathrm{Tr}^n_{m+1}(P) =$

$p^t \operatorname{Tr}^n_{m+1}(Q)$, hence for all $\sigma \in \operatorname{Gal}(\Bbbk_{m+1}/\Bbbk_m)$ we have

$$p^t({}^{\sigma}\operatorname{Tr}^n_{m+1}(Q) - \operatorname{Tr}^n_{m+1}(Q)) = 0.$$

Thus $\operatorname{Tr}^n_{m+1}(Q) \in \mathsf{E}(\Bbbk_m)$ thanks to Proposition 3.1, which implies $Q \in \mathsf{E}^{\pm}(\Bbbk_n)$ and the arrow in (3.3) 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

$$\begin{aligned} 0 \to \mathsf{E}^*(\mathscr{L}_n) \xrightarrow{\cdot p^t} \mathsf{E}^*(\mathscr{L}_n) \to \mathrm{H}^0\big(\Delta, \mathsf{E}^*(\Bbbk_n)/p^t\mathsf{E}^*(\Bbbk_n)\big) \\ \to \mathrm{H}^1(\Delta, \mathsf{E}^*(\mathscr{L}_n))_{p^t} \to 0. \end{aligned}$$

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

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

Taking Δ-invariants of the injections in (3.3) establishes the first part of the lemma. The second part 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

$$\begin{aligned} 0 \to \mathsf{E}^{\pm}(\mathscr{L}_n)/p^t\mathsf{E}^{\pm}(\mathscr{L}_n) \xrightarrow{\kappa^{\pm,p^t}_{\mathscr{L}_n}} \mathrm{H}^1(G_{\mathscr{L}_n}, \mathsf{E}_{p^t}) \\ \to \mathrm{H}^1(G_{\mathscr{L}_n}, \mathsf{E}_{p^t})/\operatorname{Im}\kappa^{\pm,p^t}_{\mathscr{L}_n} \to 0 \end{aligned} \tag{3.4}$$

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

$$\begin{aligned} 0 \to \mathcal{E}^{\pm}(\mathscr{L}_n)/p^t\mathcal{E}^{\pm}(\mathfrak{m}^{\Delta}_n) \xrightarrow{\kappa^{\pm,p^t}_{\mathscr{L}_n}} \mathrm{H}^1(G_{\mathscr{L}_n}, \mathcal{E}_{p^t}) \\ \to \mathrm{H}^1(G_{\mathscr{L}_n}, \mathcal{E}_{p^t})/\kappa^{\pm,p^t}_{\mathscr{L}_n}(\mathcal{E}^{\pm}(\mathfrak{m}^{\Delta}_n)) \to 0. \end{aligned} \tag{3.5}$$

Remark 3.5. It is perhaps interesting to stress that the signed Kummer map defined in (3.4) *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 multi-signed Selmer groups*

We use the notation introduced in Notation 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 [3, Chapters 1 and 2]. They are defined as

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

where we split the sum into two parts, one over primes in S^{ss} and the other over primes which are not supersingular. This is done mainly 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 [27] and Kobayashi [19] is of particular interest. The multi-signed residual 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 [18] by Kitajima–Otsuki. Fix a vector of signs $\ddagger \in \{+,-\}^d$ throughout. For every local place $\mathfrak{p}_i$ with $1 \le i \le d$, to ease notation write $\kappa^{\pm,p^t}_{\mathscr{L}_{n,i}}$ to denote either $\kappa^{+,p^t}_{\mathscr{L}_{n,i}}$ or $\kappa^{-,p^t}_{\mathscr{L}_{n,i}}$, according to the i-th component $\ddagger_i$ of the vector of signs.

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

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

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 multi-signed Selmer group* is defined as

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

As the notation suggests, these multi-signed residual 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 4.4, which relies on Propositions 3.8 and 3.9 below.

We start with the following technical lemma:

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

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

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

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

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

(i) *If $G \in \{\mathcal{G}_n^S, G_{\mathscr{L}_n}\}$, 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

$$0 \to \mathsf{E}_p \to \mathsf{E}_{p^\infty} \to \mathsf{E}_{p^\infty} \to 0 \tag{3.6}$$

gives an exact sequence

$$\begin{aligned} 0 \to \ker \psi_n &= \mathrm{H}^0(G, \mathsf{E}_{p^\infty})/p\,\mathrm{H}^0(G, \mathsf{E}_{p^\infty}) \\ &\to \mathrm{H}^1(G, \mathsf{E}_p) \xrightarrow{\psi_n} \mathrm{H}^1(G, \mathsf{E}_{p^\infty})_p \to 0. \end{aligned} \tag{3.7}$$

When $G \in \{\mathcal{G}_n^S, G_{\mathscr{L}_n}\}$, the first term in (3.7) 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 (3.7) 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 (3.6) by

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

to obtain an exact sequence

$$\begin{aligned}(3.8)\qquad 0 &\to \ker\widetilde{\psi_n} = \mathrm{H}^0(G,\widetilde{\mathsf{E}}_{p^\infty})/p\,\mathrm{H}^0(G,\widetilde{\mathsf{E}}_{p^\infty}) \\ &\to \mathrm{H}^1(G,\widetilde{\mathsf{E}}_p) \xrightarrow{\widetilde{\psi_n}} \mathrm{H}^1(G,\widetilde{\mathsf{E}}_{p^\infty})_p \to 0.\end{aligned}$$

The first term in (3.8) is an $\mathbb{F}_p$-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 prove that the local conditions in the definition of the multi-signed residual 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 (3.2) 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 (3.1) shows that the images of the signed Kummer maps $\kappa^{\pm,p^\infty}_{\mathcal{L}_{n,i}}(\mathsf{E}^\pm(\mathcal{L}_{i,n}))$ and $\kappa^{\pm,p^\infty}_{\mathcal{L}_{n,i}}(\mathcal{E}^\pm(\mathfrak{m}_n^\Delta))$ are isomorphic. It is straightforward to check that these isomorphisms are compatible, and in turn induce isomorphisms

$$(3.9)\qquad \mathrm{H}^1(\mathcal{L}_{n,i},\mathsf{E}_{p^\infty})/\operatorname{Im}(\kappa^{\pm,p^\infty}_{\mathcal{L}_{n,i}}) \cong \mathrm{H}^1(\mathcal{L}_{n,i},\mathcal{E}_{p^\infty})/\kappa^{\pm,p^\infty}_{\mathcal{L}_{n,i}}(\mathcal{E}^\pm(\mathfrak{m}_n^\Delta)).$$

As discussed in [19, Corollary 8.5] and [18, §3.1], there is a $\mathcal{O}_{\mathcal{L}_0} = \mathbb{Z}_p$-isomorphism

$$(3.10)\qquad \log_{\mathcal{F}_{\mathrm{ss}}} \circ \exp_{\mathcal{E}} \colon \mathcal{E} \xrightarrow{\cong} \mathcal{F}_{\mathrm{ss}},$$

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 $\mathcal{F}^\pm_{\mathrm{ss}}(\mathfrak{m}_n) \subseteq \mathcal{F}_{\mathrm{ss}}(\mathfrak{m}_n)$ 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

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

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 (3.5) for $\mathcal{F}_{\mathrm{ss}}$ and $\mathcal{F}^\pm_{\mathrm{ss}}$ instead of $\mathcal{E}$. Combining (3.9) with (3.10) gives

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

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

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*

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

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 [19, 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*

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

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 $\mathcal{E}_j$ the Néron model of E_j (see [35, 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 $(\mathcal{E}_j)_p$ is isomorphic to $(\mathsf{E}_j)_p$ (resp. to $(\widetilde{\mathsf{E}}_j)_p$), for $j = 1, 2$. Applying [31, 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

$$(\mathcal{E}_1)_p \cong (\mathcal{E}_2)_p \tag{3.11}$$

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

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

as finite flat $\mathbb{F}_\mathfrak{p}$-group schemes. This shows that the elliptic curve $\widetilde{\mathsf{E}}_2$ 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 [31, Corollaire 3.3.6] and the isomorphism (3.11) holds again, where now $\mathcal{E}_j$ denotes the Néron model of $\mathsf{E}_j/\mathrm{L}_\pi$. Taking closed fibres, we obtain

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

finishing the proof of the proposition. ∎

4. Iwasawa theory for the signed Selmer groups

4.1 – *Cyclotomic multi-signed residual Selmer groups*

In this section, we focus on the Iwasawa theory for the multi-signed residual Selmer group introduced in Definition 3.6. Retaining the notation introduced in Notation 2.2, set $\mathcal{G}_{\mathrm{cyc}}^S = \mathrm{Gal}(\mathrm{L}^S/\mathrm{L}_{\mathrm{cyc}})$. 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 $M^\wedge$. 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 $M^\wedge$ 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

$$\mathrm{corank}_{\Lambda(\Gamma)} M \le \mathrm{corank}_{\Omega(\Gamma)} M_p$$

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 $\mathrm{H}^1(\mathcal{L}_n, \mathsf{E}_p)$

$$\mathrm{Im}(\kappa_{\mathcal{L}_n}^{\pm,p}) \hookrightarrow \mathrm{Im}(\kappa_{\mathcal{L}_n}^{p}),$$

which will play a role in defining the Selmer groups. We display the subscript $1 \le i \le d$ to keep track of the local Galois cohomology groups, writing

$$\mathrm{Im}(\kappa_{\mathcal{L}_{n,i}}^{\pm,p}) \hookrightarrow \mathrm{Im}(\kappa_{\mathcal{L}_{n,i}}^{p}) \subseteq \mathrm{H}^1(\mathcal{L}_{n,i}, \mathsf{E}_p).$$

By taking the direct limit of the exact sequence (3.4) over the subextensions inside $\mathcal{L}_{\mathrm{cyc}}/\mathcal{L}$ gives the exact sequences, for all $1 \le t \le \infty$,

$$\begin{aligned} 0 \to \mathsf{E}^{\pm}(\mathcal{L}_{\mathrm{cyc}})/p^t\mathsf{E}^{\pm}(\mathcal{L}_{\mathrm{cyc}}) &\xrightarrow{\kappa^{\pm,p^t}_{\mathcal{L}_{\mathrm{cyc}}}} \mathrm{H}^1(\mathcal{L}_{\mathrm{cyc}}, \mathsf{E}_{p^t}) \\ &\to \mathrm{H}^1(\mathcal{L}_{\mathrm{cyc}}, \mathsf{E})/\operatorname{Im}(\kappa^{\pm,p^t}_{\mathcal{L}_{\mathrm{cyc},i}}) \to 0. \end{aligned}$$

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 $G \in \{\mathcal{G}^S_{\mathrm{cyc}}, G_{\mathcal{L}_{\mathrm{cyc}}}, G_{\mathrm{L}_{\mathrm{cyc},w}}\}$ 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 $G \in \{\mathcal{G}^S_{\mathrm{cyc}}, G_{\mathcal{L}_{\mathrm{cyc}}}\}$, then the map $\psi_{G,\mathrm{cyc}}$ is an isomorphism*

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

(b) *If $G = G_{\mathrm{L}_{\mathrm{cyc},w}}$ for some $w \mid \mathfrak{l} \in S^{\mathrm{bad}}$, then 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*

$$\dim_{\mathbb{F}_p}(\ker \psi_{w,\mathrm{cyc}}) = \dim_{\mathbb{F}_p} \mathsf{E}(\mathrm{L}_{\mathrm{cyc},w})_p \le 2,$$

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 $w \mid \pi \in S^{\mathrm{ord}}$, then $\widetilde{\psi_{w,\mathrm{cyc}}}$ extends to a surjective map*

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

whose kernel is finite, of dimension

$$\dim_{\mathbb{F}_p}(\ker \widetilde{\psi_{w,\mathrm{cyc}}}) = \dim_{\mathbb{F}_p} \widetilde{\mathsf{E}}(\mathbb{F}_w)_p \le 1,$$

and

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

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

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

giving

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

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 [1], in particular Theorem 2.13, noting that the cyclotomic $\mathbb{Z}_p$-extension is deeply ramified). Consider the exact sequence

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

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

$$0 \to \mathrm{H}^1(G, \mathsf{E}_{p^\infty})/\operatorname{Im}(\mathrm{H}^1(G, \mathcal{A}_{p^\infty})) \to \mathrm{H}^1(G, \widetilde{\mathsf{E}}_{p^\infty}) \to \mathrm{H}^2(G, \mathcal{A}_{p^\infty}). \tag{4.1}$$

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 the proof of [34, Chapitre II, §3.3, Proposition 9]).

Thus we obtain from (4.1) 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 [1, Proposition 4.3 and diagram (4.8)], we further have

$$\begin{aligned} \mathrm{H}^1(G, \mathsf{E})_{p^\infty} &= \mathrm{H}^1(G, \mathsf{E}_{p^\infty})/\operatorname{Im}(\kappa^{\pm,p^\infty}_{\mathrm{L}_{\mathrm{cyc},w}}) \\ &= \mathrm{H}^1(G, \mathsf{E}_{p^\infty})/\operatorname{Im}(\mathrm{H}^1(G, \mathcal{A}_{p^\infty})) \cong \mathrm{H}^1(G, \widetilde{\mathsf{E}}_{p^\infty}). \end{aligned} \tag{4.2}$$

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

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

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 than 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, $\mathsf{E}^{\pm}(\mathcal{L}_{\mathrm{cyc}})_p = \mathcal{E}^{\pm}(\mathfrak{m}_\infty^\Delta)_p$ 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

$\mathsf{E}^{\pm}(\mathscr{L}_{\rm cyc})_p = 0$. In particular, $\mathsf{E}^{\pm}(\mathscr{L}_{\rm cyc})$ is a direct limit of free $\mathbb{Z}_p$-modules of finite rank, hence $\mathrm{Tor}^1_{\mathbb{Z}_p}(\mathsf{E}^{\pm}(\mathscr{L}_{\rm cyc}), \mathbb{Q}_p/\mathbb{Z}_p) = 0$. Consider the exact sequence

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

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

$$\mathsf{E}^{\pm}(\mathscr{L}_{\rm cyc}) \otimes \mathbb{Z}/p \cong (\mathsf{E}^{\pm}(\mathscr{L}_{\rm cyc}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)_p. \tag{4.3}$$

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

$$\tag{4.4} \begin{tikzcd}
0 \arrow[d] & & 0 \arrow[d] \\
\mathsf{E}^{\pm}(\mathscr{L}_{\rm cyc}) \otimes \mathbb{Z}/p \arrow[rr, "\cong"] \arrow[d, "\kappa^{\pm,p}_{\mathscr{L}_{\rm cyc}}"] & & (\mathsf{E}^{\pm}(\mathscr{L}_{\rm cyc}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)_p \arrow[d, "\kappa^{\pm,p^\infty}_{\mathscr{L}_{\rm cyc}}"] \\
\mathrm{H}^1(\mathscr{L}_{\rm cyc}, \mathsf{E}_p) \arrow[rr, "\cong", "\psi_{\mathcal{G}^S_{\rm cyc}}"'] \arrow[d] & & \mathrm{H}^1(\mathscr{L}_{\rm cyc}, \mathsf{E}_{p^\infty})_p \arrow[d, "\alpha"] \\
\mathrm{H}^1(\mathscr{L}_{\rm cyc}, \mathsf{E}_p)/\operatorname{Im}\kappa^{\pm,p}_{\mathscr{L}_{\rm cyc}} \arrow[rr, "\psi^{\pm}_{\mathfrak{p},\rm cyc}"] \arrow[d] & & (\mathrm{H}^1(\mathscr{L}_{\rm cyc}, \mathsf{E}_{p^\infty})/\operatorname{Im}\kappa^{\pm,p^\infty}_{\mathscr{L}_{\rm cyc}})_p \\
0 & &
\end{tikzcd}$$

The first horizontal arrow is an isomorphism in light of (4.3), and the second horizontal arrow is an isomorphism thanks to (a). The snake lemma implies that $\psi^{\pm}_{\mathfrak{p},\rm cyc}$ is injective and $\operatorname{coker}(\psi^{\pm}_{\mathfrak{p},\rm cyc}) = \operatorname{coker}(\alpha)$. To show that α is surjective observe that the second column in (4.4) is the beginning of the $\mathrm{Tor}^i_{\mathbb{Z}_p}(-, \mathbb{Z}/p)$-sequence of the tautological exact sequence

$$\begin{aligned} 0 \to \mathsf{E}^{\pm}(\mathscr{L}_{\rm cyc}) \otimes \mathbb{Q}_p/\mathbb{Z}_p &\xrightarrow{\kappa^{\pm,p^\infty}_{\mathscr{L}_{\rm cyc}}} \mathrm{H}^1(\mathscr{L}_{\rm cyc}, \mathsf{E}_{p^\infty}) \\ &\to \mathrm{H}^1(\mathscr{L}_{\rm cyc}, \mathsf{E}_{p^\infty})/\operatorname{Im}\kappa^{\pm,p^\infty}_{\mathscr{L}_{\rm cyc}} \to 0 \end{aligned}$$

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

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

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

Let us now pass to Selmer groups. We refer to [3, 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 multi-signed residual Selmer group $\mathscr{R}^{\ddagger}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})$ is defined as

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

and the usual multi-signed Selmer group is defined as

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

The groups $\mathscr{R}^{\ddagger}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})$ are discrete $\Omega(\Gamma)$-modules, whose Pontryagin duals are compact, finitely generated over $\Omega(\Gamma)$. Similarly, the groups $\mathrm{Sel}^{\ddagger}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$ 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

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

Remark 4.3. It is not *a priori* obvious that the groups ${}^{\pm}\widetilde{K}_v(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})$ depend only upon the isomorphism class of E_p, as the notation would suggest. Indeed, for a supersingular prime $\mathfrak{p} \in S^{\mathrm{ss}}$, the definition of the map $\kappa^{\pm,p}_{\mathscr{L}_{\mathrm{cyc},i}}$ is given in terms of the full torsion module E_{p^∞}. Below, we will see that in fact the groups ${}^{\pm}\widetilde{K}_v(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})$ only depend upon E_p.

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

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

where, as in Proposition 4.1, we set

$$\kappa^{\pm,p^\infty}_{\mathrm{L}_{w,\mathrm{cyc}}} = \kappa^{p^\infty}_{\mathrm{L}_{w,\mathrm{cyc}}} \quad \text{for all } w \mid v \in S \setminus S^{\mathrm{ss}}.$$

As in Definition 3.6, when a vector $\ddagger \in \{+,-\}^d$ is fixed, we simply use ${}^{\pm}\widetilde{K}_v(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})$ (resp. $J_v^{\pm}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$) to denote the module ${}^{+}\widetilde{K}_v(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})$ or ${}^{-}\widetilde{K}_v(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})$ (resp. the module $J_v^{+}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$ or $J_v^{-}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$) according to the i-th component $\ddagger_i \in \{+,-\}$. Then the multi-signed residual Selmer group and the usual multi-signed

Selmer group sit in the following exact sequences:

$$0 \to \mathcal{R}^{\ddagger}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) \to \mathrm{H}^1(\mathcal{G}^S_{\mathrm{cyc}}, \mathsf{E}_p) \xrightarrow{\xi^{\ddagger}_p} \bigoplus_{v\in S} {}^{\pm}\widetilde{K}_v(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) \tag{4.5}$$

resp.

$$0 \to \mathrm{Sel}^{\ddagger}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}}) \to \mathrm{H}^1(\mathcal{G}^S_{\mathrm{cyc}}, \mathsf{E}_{p^\infty}) \xrightarrow{\xi^{\ddagger}_{p^\infty}} \bigoplus_{v\in S} J^{\pm}_v(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}}). \tag{4.6}$$

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 (ii) at all primes $\pi \in S^{\mathrm{ord}}$ by taking the 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 multi-signed residual Selmer group. We record this as follows.

Corollary 4.4. *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, the sets S^{ss}_1 and S^{ss}_2 of primes of supersingular reduction for E_1 and E_2 coincide and for every vector of signs $\ddagger \in \{+,-\}^d$,*

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

Proof. The equality $S^{\mathrm{ss}}_1 = S^{\mathrm{ss}}_2$ is a consequence of Proposition 3.9 (i), and the isomorphism of the corresponding multi-signed residual Selmer groups follows from the above discussion. ■

Kim considers in [15] the primitive and non-primitive Selmer groups along the lines of [8]. Corollary 4.6 below is the analogue of [15, Proposition 2.10] for the multi-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 $\mathbb{Z}_p$-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 4.5. 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 4.6. *There are injections*

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

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

$$\operatorname{corank}_{\Omega(\Gamma)} \mathscr{R}^{\ddagger}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) = \operatorname{corank}_{\Omega(\Gamma)} \mathrm{Sel}^{\ddagger}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})_p.$$

Moreover, when $\xi_p^{\ddagger}$ *is surjective,* $\dim_{\mathbb{F}_p} \operatorname{coker}(\varphi^{\ddagger}) = \delta_{\mathsf{E}}$, *independently of the vector* $\ddagger$.

Proof. Consider the commutative diagram
(4.7)

$$\begin{tikzcd}
0 \arrow[r] & \mathscr{R}^{\ddagger}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) \arrow[r] \arrow[d, "\varphi^{\ddagger}"] & \mathrm{H}^1(\mathcal{G}^S_{\mathrm{cyc}}, \mathsf{E}_p) \arrow[r, "\xi_p^{\ddagger}"] \arrow[d, "\wr\|"] & \bigoplus_{v\in S} {}^{\pm}\widetilde{K}_v(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) \arrow[d, "\oplus\varphi_v^{\pm}"] \\
0 \arrow[r] & \mathrm{Sel}^{\ddagger}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})_p \arrow[r] & \mathrm{H}^1(\mathcal{G}^S_{\mathrm{cyc}}, \mathsf{E}_{p^\infty})_p \arrow[r, "\xi_{p^\infty}^{\ddagger}"] & \bigoplus_{v\in S} (J_v^{\pm}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}}))_p.
\end{tikzcd}$$

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

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

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

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

Indeed, the first equality

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

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

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

follows from (4.2). Similarly, the fact that $\psi^{\pm}_{\mathfrak{p},\mathrm{cyc}}$ takes values in

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

and is an isomorphism follows from Proposition 4.1 (d).

By applying the snake lemma to (4.7), we see that

$$\operatorname{coker}(\varphi^{\ddagger}) \subseteq \bigoplus_{\mathfrak{q}\,|\,\mathfrak{l}\in\mathcal{S}^{\mathrm{bad}}} \ker(\psi_{\mathfrak{q},\mathrm{cyc}}) \oplus \bigoplus_{w\,|\,\pi\in\mathcal{S}^{\mathrm{ord}}} \ker(\widetilde{\psi_{w,\mathrm{cyc}}}) \tag{4.8}$$

and the inclusion in (4.8) is an equality when $\xi_p^{\ddagger}$ is surjective.

It follows from (4.8) and Proposition 4.1 (b), (c) that

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

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

$$\dim_{\mathbb{F}_p} \mathsf{E}(\mathrm{L}_{\mathrm{cyc},\mathfrak{q}})_p = \mathsf{E}(\mathrm{L}^1_{\mathfrak{q}})_p \qquad \text{if } \mathfrak{q} \mid \mathfrak{l} \in \mathcal{S}^{\mathrm{bad}}, \tag{4.9}$$

$$\dim_{\mathbb{F}_p} \widetilde{\mathsf{E}}(\mathbb{F}_w)_p = \dim_{\mathbb{F}_p} \widetilde{\mathsf{E}}(\mathbb{F}_\pi)_p \qquad \text{for all } w \mid \pi \in \mathcal{S}^{\mathrm{ord}}. \tag{4.10}$$

The equality in (4.10) 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 (4.9), 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 $\mathsf{E}(\mathrm{L}_{\mathfrak{l}})_p = \mathsf{E}(\mathrm{L}^1_{\mathfrak{q}})_p = \mathsf{E}(\mathrm{L}_{\mathrm{cyc},\mathfrak{q}})_p$. 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 $\mathsf{E}(\mathrm{L}_{\mathrm{cyc},\mathfrak{q}})_p = 0 = \mathsf{E}(\mathrm{L}^1_{\mathfrak{q}})_p$. 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 $\dim_{\mathbb{F}_p} \mathsf{E}(\mathrm{L}^1_{\mathfrak{q}})_p = 2$. The assumption that $\dim_{\mathbb{F}_p} \mathsf{E}(\mathrm{L}_{\mathrm{cyc},\mathfrak{q}})_p = 2$ implies that the action of Γ in $\mathrm{Aut}(\mathsf{E}(\mathrm{L}_{\mathrm{cyc},w})_p)$ induces, upon fixing a basis, a 2-dimensional linear representation

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

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

4.2 – *Cassels–Poitou–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

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

These modules clearly admit multi-signed versions, defined as

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

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

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

Both $\mathrm{X}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$ and $\mathrm{X}^{\ddagger}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$ are finitely generated compact $\Lambda(\Gamma)$-modules and it follows from Corollary 4.6 that the $\Omega(\Gamma)$-modules $\mathrm{Y}^{\ddagger}(\mathsf{E}_p/\mathrm{L}_n)$ are finitely generated. Further, Corollary 4.4 implies that they only depend upon the isomorphism class of E_p. As a last piece of notation, suppose that $K \in \{\mathscr{L}_n, \mathrm{L}_v, \mathrm{L}_n\}$ for some $0 \le n < \infty$, and retain notation from Notation 2.2: in particular,

$$\widetilde{K} = \begin{cases} \overline{\mathbb{Q}_p} & \text{if } K = \mathscr{L}_n, \\ \overline{\mathrm{L}_v} & \text{if } K = \mathrm{L}_v, \\ \mathrm{L}^S & \text{if } K = \mathrm{L}. \end{cases}$$

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 $i \ge 1$) are defined as the inverse limit, with respect to corestriction maps

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

The reader is referred to [28, §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 [3, 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

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

where $\mathcal{A}_\pi$ denotes the formal group of $\mathsf{E}/\mathcal{O}_{\mathrm{L}_\pi}$, and the sign $\pm$ depends on the i-th component of $\ddagger$. These coincide with the local conditions in Definition 3.6, so that the group $\mathscr{R}^{\ddagger}(\mathsf{E}_p/\mathrm{L}_n)$ sits in the exact sequence

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

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

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

and define $\mathfrak{R}^{\ddagger}(\mathsf{E}_p/\mathrm{L})$ as the kernel

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

This gives the Cassels–Poitou–Tate exact sequence

$$\begin{aligned} (4.11) \qquad & 0 \to \mathscr{R}^{\ddagger}(\mathsf{E}_p/\mathrm{L}_n) \to \mathrm{H}^1(\mathcal{G}_n^S, \mathsf{E}_p) \to \bigoplus_{v \in S} \mathrm{H}^1(\mathrm{L}_{v,n}, \mathsf{E}_p)/W_v \\ & \to (\mathfrak{R}^{\ddagger}(\mathsf{E}_p/\mathrm{L}_n))^{\wedge} \to \mathrm{H}^2(\mathcal{G}_n^S, \mathsf{E}_p) \to \bigoplus_{w \mid v \in S} \mathrm{H}^2(\mathrm{L}_{n,v}, \mathsf{E}_p) \to 0, \end{aligned}$$

where the final 0 comes from Proposition 3.1. Similarly, put

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

and define $U_v^{\perp} \subseteq \mathrm{H}^1(\mathrm{L}_{n,v}, T_p(\mathsf{E}))$ to be the orthogonal complement of U_v. Defining $\mathfrak{S}^{\ddagger}(T_p(\mathsf{E})/\mathrm{L})$ as the kernel

$$0 \to \mathfrak{S}^{\ddagger}(T_p(\mathsf{E})/\mathrm{L}_n) \to \mathrm{H}^1(\mathcal{G}_n^S, T_p(\mathsf{E})) \to \bigoplus_{v \in S} \mathrm{H}^1(\mathrm{L}_{v,n}, T_p(\mathsf{E}))/U_v^{\perp},$$

we obtain the Cassels–Poitou–Tate exact sequence

$$\begin{aligned} (4.12) \qquad & 0 \to \mathrm{Sel}^{\ddagger}(\mathsf{E}_{p^{\infty}}/\mathrm{L}_n) \to \mathrm{H}^1(\mathcal{G}_n^S, \mathsf{E}_{p^{\infty}}) \to \bigoplus_{v \in S} \mathrm{H}^1(\mathrm{L}_{v,n}, \mathsf{E}_{p^{\infty}})/U_v \\ & \to (\mathfrak{S}^{\ddagger}(T_p(\mathsf{E})/\mathrm{L}_n))^{\wedge} \to \mathrm{H}^2(\mathcal{G}_n^S, \mathsf{E}_{p^{\infty}}) \to \bigoplus_{w \mid v \in S} \mathrm{H}^2(\mathrm{L}_{n,v}, \mathsf{E}_{p^{\infty}}) \to 0. \end{aligned}$$

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

$$\begin{aligned} \mathcal{R}^{\ddagger}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) &= \varprojlim \mathfrak{R}^{\ddagger}(\mathsf{E}_p/\mathrm{L}_n) \subseteq \mathrm{H}^1_{\mathrm{Iw}}(\mathrm{L}, \mathsf{E}_p), \\ \mathcal{S}^{\ddagger}(T_p(\mathsf{E})/\mathrm{L}_{\mathrm{cyc}}) &= \varprojlim \mathfrak{S}^{\ddagger}(T_p(\mathsf{E})/\mathrm{L}_n) \subseteq \mathrm{H}^1_{\mathrm{Iw}}(\mathrm{L}, T_p(\mathsf{E})), \end{aligned}$$

where inverse limits are taken with respect to corestriction maps. These are, respectively, an $\Omega(\Gamma)$-module and a $\Lambda(\Gamma)$-module and their relevance for our study comes from the following observation (cf. [23, Lemma 2.6 and Remark 2.7], where the case of an elliptic curve with ordinary reduction at p is considered):

Lemma 4.7. *There are isomorphisms*

$$\begin{aligned} \mathcal{R}^{\ddagger}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})^{\wedge} &\cong \varinjlim\, (\mathfrak{R}^{\ddagger}(\mathsf{E}_p/\mathrm{L}_n))^{\wedge}, \\ \mathcal{S}^{\ddagger}(T_p(\mathsf{E})/\mathrm{L}_{\mathrm{cyc}})^{\wedge} &\cong \varinjlim\, (\mathfrak{S}^{\ddagger}(*/T_p(\mathsf{E}))\mathrm{L}_n)^{\wedge}, \end{aligned}$$

where the direct limits are taken with respect to the dual of corestriction maps. Moreover, the group $\mathcal{R}^{\ddagger}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})$ is free as $\Omega(\Gamma)$-module and $\mathcal{S}^{\ddagger}(T_p(\mathsf{E})/\mathrm{L}_{\mathrm{cyc}})$ has no non-zero torsion $\Lambda(\Gamma)$-submodules.

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

$$\begin{aligned} \mathcal{R}^{\ddagger}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})^{\wedge} &= \mathrm{Hom}\big(\varprojlim \mathfrak{R}^{\ddagger}(*/\mathsf{E}_p)\mathrm{L}_n, \mathbb{Q}_p/\mathbb{Z}_p\big) \\ &= \varinjlim \mathrm{Hom}(\mathfrak{R}^{\ddagger}(*/\mathsf{E}_p)\mathrm{L}_n, \mathbb{Q}_p/\mathbb{Z}_p) \\ &= \varinjlim\, (\mathfrak{R}^{\ddagger}(\mathsf{E}_p/\mathrm{L}_n))^{\wedge}. \end{aligned}$$

The second isomorphism is analogous.

To show that $\mathcal{R}^{\ddagger}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})$ is a free $\Omega(\Gamma)$-module, note that Jannsen's spectral sequence [12, Corollary 13] takes the form

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

By Proposition 3.1, $E_2^{p,0} = 0$ for all $p \geq 0$. Therefore we have $E_\infty^{1,0} = E_2^{1,0} = 0$ and $E_2^{0,1} = E_\infty^{0,1}$, and it follows that

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

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 the inverse limit, with respect to corestriction, of the inclusions $\mathfrak{R}^{\ddagger}(\mathsf{E}_p/\mathrm{L}_n) \hookrightarrow \mathrm{H}^1(\mathcal{G}^S_n, \mathsf{E}_p)$, we obtain an injection

$$\mathcal{R}^{\ddagger}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) \hookrightarrow \mathrm{H}^1_{\mathrm{Iw}}(\mathrm{L}, \mathsf{E}_p).$$

Since $\Omega(\Gamma)$ is a principal ideal domain, a submodule of a free module is itself free, thereby proving the claim concerning $\mathcal{R}^{\ddagger}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})$. Passing to the Galois representation E_{p^∞}, Jannsen's spectral sequence [12, Theorem 1] gives

$$E_2^{p,q} = \mathrm{Ext}^p_{\Lambda(\Gamma)}\big(\mathrm{Hom}(\mathrm{H}^q(\mathcal{G}^S_{\mathrm{cyc}}, \mathsf{E}_{p^\infty}), \mathbb{Q}_p/\mathbb{Z}_p), \Lambda(\Gamma)\big) \Longrightarrow \mathrm{H}^{p+q}_{\mathrm{Iw}}(\mathrm{L}, T_p(\mathsf{E})).$$

Again, Proposition 3.1 yields $E_2^{p,0} = 0$ for all $p \geq 1$ and the same argument as above shows that the first Iwasawa cohomology group of $T_p(\mathsf{E})$ is torsion-free over $\Lambda(\Gamma)$. In particular, the same holds for its submodule $\mathcal{S}^\ddagger(T_p(\mathsf{E})/\mathrm{L}_{\mathrm{cyc}})$. ■

In Section 4.2.1, there is a summary of the notation for the various Selmer groups, and their signed versions, for both E_p and for E_{p^∞}.

Given two subextensions $\mathrm{L} \subseteq \mathrm{L}_n \subseteq \mathrm{L}_m \subseteq \mathrm{L}_{\mathrm{cyc}}$, consider the corresponding exact sequences (4.11). 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

$$(\mathrm{cores})^\wedge \colon (\mathfrak{R}^\ddagger(\mathsf{E}_p/\mathrm{L}_n))^\wedge \to (\mathfrak{R}^\ddagger(\mathsf{E}_p/\mathrm{L}_m))^\wedge \quad (m \geq n \geq 0)$$

of (4.11) gives commutative diagrams of exact sequences. By taking the direct limit over n, Lemma 4.7 gives exact sequences

$$\begin{aligned} 0 \to \mathscr{R}^\ddagger(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) \to \mathrm{H}^1(\mathcal{G}^S_{\mathrm{cyc}}, \mathsf{E}_p) &\xrightarrow{\xi_p^\ddagger} \bigoplus_{v \in S} {}^{\pm}\widetilde{K}_v(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) \\ \to \mathfrak{R}^\ddagger(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})^\wedge \to \mathrm{H}^2(\mathcal{G}^S_{\mathrm{cyc}}, \mathsf{E}_p) &\to \bigoplus_{w \mid v \in S} \mathrm{H}^2(\mathrm{L}_{\mathrm{cyc},w}, \mathsf{E}_p) \to 0, \end{aligned} \tag{4.13}$$

where the morphism $\xi_p^\ddagger$ and the $\Omega(\Gamma)$-modules ${}^{\pm}\widetilde{K}_v(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})$ were introduced in (4.5). Replacing the Galois representation E_p by E_{p^∞}, we obtain the analogous exact sequence

$$\begin{aligned} 0 \to \mathrm{Sel}^\ddagger(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}}) \to \mathrm{H}^1(\mathcal{G}^S_{\mathrm{cyc}}, \mathsf{E}_{p^\infty}) &\xrightarrow{\xi_{p^\infty}^\ddagger} \bigoplus_{v \in S} J_v^{\pm}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}}) \\ \to \mathcal{S}^\ddagger(T_p(\mathsf{E})/\mathrm{L}_{\mathrm{cyc}})^\wedge \to \mathrm{H}^2(\mathcal{G}^S_{\mathrm{cyc}}, \mathsf{E}_{p^\infty}) &\to \bigoplus_{w \mid v \in S} \mathrm{H}^2(\mathrm{L}_{\mathrm{cyc},w}, \mathsf{E}_{p^\infty}) \to 0. \end{aligned} \tag{4.14}$$

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

$$\begin{aligned} \mathrm{Sel}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}}) &= \ker\Big(\mathrm{H}^1(\mathcal{G}^S_\infty, \mathsf{E}_{p^\infty}) \to \bigoplus_{w \mid v \in S} \mathrm{H}^1(\mathrm{L}_{\mathrm{cyc},w}, \mathsf{E})_{p^\infty}\Big) \\ &= \ker\Big(\mathrm{H}^1(\mathcal{G}^S_\infty, \mathsf{E}_{p^\infty}) \to \bigoplus_{w \mid v \in S \setminus S^{\mathrm{ss}}} \mathrm{H}^1(\mathrm{L}_{\mathrm{cyc},w}, \mathsf{E})_{p^\infty} \\ &\qquad \oplus \bigoplus_{i=1}^{d} \mathrm{H}^1(\mathscr{L}_{\mathrm{cyc},i}, \mathsf{E}_{p^\infty}) / \operatorname{Im}(\kappa^{p^\infty}_{\mathscr{L}_{\mathrm{cyc},i}})\Big) \end{aligned} \tag{4.15}$$

is not $\Lambda(\Gamma)$-cotorsion, in general. Indeed, as is discussed in the proof of [3, Theorem 2.6], each local term $\mathrm{H}^1(\mathscr{L}_{\mathrm{cyc},i}, \mathsf{E})_{p^\infty}$ 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 [25, §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 [3, Theorems 2.8 and 2.18]).

In the supersingular setting, both Perrin-Riou and Kobayashi reduce the size of the kernels in (4.15) by replacing $\mathrm{Im}(\kappa^{p^\infty}_{\mathscr{L}_{\mathrm{cyc}}})$ with the smaller subgroup $\mathrm{Im}(\kappa^{\pm,p^\infty}_{\mathscr{L}_{\mathrm{cyc}}})$, 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 multi-signed* residual versions.

4.2.1. Notation.

- The local conditions $J_v^{\pm}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$ and ${}^{\pm}\widetilde{K}_v(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})$ are defined right after Definition 4.2 and are subgroups of global cohomology groups of E_{p^∞} and of E_p, respectively.
- These local conditions yield the definition of the (signed) Selmer groups $\mathrm{Sel}^{\ddagger}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$ and $\mathscr{R}^{\ddagger}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})$. The rationale beneath the choice of the letter R for the Selmer group of the representation E_p is to hint at a *residual* Selmer group.
- Taking Pontryagin duals of the above groups, one obtains the groups

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

  defined at the beginning of Section 4.2.
- By local Tate duality, the local conditions $J_v^{\pm}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$ and ${}^{\pm}\widetilde{K}_v(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})$ give rise to dual local conditions. These, in turn, define dual compact Selmer groups $\mathfrak{S}^{\ddagger}(T_p(\mathsf{E})/\mathrm{L}_n)$ and $\mathfrak{R}^{\ddagger}(\mathsf{E}_p/\mathrm{L}_n)$, appearing in equations (4.12) and (4.11), respectively. Again, the choice of letters S and R reflects the fact that these are the compact versions of the "full" Selmer group and of the residual Selmer group, respectively.
- Taking inverse limits, with respect to corestriction maps, over the cyclotomic tower of the compact groups $\mathfrak{S}^{\ddagger}(T_p(\mathsf{E})/\mathrm{L}_n)$ and $\mathfrak{R}^{\ddagger}(\mathsf{E}_p/\mathrm{L}_n)$ defines the $\Lambda(\Gamma)$-modules $\mathcal{S}^{\ddagger}(T_p(\mathsf{E})/\mathrm{L}_{\mathrm{cyc}})$ and $\mathcal{R}^{\ddagger}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})$ (the latter is in fact a $\Omega(\Gamma)$-module). Once more, the choice of letters is coherent with the previous rationale. The relation between Pontryagin and Tate duality is summarised in Lemma 4.7

4.3 – *Rank computation*

To approach $\mathscr{R}^\ddagger(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})$, the main objects of study will be the maps $\xi_p^\ddagger$ and $\xi_{p^\infty}^\ddagger$ appearing in the exact sequences (4.13) and (4.14). We will ultimately relate the surjectivity of $\xi_p^\ddagger$ to the structure of $\mathrm{X}^\ddagger(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$ as a $\Lambda(\Gamma)$-module (see Theorem 4.13). In this direction, the following hypothesis (which is the multi-sign analogue of condition (vi) in [18, Theorem 1.3]) is crucial:

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

The exact sequence which is crucial in our approach is (4.13). Concerning the term $\mathrm{H}^2(\mathcal{G}_{\mathrm{cyc}}^S, \mathsf{E}_p)$ in it, Coates and the second author have proposed in [2] the following conjecture:

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

The original formulation of Conjecture A in [2] is that the dual fine Selmer group $\mathcal{Y}(\mathsf{E}/\mathrm{L}_{\mathrm{cyc}})$ over $\mathrm{L}_{\mathrm{cyc}}$ (see [2, §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 4.9 below).

Proposition 4.8. *Conjecture* A *implies that* $\mathrm{H}^2(\mathcal{G}_{\mathrm{cyc}}^S, \mathsf{E}_{p^\infty}) = 0$. *Moreover, if* E *satisfies* Hyp $2_\ddagger$, *and if* $\mu^\ddagger = 0$, *then Conjecture* A *holds.*

Proof. Taking $\mathcal{G}_{\mathrm{cyc}}^S$-cohomology of the exact sequence (3.6) yields

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

where the surjection comes from the fact that $\mathrm{Gal}(\overline{\mathrm{L}}/\mathrm{L}_{\mathrm{cyc}})$ has cohomological dimension 2 (see [26, Theorem 10.11.3 and Proposition 3.3.5]). Therefore, if $\mathrm{H}^2(\mathcal{G}_{\mathrm{cyc}}^S, \mathsf{E}_p) = 0$ then multiplication by p is injective on $\mathrm{H}^2(\mathcal{G}_{\mathrm{cyc}}^S, \mathsf{E}_{p^\infty})$. On the other hand, every class in $\mathrm{H}^2(\mathcal{G}_{\mathrm{cyc}}^S, \mathsf{E}_{p^\infty})$ has finite p-power order, hence multiplication by p is injective if and only if $\mathrm{H}^2(\mathcal{G}_{\mathrm{cyc}}^S, \mathsf{E}_{p^\infty}) = 0$.

Suppose now that $\mathrm{X}^\ddagger(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$ is $\Lambda(\Gamma)$-torsion and $\mu^\ddagger = 0$. The dual fine Selmer group $\mathcal{Y}(\mathsf{E}/\mathrm{L}_{\mathrm{cyc}})$ is defined in [2, (42)] as the Pontryagin dual of

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

Since this kernel injects into $\mathrm{Sel}^\ddagger(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$ by (4.6), we obtain a surjection

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

Our assumptions imply then that $\mathscr{Y}(\mathsf{E}/\mathrm{L}_{\mathrm{cyc}})$ is a torsion $\Lambda(\Gamma)$-module with trivial μ-invariant, which is the formulation of [2, Conjecture A]. We are thus left to show that if $\mathscr{Y}(\mathsf{E}/\mathrm{L}_{\mathrm{cyc}})$ is $\Lambda(\Gamma)$-torsion and has trivial μ-invariant, then $\mathrm{H}^2(\mathcal{G}^S_{\mathrm{cyc}}, \mathsf{E}_p) = 0$. But Greenberg shows in [7, Proposition 4.1.6] that the vanishing of $\mathrm{H}^2(\mathcal{G}^S_{\mathrm{cyc}}, \mathsf{E}_p)$ is equivalent to the p-torsion subgroup $\mathscr{Y}(\mathsf{E}/\mathrm{L}_{\mathrm{cyc}})_p$ being finite, and this is certainly the case when $\mathscr{Y}(\mathsf{E}/\mathrm{L}_{\mathrm{cyc}})$ is $\Lambda(\Gamma)$-torsion and has trivial μ-invariant. ■

Remark 4.9. (1) The vanishing of $\mathrm{H}^2(\mathcal{G}^S_{\mathrm{cyc}}, \mathsf{E}_{p^\infty})$ is known as the *weak Leopoldt conjecture* (see [33, p. 348] and [5, Conjecture 3]). If $\mathrm{L} = \mathbb{Q}$, it holds by [13, 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 [29, p. 33, (1.4.3)] with Jannsen's spectral sequence from [12, Theorem 1]. Over an arbitrary base L, if $\mathrm{Sel}(\mathsf{E}/\mathrm{L})$ is finite, the vanishing can be proven by combining [3, Proposition 1.9] with the Hochschild–Serre spectral sequence.

(2) 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 4.10, global cohomology and local cohomology at primes where E does not have supersingular reduction are considered. Then, in Lemma 4.11, supersingular primes are treated.

Lemma 4.10. *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 $\mathrm{H}^1(\mathcal{G}^S_{\mathrm{cyc}}, \mathsf{E}_{p^\infty})$ has trivial μ invariant as well.*

As a consequence,

$$\begin{aligned}\operatorname{corank}_{\Omega(\Gamma)} &\mathrm{H}^1(\mathrm{L}_{\mathrm{cyc},w}, \mathsf{E}_p)\\ &= \operatorname{corank}_{\Lambda(\Gamma)} \mathrm{H}^1(\mathrm{L}_{\mathrm{cyc},w}, \mathsf{E}_{p^\infty}), \qquad w \mid \mathfrak{l} \in S^{\mathrm{bad}},\end{aligned} \tag{4.16}$$

$$\begin{aligned}\operatorname{corank}_{\Omega(\Gamma)} &\mathrm{H}^1(\mathrm{L}_{\mathrm{cyc},w}, \widetilde{\mathsf{E}}_p)\\ &= \operatorname{corank}_{\Lambda(\Gamma)}(\mathrm{H}^1(\mathrm{L}_{\mathrm{cyc},w}, \mathsf{E}_{p^\infty})/\operatorname{Im}(\kappa^{p^\infty}_{\mathrm{L}_{\mathrm{cyc},w}})), \quad w \mid \pi \in S^{\mathrm{ord}},\end{aligned} \tag{4.17}$$

and, assuming Conjecture A,

$$\operatorname{corank}_{\Omega(\Gamma)} \mathrm{H}^1(\mathcal{G}^S_{\mathrm{cyc}}, \mathsf{E}_p) = \operatorname{corank}_{\Lambda(\Gamma)} \mathrm{H}^1(\mathcal{G}^S_{\mathrm{cyc}}, \mathsf{E}_{p^\infty}). \tag{4.18}$$

Proof. We start with local cohomology, and let $v \in S \setminus S^{\mathrm{ss}}$ be any prime. Greenberg proves in [5, 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 (3.6) induces

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

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 property holds for the quotient module $\mathrm{H}^1(\mathrm{L}_{\mathrm{cyc},w}, \mathsf{E}_{p^\infty})/\operatorname{Im}(\kappa^{p^\infty}_{\mathrm{L}_{\mathrm{cyc},w}})$. 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 $\mathrm{H}^1(\mathcal{G}^S_{\mathrm{cyc}}, \mathsf{E}_{p^\infty})$, whence (iii).

By Proposition 4.1 (a) (resp. Proposition 4.1 (b)), the Pontryagin duals of the $\Omega(\Gamma)$-modules $\mathrm{H}^1(\mathcal{G}^S_{\mathrm{cyc}}, \mathsf{E}_p)$ and $\mathrm{H}^1(\mathcal{G}^S_{\mathrm{cyc}}, \mathsf{E}_{p^\infty})_p$ (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 (4.16) and (4.18) 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 (4.17). ■

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 [18, Proposition 3.32].

Lemma 4.11. *For each choice of sign ±, 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

$$\left(\mathrm{H}^1(\mathcal{L}_{\mathrm{cyc}}, \mathsf{E}_{p^\infty})/\operatorname{Im}(\kappa^{\pm,p^\infty}_{\mathcal{L}_{\mathrm{cyc}}})\right)^\wedge \cong \Lambda(\Gamma), \tag{4.19}$$

thanks to Proposition 4.1 (d).

The freeness claimed in (4.19) follows from [18, Lemma 3.31]. Indeed,

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

where $\mathrm{H}^1(\mathcal{L}_{\mathrm{cyc}}, \mathsf{E}_{p^\infty})^\wedge$ is $\Lambda(\Gamma)$-free of rank 2, as proven in [5, Corollary 1], and $\mathrm{Im}(\kappa^{\pm,p^\infty}_{\mathcal{L}_{\mathrm{cyc}}})^\wedge$ is of $\Lambda(\Gamma)$-rank equal to 1 and has no non-trivial finite $\Lambda(\Gamma)$-submodules, as follows from [18, 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 [11, Proposition 6.1]).

Proposition 4.12. *Suppose that Conjecture A holds for* E/L. *Then we have*

$$\begin{aligned}(4.20)\quad &\mathrm{corank}_{\Lambda(\Gamma)}\, \mathrm{H}^1(\mathcal{G}^S_{\mathrm{cyc}}, \mathsf{E}_{p^\infty})\\ &\quad = \sum_{\pi \in \mathcal{S}^{\mathrm{ord}}} \mathrm{corank}_{\Lambda(\Gamma)}\, J^{\pm}_{\pi}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}}) + \sum_{i=1}^{d} \mathrm{corank}_{\Lambda(\Gamma)}\, J^{\pm}_{\mathfrak{p}_i}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}}),\end{aligned}$$

$$\begin{aligned}(4.21)\quad &\mathrm{corank}_{\Omega(\Gamma)}\, \mathrm{H}^1(\mathcal{G}^S_{\mathrm{cyc}}, \mathsf{E}_{p})\\ &\quad = \sum_{\pi \in \mathcal{S}^{\mathrm{ord}}} \mathrm{corank}_{\Omega(\Gamma)}\, {}^{\pm}\widetilde{K}_{\pi}(\mathsf{E}_{p}/\mathrm{L}_{\mathrm{cyc}}) + \sum_{i=1}^{d} \mathrm{corank}_{\Omega(\Gamma)}\, {}^{\pm}\widetilde{K}_{\mathfrak{p}_i}(\mathsf{E}_{p}/\mathrm{L}_{\mathrm{cyc}}).\end{aligned}$$

Moreover,

$$\sum_{\mathfrak{l} \in \mathcal{S}^{\mathrm{bad}}} \mathrm{corank}_{\Lambda(\Gamma)}\, J^{\pm}_{\mathfrak{l}}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}}) = \sum_{\mathfrak{l} \in \mathcal{S}^{\mathrm{bad}}} \mathrm{corank}_{\Omega(\Gamma)}\, {}^{\pm}\widetilde{K}_{\mathfrak{l}}(\mathsf{E}_{p}/\mathrm{L}_{\mathrm{cyc}}) = 0.$$

Proof. The proof is an adaptation of [3, proof of Theorem 2.6]. We first compute the left-hand sides of both (4.20) and (4.21). In [5, Proposition 3] Greenberg proves that both $\mathrm{H}^1(\mathcal{G}^S_{\mathrm{cyc}}, \mathsf{E}_{p^\infty})$ and $\mathrm{H}^2(\mathcal{G}^S_{\mathrm{cyc}}, \mathsf{E}_{p^\infty})$ are co-finitely generated over $\Lambda(\Gamma)$ and further

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

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 4.8, 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,

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

Now (4.18) of Lemma 4.10 implies

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

Passing to the computation of the local coranks, let first $\pi \in S^{\mathrm{ord}}$. By [3, §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 $\pi \in S^{\mathrm{ord}}$, together with (4.2)) we know

$$\text{(4.22)} \qquad \operatorname{corank}_{\Lambda(\Gamma)} \bigoplus_{w|\pi} (\mathrm{H}^1(\mathrm{L}_{\mathrm{cyc},w}, \mathsf{E}_{p^\infty}) / \operatorname{Im}(\kappa^{\pm,p^\infty}_{\mathrm{L}_{\mathrm{cyc},w}})) = [\mathrm{L}_\pi : \mathbb{Q}_p].$$

Hence equation (4.17) of Lemma 4.10 yields

$$\text{(4.23)} \quad \operatorname{corank}_{\Omega(\Gamma)} \bigoplus_{w|\pi} \mathrm{H}^1(\mathrm{L}_{\mathrm{cyc},w}, \widetilde{\mathsf{E}}_p) = \operatorname{corank}_{\Omega(\Gamma)} {}^{\pm}\widetilde{K}_\pi(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) = [\mathrm{L}_\pi : \mathbb{Q}_p].$$

Consider now a prime $\mathfrak{p}_i \in S^{\mathrm{ss}}$. Lemma 4.11 implies that

$$\text{(4.24)} \quad \operatorname{corank}_{\Omega(\Gamma)}(\mathrm{H}^1(\mathscr{L}_{\mathrm{cyc},i}, \mathsf{E}_p) / \operatorname{Im}(\kappa^{\pm,p}_{\mathscr{L}_{\mathrm{cyc}}})) = \operatorname{corank}_{\Omega(\Gamma)} {}^{\pm}\widetilde{K}_{\mathfrak{p}_i}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) = 1.$$

Combining (4.22) and (4.19), we find

$$\sum_{\pi \in S^{\mathrm{ord}}} \operatorname{corank}_{\Lambda(\Gamma)} J^{\pm}_\pi(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}}) + \sum_{i=1}^{d} \operatorname{corank}_{\Lambda(\Gamma)} J^{\pm}_{\mathfrak{p}_i}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}}) = N.$$

Similarly, (4.23) and (4.24) together imply

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

and this establishes equations (4.20) and (4.21).

Finally, 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 [5, Proposition 2] that the $\Lambda(\Gamma)$-module $\mathrm{H}^1(\mathrm{L}_{\mathrm{cyc},\mathfrak{q}}, \mathsf{E}_{p^\infty})$ is cotorsion. Hence

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

and (4.16) of Lemma 4.10 implies

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

as well. 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 (4.13):

$$0 \to \mathcal{R}^{\ddagger}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) \to \mathrm{H}^1(\mathcal{G}^S_{\mathrm{cyc}}, \mathsf{E}_p) \xrightarrow{\xi^{\ddagger}_p} \bigoplus_{v\in S} {}^{\pm}\widetilde{K}_v(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})$$
$$\to \mathfrak{R}^{\ddagger}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})^{\wedge} \to \mathrm{H}^2(\mathcal{G}^S_{\mathrm{cyc}}, \mathsf{E}_p) \to \bigoplus_{w|v\in S} \mathrm{H}^2(\mathrm{L}_{\mathrm{cyc},w}, \mathsf{E}_p) \to 0.$$

Consider the projection

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

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

THEOREM 4.13. *Under our standing assumption* Hyp 1, *suppose that* Hyp $2_{\ddagger}$ *holds as well. Then the following assertions are equivalent:*

(a) $\xi^{\ddagger}_p$ *is surjective and Conjecture* A *holds.*

(b) $\vartheta^{\ddagger}_{p,S_p}$ *is surjective and Conjecture* A *holds.*

(c) $\mathcal{R}^{\ddagger}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})$ *is* $\Omega(\Gamma)$*-cotorsion.*

(d) $\mathrm{X}^{\ddagger}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$ *has trivial* μ*-invariant.*

PROOF. To show that (a) ⇒ (c), take Pontryagin duals of the short exact sequence

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

to obtain

$$0 \to \bigoplus_{v\in S} {}^{\pm}\widetilde{K}_v(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})^{\wedge} \xrightarrow{\xi^{\ddagger\wedge}_p} \mathrm{H}^1(\mathcal{G}^S_{\mathrm{cyc}}, \mathsf{E}_p)^{\wedge} \to \mathrm{Y}^{\ddagger}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) \to 0.$$

By Proposition 4.12, 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 $\vartheta^{\ddagger}_{p,S_p} = \mathrm{pr}_{S_p} \circ \xi^{\ddagger}_p$ is surjective, yielding (a) ⇒ (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 4.6 shows that the kernel of

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

is finite, showing the equivalence between (c) and (d).

So far, we have shown that (b) ⇐ (a) ⇒ (c) ⇔ (d). We are left with the implications (c) ⇒ (a) and (b) ⇒ (a). Since (c) ⇒ (d) ⇒ Conjecture A by Proposition 4.8, and (b) contains Conjecture A, we can assume from now on that $\mathrm{H}^2(\mathcal{G}^S_{\mathrm{cyc}}, \mathsf{E}_p) = 0$. In particular, the sequence (4.25) becomes

$$(4.25)\qquad 0 \to \mathscr{R}^\ddagger(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) \to \mathrm{H}^1(\mathcal{G}^S_{\mathrm{cyc}}, \mathsf{E}_p) \xrightarrow{\xi^\ddagger_p} \bigoplus_{v\in S} {}^{\pm}\widetilde{K}_v(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})$$
$$\to \mathcal{R}^\ddagger(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})^\wedge = \mathrm{coker}(\xi^\ddagger_p) \to 0,$$

and Proposition 4.12 yields

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

Assuming (c), it follows that $\mathcal{R}^\ddagger(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})$ is $\Omega(\Gamma)$-torsion. On the other $\mathcal{R}^\ddagger(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})$ is $\Omega(\Gamma)$-free, in light of Lemma 4.7, and to be $\Omega(\Gamma)$-torsion it must be trivial, establishing (c) ⇒ (a).

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

$$\begin{tikzcd}
\mathrm{H}^1(\mathcal{G}^S_{\mathrm{cyc}}, \mathsf{E}_p) \arrow[r, "\xi^\ddagger_p"] \arrow[dr, "\vartheta^\ddagger_{p,S_p}"'] & \bigoplus_{\mathfrak{l}\in S^{\mathrm{bad}}} {}^{\pm}\widetilde{K}_{\mathfrak{l}}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) \oplus \bigoplus_{v\in S_p} {}^{\pm}\widetilde{K}_v(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) \arrow[d, "\mathrm{pr}_{S_p}"] \\
 & \bigoplus_{v\in S_p} {}^{\pm}\widetilde{K}_v(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}).
\end{tikzcd}$$

It induces an exact sequence

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

which implies that $\mathrm{coker}(\xi^\ddagger_p)$ is cotorsion, thanks to Proposition 4.12. Since $\mathrm{coker}(\xi^\ddagger_p)$ is isomorphic to $\mathcal{R}^\ddagger(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})^\wedge$ by (4.25), and $\mathcal{R}^\ddagger(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}})$ is free by Lemma 4.7, this forces $\mathrm{coker}(\xi^\ddagger_p) = 0$, establishing the final implication (b) ⇒ (a). ■

REMARK 4.14. 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 4.13, we obtain a result along the lines of Greenberg–Vatsal's work [8, Theorem 1.4] in the supersingular setting. Results somewhat similar to Theorem 4.15 below, again in the supersingular setting, have been obtained by Kim in [15, Corollary 2.13] and by Hatley–Lei in [10, Theorem 4.6], by different methods.

Theorem 4.15. *Let $\mathsf{E}_1, \mathsf{E}_2$ be two elliptic curves defined over* L, *satisfying Hypothesis* Hyp 1 *and such that the residual Galois representations $(\mathsf{E}_1)_p$ and $(\mathsf{E}_2)_p$ are isomorphic. Then, the sets S_1^{ss} and S_2^{ss} of primes of supersingular reduction for E_1 and E_2 coincide. Given a vector $\ddagger \in \{+,-\}^d$, assume that both curves satisfy* Hyp $2_\ddagger$ *and let $\mu^{\ddagger}_{\mathsf{E}_j}$ be the Iwasawa μ-invariants of $\mathrm{X}^{\ddagger}((\mathsf{E}_j)_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$, for $j = 1, 2$. Then*

$$\mu^{\ddagger}_{\mathsf{E}_1} = 0 \Longleftrightarrow \mu^{\ddagger}_{\mathsf{E}_2} = 0. \tag{4.26}$$

Proof. Observe first that if $\mu^{\ddagger}_{\mathsf{E}_j} = 0$ for one curve E_j, then Conjecture A holds for both curves, thanks to Proposition 4.8. 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

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

defined before Theorem 4.13. 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 Proposition 3.9 (ii). Similarly, at every prime in S^{ss}, Proposition 3.8 gives an isomorphism between the groups

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

for $j = 1, 2$. It follows that $\vartheta^{\ddagger}_{(\mathsf{E}_1)_p, S_p}$ is surjective if and only if $\vartheta^{\ddagger}_{(\mathsf{E}_2)_p, S_p}$ is surjective. Theorem 4.13 now yields (4.26). ■

In order to prove the next theorem, we need the following proposition, which is the analogue for the Galois representation E_{p^∞} of the equivalence between (a) and (c) of Theorem 4.13, as well as its Corollary 4.18. To state them, recall the exact sequence (4.14):

$$\begin{aligned}0 \to \mathrm{Sel}^{\ddagger}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}}) \to \mathrm{H}^1(\mathcal{G}^S_{\mathrm{cyc}}, \mathsf{E}_{p^\infty}) &\xrightarrow{\xi^{\ddagger}_{p^\infty}} \bigoplus_{v \in S} J^{\pm}_v(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}}) \\ \to \mathcal{S}^{\ddagger}(T_p(\mathsf{E})/\mathrm{L}_{\mathrm{cyc}})^{\wedge} \to \mathrm{H}^2(\mathcal{G}^S_{\mathrm{cyc}}, \mathsf{E}_{p^\infty}) &\to \bigoplus_{w \mid v \in S} \mathrm{H}^2(\mathrm{L}_{\mathrm{cyc},w}, \mathsf{E}_{p^\infty}) \to 0.\end{aligned}$$

Proposition 4.16. *Under the standing assumption* Hyp 1, *assume further that Conjecture* A *holds. Then* Hyp $2_\ddagger$ *holds if and only if $\xi^{\ddagger}_{p^\infty}$ is surjective.*

Proof. By Proposition 4.8, Conjecture A yields that $\mathrm{H}^2(\mathcal{G}_{\mathrm{cyc}}^S, \mathsf{E}_{p^\infty}) = 0$, thus

$$\operatorname{coker}(\xi_{p^\infty}^\ddagger) = \mathcal{S}^\ddagger(T_p(\mathsf{E})/\mathrm{L}_{\mathrm{cyc}})^\wedge.$$

Thanks to (4.14), we need to show that $\mathcal{S}^\ddagger(T_p(\mathsf{E})/\mathrm{L}_{\mathrm{cyc}})^\wedge = 0$ if and only if $\mathrm{X}^\ddagger(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$ is $\Lambda(\Gamma)$-torsion. The rank computations performed in Proposition 4.12 yield that

$$\operatorname{corank}_{\Lambda(\Gamma)} \operatorname{coker}(\xi_{p^\infty}^\ddagger) = \operatorname{corank}_{\Lambda(\Gamma)} \ker(\xi_{p^\infty}^\ddagger) = \operatorname{corank}_{\Lambda(\Gamma)} \mathrm{Sel}^\ddagger(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}}).$$

Therefore, Hyp $2_\ddagger$ is equivalent to the statement that $\operatorname{coker}(\xi_{p^\infty}^\ddagger)^\wedge = \mathcal{S}^\ddagger(T_p(\mathsf{E})/\mathrm{L}_{\mathrm{cyc}})$ is $\Lambda(\Gamma)$-torsion. By Lemma 4.7 this can happen if and only if it is trivial, finishing the proof. ■

Before deriving Corollary 4.18, recall the following result due to Greenberg (see [6, pp. 104–105]). We give a different, homological proof that works in a broader context. The second author is grateful to Akhil Matthew for helpful discussions in this regard.

Proposition 4.17. *Let $0 \to M \to N \to M/N \to 0$ be an exact sequence of $\Lambda(\Gamma)$-modules. Suppose that M is free and that N has no non-zero finite $\Lambda(\Gamma)$-submodules. Then M/N has no non-zero finite $\Lambda(\Gamma)$-submodules.*

Proof. Let us prove that the maximal finite $\Lambda(\Gamma)$-submodule $W \subseteq M/N$ is zero. Being pseudo-null, it satisfies $\mathrm{Ext}^i_{\Lambda(\Gamma)}(W, \Lambda(\Gamma)) = 0$, for $i = 0, 1$, as shown in [26, Proposition 5.5.3 (ii)]. Since M is free, this implies $\mathrm{Ext}^1_{\Lambda(\Gamma)}(W, M) = 0$. Applying the functor $\mathrm{Hom}_{\Lambda(\Gamma)}(W, -)$ to the exact sequence in the statement therefore gives an exact sequence

$$0 \to \mathrm{Hom}_{\Lambda(\Gamma)}(W, M) \to \mathrm{Hom}_{\Lambda(\Gamma)}(W, N) \to \mathrm{Hom}_{\Lambda(\Gamma)}(W, M/N) \to 0.$$

As N contains no non-zero finite $\Lambda(\Gamma)$-submodules, the term $\mathrm{Hom}_{\Lambda(\Gamma)}(W, N)$ vanishes, and therefore $\mathrm{Hom}_{\Lambda(\Gamma)}(W, M/N) = 0$. This implies the proposition, since $W \subseteq M/N$. ■

Corollary 4.18. *Assume Hyp 1 and Hyp $2_\ddagger$ as well as Conjecture A. If the Pontryagin dual $\mathrm{X}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$ of the usual Selmer group does not have any non-zero finite $\Lambda(\Gamma)$-submodule, then the same holds for the Pontryagin dual $\mathrm{X}^\ddagger(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$ of the multi-signed Selmer group.*

Proof. For every $v \in S$, define the usual local conditions as

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

the group $J_v(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$ is a quotient of $J_v^{\pm}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$, and it actually coincides with it for all $v \in S \setminus S^{\mathrm{ss}}$. Consider the commutative triangle

$$\begin{tikzcd}
\mathrm{H}^1(\mathcal{G}^S_{\mathrm{cyc}}, \mathsf{E}_{p^\infty}) \arrow[r, "\xi^{\ddagger}_{p^\infty}"] \arrow[dr, "\xi_{p^\infty}"'] & \bigoplus_{v\in S} J_v^{\pm}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}}) \arrow[d, two heads, "\eta"] \\
 & \bigoplus_{v\in S} J_v(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}}),
\end{tikzcd}$$

where η is the canonical surjection. By Proposition 4.16, the morphism $\xi^{\ddagger}_{p^\infty}$ is surjective, and therefore there is a short exact sequence

$$0 \to \ker \xi^{\ddagger}_{p^\infty} \to \ker \xi_{p^\infty} \to \ker \eta \to 0. \tag{4.27}$$

By definition, $\ker \xi^{\ddagger}_{p^\infty} = \mathrm{Sel}^{\ddagger}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$ and $\ker \xi_{p^\infty} = \mathrm{Sel}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$, while

$$\ker \eta = \bigoplus_{i=1}^{d} \operatorname{Im}(\kappa^{p^\infty}_{\mathfrak{L}_{\mathrm{cyc},i}})/\operatorname{Im}(\kappa^{\pm,p^\infty}_{\mathfrak{L}_{\mathrm{cyc},i}}).$$

Observe now that

$$\operatorname{Im}(\kappa^{p^\infty}_{\mathfrak{L}_{\mathrm{cyc},i}}) = \mathrm{H}^1(\mathrm{L}_{w,\mathrm{cyc}}, \mathsf{E}_{p^\infty})$$

by [1, Proposition 4.8], so that $(\ker \eta)^\wedge$ is $\Lambda(\Gamma)$-free by [18, Proposition 3.32]. The corollary follows from Proposition 4.17 applied to the Pontryagin dual of (4.27). ∎

Remark 4.19. The above result has been obtained by Kitajima–Otsuki in [18, Theorem 4.8] in the special case when $\ddagger = \{+, +, \dots, +\}$ or $\ddagger = \{-, -, \dots, -\}$ and under the more restrictive hypothesis that both $\mathrm{X}^+(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$ *and* $\mathrm{X}^-(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$ are torsion $\Lambda(\Gamma)$-modules. Our approach through the exact sequence (4.14) allows us to make the weaker assumption that just one of these modules be torsion. On the other hand, assuming that both $\mathrm{X}^+(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$ *and* $\mathrm{X}^-(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$ are torsion $\Lambda(\Gamma)$-modules, they prove in [18, Theorem 4.5] that the Pontryagin dual $\mathrm{X}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$ of the usual Selmer group does not contain any non-zero, finite $\Lambda(\Gamma)$-submodule.

In [21, Theorems 2.14 and 4.8] Lei and the second author give other criteria for the vanishing of the maximal finite $\Lambda(\Gamma)$-submodule of $\mathrm{X}(\mathsf{E}_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$.

Along the lines of Kim's and Hatley–Lei's results quoted above, when the $\mu^{\ddagger}$-invariants of two residually isomorphic elliptic curves vanish, we can relate their $\lambda^{\ddagger}$-invariants: this is the main content of Theorem 4.20 below. We denote by

$$\rho_{\mathsf{E}}^{\ddagger} = \dim_{\mathbb{F}_p} \mathrm{Y}^{\ddagger}(\mathsf{E}_p/\mathrm{L}_{\mathrm{cyc}}) \tag{4.28}$$

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

Theorem 4.20. *Let $\mathsf{E}_1, \mathsf{E}_2$ be two elliptic curves defined over* L, *satisfying the hypotheses of Theorem 4.15. Assume that their Iwasawa $\mu^{\ddagger}$-invariants vanish and suppose further that the Pontryagin duals $\mathrm{X}((\mathsf{E}_j)_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$ of the usual Selmer groups do not have any non-zero finite $\Lambda(\Gamma)$-submodule. Then,*

$$\lambda_{\mathsf{E}_j}^{\ddagger} = \rho^{\ddagger} + \delta_{\mathsf{E}_j}, \tag{4.29}$$

where δ_{E_j} is as in Definition 4.5 and $\rho^{\ddagger} := \rho_{\mathsf{E}_1}^{\ddagger} = \rho_{\mathsf{E}_2}^{\ddagger}$ is as in (4.28).

Remark 4.21. The hypothesis that the Pontryagin duals of the signed Selmer groups have no non-zero finite $\Lambda(\Gamma)$-submodule, which we deduce from the analogous result for the usual Selmer group, is known to hold in many cases: see, for instance, [18, Theorem 4.5] and [10, Theorem 3.1].

Remark 4.22. As already observed in Corollary 4.6, the quantity δ_{E} is independent of the vector $\ddagger$. In particular, for elliptic curves satisfying Hyp 1 and Hyp $2_{\ddagger}$ for two vectors $\ddagger_1$ and $\ddagger_2$, and such that their multi-signed invariants $\mu^{\ddagger_1}$ and $\mu^{\ddagger_2}$ are both 0, the difference $\lambda^{\ddagger_1} - \lambda^{\ddagger_2}$ of the multi-signed λ-invariants depends only on the isomorphism class of the residual representation.

The concrete manner in which this result will be applied later is the following. Suppose we are given a family of elliptic curves (satisfying Hyp 1) with the property that their residual representations are isomorphic. Given a vector $\ddagger$, suppose that all members in the family satisfy Hyp $2_{\ddagger}$. A consequence of Theorem 4.15 is that if one member A in the family satisfies $\mu_{\mathsf{A}}^{\ddagger} = 0$, then for all other members E in the family, we obtain $\mu_{\mathsf{E}}^{\ddagger} = 0$. Moreover, Theorem 4.20 shows that if A satisfies $\mu_{\mathsf{A}}^{\ddagger_1} = \mu_{\mathsf{A}}^{\ddagger_2} = 0$ for two vectors $\ddagger_1, \ddagger_2$, the difference of multi-signed Iwasawa invariants

$$\lambda_{\mathsf{E}}^{\ddagger_1} - \lambda_{\mathsf{E}}^{\ddagger_2} = \rho_{\mathsf{A}}^{\ddagger_1} - \rho_{\mathsf{A}}^{\ddagger_2}$$

is constant. In particular, if $\rho_{\mathsf{A}}^{\ddagger_1} = \rho_{\mathsf{A}}^{\ddagger_2}$, then $\lambda_{\mathsf{E}}^{\ddagger_1} = \lambda_{\mathsf{E}}^{\ddagger_2}$ for all curves E in the family. This hints at an appropriate generalisation of our results for Coleman families and we hope to investigate it in the future.

Proof of Theorem 4.20. Corollary 4.18 implies that the Pontryagin duals $\mathrm{X}^{\ddagger}((\mathsf{E}_j)_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})$ of the multi-signed Selmer groups do not have any non-zero finite $\Lambda(\Gamma)$-submodule, for $j = 1, 2$. Further, they are $\Lambda(\Gamma)$-torsion thanks to Hypothesis Hyp $2_{\ddagger}$. Since $\mu^{\ddagger}_{\mathsf{E}_1} = \mu^{\ddagger}_{\mathsf{E}_2} = 0$, we have

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

On the other hand, taking Pontryagin duals in Corollary 4.6 gives an exact sequence

$$\begin{aligned} V_j &\hookrightarrow \left(\mathrm{Sel}^{\ddagger}((\mathsf{E}_j)_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})_p\right)^{\wedge} \\ &= \mathrm{X}^{\ddagger}((\mathsf{E}_j)_{p^\infty}/\mathrm{L}_{\mathrm{cyc}})/p\,\mathrm{X}^{\ddagger}((\mathsf{E}_j)_{p^\infty}/\mathrm{L}_{\mathrm{cyc}}) \\ &\twoheadrightarrow \mathrm{Y}^{\ddagger}((\mathsf{E}_j)_p/\mathrm{L}_{\mathrm{cyc}}), \end{aligned} \tag{4.30}$$

where V_j is an $\mathbb{F}_p$-vector space of finite dimension. Since we are assuming $\mu^{\ddagger}_{\mathsf{E}_j} = 0$, Theorem 4.13 implies that $\xi^{\ddagger}_{(\mathsf{E}_j)_p}$ is surjective and therefore, again by Corollary 4.6, we have $\dim_{\mathbb{F}_p} V_j = \delta_{\mathsf{E}_j}$. Taking lengths in (4.30) gives

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

and this finishes the proof of Theorem 4.20. ∎

In the next two corollaries, we consider the main setting of Theorem 4.15. Thus, let $\mathsf{E}_1, \mathsf{E}_2$ be two elliptic curves defined over L satisfying hypotheses Hyp 1 and Hyp $2_{\ddagger}$, and such that the residual Galois representations $(\mathsf{E}_1)_p$ and $(\mathsf{E}_2)_p$ are isomorphic, so $\rho^{\ddagger}_{\mathsf{E}_1} = \rho^{\ddagger}_{\mathsf{E}_2} := \rho^{\ddagger}$. 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 $\mu^{\ddagger}_{\mathsf{E}_1} = 0$, which is equivalent to assuming $\mu^{\ddagger}_{\mathsf{E}_2} = 0$ by Theorem 4.15. Moreover, this implies that Conjecture A holds for both curves, again by Theorem 4.15. Finally, suppose that the Pontryagin duals of the usual Selmer groups do not contain any non-trivial, finite $\Lambda(\Gamma)$-submodule, so that Theorem 4.20 applies.

Corollary 4.23. *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*

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

Proof. Recall from Definition 4.5 that

$$\delta_{\mathsf{E}_j} = \sum_{\mathfrak{l} \in S_j^{\mathrm{bad}}} g_{\mathfrak{l}} \cdot \dim_{\mathbb{F}_p} \mathsf{E}_j(\mathrm{L}^1_{\mathfrak{q}})_p + \sum_{\pi \in S^{\mathrm{ord}}} g_{\pi} \dim_{\mathbb{F}_p} \widetilde{\mathsf{E}}_j(\mathbb{F}_{\pi})_p, \tag{4.31}$$

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

The same argument as in the proof of Corollary 4.6 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 hypotheses 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 (4.31) vanish and $\delta_{\mathsf{E}_1} = \delta_{\mathsf{E}_2} = 0$. The corollary follows from (4.29) in Theorem 4.20. ■

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 4.24. *Suppose that* E_1 *is a CM curve. Then*

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

Remark 4.25. The interest of Corollary 4.24 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 $\mathbb{Z}_p$-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 $\mathrm{Aut}((\mathsf{E}_1)_p) \subseteq \mathrm{GL}_2(\mathbb{F}_p)$ is contained in the normalizer of a Cartan subgroup, which is certainly the case when E_1 is CM.

Proof of Corollary 4.24. Since E_1 is CM and $p \geq 3$, the image of $\mathrm{Gal}(\overline{\mathrm{L}}/\mathrm{L})$ inside $\mathrm{Aut}((\mathsf{E}_1)_p) \subseteq \mathrm{GL}_2(\mathbb{F}_p)$ is contained in the normalizer of a Cartan subgroup. 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 $\mathrm{Aut}((\mathsf{E}_2)_p)$ 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 (4.29), combined with Definition 4.5. ■

5. Numerical examples

Our class of examples comes from the work [32]. Both for $p = 3$ and $p = 5$, Rubin and Silverberg define, for each $D \not\equiv 0 \pmod{p}$, a family parameterised by[1] $t \in \mathbb{Z}$. All

[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 $t \in \mathbb{Z}$

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 families contain a CM member, and so Corollary 4.24 applies. Since the field of definition of all curves is $\mathbb{Q}$, we have $d = 1$, allowing for simplified notation; hence, write $\pm$ for the generic vector $\ddagger \in \{+, -\}$. For all choices of (p, D), the strategy will be as follows:

(1) Find one curve A in the family for which the Iwasawa invariants $\mu_{\mathsf{A}}^{\pm}$ and $\lambda_{\mathsf{A}}^{\pm}$ have been computed in [24] and such that $\mu_{\mathsf{A}}^{+} = \mu_{\mathsf{A}}^{-} = 0$. In practice, we take for A the CM curve corresponding to the parameter $t = 0$.

(2) Apply Theorem 4.15 (see in particular Remark 4.21) to deduce that $\mu^{\pm} = 0$ for all other members in the family. In particular, Conjecture A holds for the whole family, by Proposition 4.8.

(3) Deduce from Theorem 4.20 (which can be applied thanks to [18, Theorem 4.5]) that $\rho_{\mathsf{A}}^{\pm} = \lambda_{\mathsf{A}}^{\pm} - \delta_{\mathsf{A}}$ for A, and set $\rho^{\pm} := \rho_{\mathsf{A}}^{\pm}$.

(4) By Corollary 4.24, we obtain

$$\lambda_{\mathsf{E}}^{\pm} = \rho^{\pm} + \delta_{\mathsf{E}} = \rho^{\pm} + \sum_{\ell \in S^{\mathrm{bad}}} g_{\ell} \dim_{\mathbb{F}_p} \mathsf{E}(\mathbb{Q}_{\ell})_p$$

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 $2_{\ddagger}$ is always satisfied by [19, Theorem 1.2] and the usual Selmer group never contains non-trivial, finite $\Lambda(\Gamma)$-submodules by [18, Theorem 4.5] combined with Corollary 4.18.

(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 $\lambda_{\mathsf{E}}^{\pm}$.

We will consider the families attached to $D = 1$ and $D = -1$ for $p = 3$, and the families attached to $D = 3$ and $D = 14$ for $p = 5$. Our source of numerical data is [24]. Labels of elliptic curves follow Cremona's tables as in [24], when available (i.e. for discriminant less than 500.000 as per October 2019). The computations have been made in `SAGE`. (We used commands `E.q_expansion(4)` to compute a_3 and `E(Q).division_points(p)` to compute torsion points.)

5.1 – *The case* $p = 3$

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 [24], 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 (4.29) gives $\lambda_{\mathsf{E}_3}^{\pm} = 1$, in accordance with the numerical value found in [24].

To show a somehow extreme example, consider $t = 18$. It satisfies $a_3(\mathsf{E}_{18}) = 0$ and its conductor is $90{,}885{,}856 = 2^5 \cdot 2{,}840{,}183$. The dimensions of its local 3-torsion are

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

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 4.15. 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 [15, p. 190]), although he does not produce explicit examples. Note also that these Iwasawa invariants are not available on [24].

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 [24], and have $a_3(\mathsf{E}_i) = 0$, but the Iwasawa invariants are available only for E_2 and E_5: they read $\lambda_{\mathsf{E}_2}^{\pm} = 3$ and $\lambda_{\mathsf{E}_5}^{\pm} = 0$. This is in accordance with formula (4.29): indeed, $S_{\mathsf{E}_2}^{\mathrm{bad}} = \{2, 359\}$, $S_{\mathsf{E}_5}^{\mathrm{bad}} = \{2, 2053\}$ and

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

$$\dim_{\mathbb{F}_3}(\mathsf{E}_5(\mathbb{Q}_\ell)_3) = \begin{cases} 0 & \text{for } \ell = 2, \\ 0 & \text{for } \ell = 2053. \end{cases}$$

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

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

Further, $g_{37} = g_{179} = 3$, whence $\lambda_{\mathsf{E}_4}^{\pm} = 9$, a value which is not available on [24]. Also, all curves satisfy $\mu^{\pm} = 0$ by Theorem 4.15.

We finish this series of examples with the curve E_{149} for $t = 149$. Its conductor is $106{,}459{,}833{,}664 = 2^6 \cdot 1{,}663{,}434{,}901$, 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 $\mu_{\mathsf{E}_{149}}^{\pm} = \lambda_{\mathsf{E}_{149}}^{\pm} = 0$.

5.2 – *The case $p = 5$*

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 [24] and $\mu_{\mathsf{A}}^{\pm} = 0, \lambda_{\mathsf{A}}^{\pm} = 1$. To find $\rho^{\pm} = \rho_{\mathsf{A}}^{\pm}$, we need to compute δ_{A}. The primes of bad reduction are $S_{\mathsf{A}}^{\mathrm{bad}} = \{2, 3\}$ and $\mathsf{A}(\mathbb{Q}_\ell)_3 = 0$ for both $\ell \in S_{\mathsf{A}}^{\mathrm{bad}}$, 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 [24]. Computing Iwasawa invariants through formula (4.29) 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 4.15 that $\mu_{\mathsf{E}_6}^{\pm} = \mu_{\mathsf{E}_{14}}^{\pm} = 0$.

The conductor of E_6 is

$$16{,}847{,}046{,}490{,}346{,}928 = 2^4 \cdot 3^5 \cdot 4{,}333{,}088{,}089{,}081.$$

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 $\lambda_{\mathsf{E}_6}^{\pm} = \rho^{\pm} = 1$. The conductor of E_{14} is

$$445{,}766{,}016{,}078{,}830{,}163{,}888 = 2^4 \cdot 3^5 \cdot 29 \cdot 602{,}279 \cdot 6{,}564{,}248{,}011$$

and E_{14} neither has $\mathbb{Q}_2$-rational nor $\mathbb{Q}_3$-rational 5-torsion points. On the other hand,

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

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 $\lambda_{\mathsf{E}_{14}}^{\pm} = \delta_{\mathsf{E}_{14}} + \rho^{\pm} = 5$.

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 $\mu_{\mathsf{A}}^{\pm} = 0$, 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 4.21, 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 [24]. As examples, we consider the curves for $t = 6$ and $t = 8$. The first has $S_{\mathsf{E}_6}^{\mathrm{bad}} = \{2, 3, 7, 22621, 92081500261\}$ and there are no $\mathbb{Q}_\ell$-rational 5-torsion points at $\ell \in S_{\mathsf{E}_6}^{\mathrm{bad}}$ except for $\ell = 92081500261$, where $\dim_{\mathbb{F}_5}(\mathsf{E}_6(\mathbb{Q}_\ell)_5) = 2$. Since $g_{92081500261} = 1$, we find $\delta_{\mathsf{E}_6} = 2$ and

$$\lambda_{\mathsf{E}_6}^{+} = 5 \quad \text{and} \quad \lambda_{\mathsf{E}_6}^{-} = 3.$$

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

$$\lambda_{\mathsf{E}_6}^{+} = 3 \quad \text{and} \quad \lambda_{\mathsf{E}_6}^{-} = 1.$$

Acknowledgements – 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. The first author gratefully acknowledges the support and hospitality of PIMS and of the University of British Columbia. We would also like to thank Matthieu Romagny for helpful correspondence.

Funding – The first author was supported by an *acceuil en délégation à l'UMI-3069 du CNRS*, the second author by NSERC Discovery grant 201903987.

References

[1] J. Coates – R. Greenberg, Kummer theory for abelian varieties over local fields. *Invent. Math.* **124** (1996), no. 1-3, 129–174. Zbl 0858.11032 MR 1369413

[2] J. Coates – R. Sujatha, Fine Selmer groups of elliptic curves over p-adic Lie extensions. *Math. Ann.* **331** (2005), no. 4, 809–839. Zbl 1197.11142 MR 2148798

[3] J. Coates – R. Sujatha, *Galois cohomology of elliptic curves*. Second edn., Narosa Publishing House, New Delhi (published for the Tata Institute of Fundamental Research), 2010. Zbl 1213.11115 MR 3060733

[4] M. Emerton – R. Pollack – T. Weston, Variation of Iwasawa invariants in Hida families. *Invent. Math.* **163** (2006), no. 3, 523–580. Zbl 1093.11065 MR 2207234

[5] R. Greenberg, Iwasawa theory for p-adic representations. In *Algebraic number theory*, pp. 97–137, Adv. Stud. Pure Math. 17, Academic Press, Boston, MA, 1989. Zbl 0739.11045 MR 1097613

[6] R. Greenberg, Iwasawa theory for elliptic curves. In *Arithmetic theory of elliptic curves (Cetraro, 1997)*, pp. 51–144, Lecture Notes in Math. 1716, Springer, Berlin, 1999. Zbl 0946.11027 MR 1754686

[7] R. Greenberg, Iwasawa theory, projective modules, and modular representations. *Mem. Amer. Math. Soc.* **211** (2011), no. 992. Zbl 1247.11085 MR 2807791

[8] R. Greenberg – V. Vatsal, On the Iwasawa invariants of elliptic curves. *Invent. Math.* **142** (2000), no. 1, 17–63. Zbl 1032.11046 MR 1784796

[9] Y. Hachimori, Iwasawa λ-invariants and congruence of Galois representations. *J. Ramanujan Math. Soc.* **26** (2011), no. 2, 203–217. Zbl 1256.11061 MR 2816789

[10] J. Hatley – A. Lei, Arithmetic properties of signed Selmer groups at non-ordinary primes. *Ann. Inst. Fourier (Grenoble)* **69** (2019), no. 3, 1259–1294. Zbl 1477.11183 MR 3986915

[11] A. Iovita – R. Pollack, Iwasawa theory of elliptic curves at supersingular primes over $\mathbb{Z}_p$-extensions of number fields. *J. Reine Angew. Math.* **598** (2006), 71–103. Zbl 1114.11053 MR 2270567

[12] U. Jannsen, A spectral sequence for Iwasawa adjoints. *Münster J. Math.* **7** (2014), no. 1, 135–148. Zbl 1316.11099 MR 3271243

[13] K. Kato, p-adic Hodge theory and values of zeta functions of modular forms. *Asterisque* (2004), no. 295, 117–290. Zbl 1142.11336 MR 2104361

[14] K. Kidwell, On the structure of Selmer groups of p-ordinary modular forms over $\mathbf{Z}_p$-extensions. *J. Number Theory* **187** (2018), 296–331. Zbl 1403.11068 MR 3766913

[15] B. D. Kim, The Iwasawa invariants of the plus/minus Selmer groups. *Asian J. Math.* **13** (2009), no. 2, 181–190. Zbl 1268.11078 MR 2559107

[16] B. D. Kim, The plus/minus Selmer groups for supersingular primes. *J. Aust. Math. Soc.* **95** (2013), no. 2, 189–200. Zbl 1291.11094 MR 3142355

[17] B. D. Kim, 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. Zbl 1405.11145 MR 3715241

[18] T. Kitajima – R. Otsuki, On the plus and the minus Selmer groups for elliptic curves at supersingular primes. *Tokyo J. Math.* **41** (2018), no. 1, 273–303. Zbl 1411.11106 MR 3830819

[19] S.-i. Kobayashi, Iwasawa theory for elliptic curves at supersingular primes. *Invent. Math.* **152** (2003), no. 1, 1–36. Zbl 1047.11105 MR 1965358

[20] A. Lei – D. Loeffler – S. L. Zerbes, Wach modules and Iwasawa theory for modular forms. *Asian J. Math.* **14** (2010), no. 4, 475–528. Zbl 1281.11095 MR 2774276

[21] A. Lei – R. Sujatha, On Selmer groups in the supersingular reduction case. *Tokyo J. Math.* **43** (2020), no. 2, 455–479. Zbl 1465.11213 MR 4185844

[22] M. F. Lim – R. Sujatha, Fine Selmer groups of congruent Galois representations. *J. Number Theory* **187** (2018), 66–91. Zbl 1430.11148 MR 3766902

[23] M. F. Lim – R. Sujatha, On the structure of fine Selmer groups and Selmer groups of CM elliptic curves. In *Proceedings of Ropar Conference in honour of Srinivasa Ramanujan*, pp. 1–22, Ramanujan Math. Soc. Lect. Notes Ser. 26, Ramanujan Mathematical Society, Mysore, 2019.

[24] The LMFDB Collaboration, The L-functions and modular forms database. http://www.lmfdb.org, 2013 (accessed 31 October 2019).

[25] B. Mazur, Rational points of abelian varieties with values in towers of number fields. *Invent. Math.* **18** (1972), 183–266. Zbl 0245.14015 MR 444670

[26] J. Neukirch – A. Schmidt – K. Wingberg, *Cohomology of number fields*. Second edn., Grundlehren Math. Wiss. 323, Springer, Berlin, 2008. Zbl 1136.11001 MR 2392026

[27] B. Perrin-Riou, Théorie d'Iwasawa p-adique locale et globale. *Invent. Math.* **99** (1990), no. 2, 247–292. Zbl 0715.11030 MR 1031902

[28] B. Perrin-Riou, Théorie d'Iwasawa et hauteurs p-adiques. *Invent. Math.* **109** (1992), no. 1, 137–185. Zbl 0781.14013 MR 1168369

[29] B. Perrin-Riou, Fonctions L p-adiques des représentations p-adiques. *Astérisque* (1995), no. 229. Zbl 0845.11040 MR 1327803

[30] R. Pollack, On the p-adic L-function of a modular form at a supersingular prime. *Duke Math. J.* **118** (2003), no. 3, 523–558. Zbl 1074.11061 MR 1983040

[31] M. Raynaud, Schémas en groupes de type $(p, \dots, p)$. *Bull. Soc. Math. France* **102** (1974), 241–280. Zbl 0325.14020 MR 419467

[32] K. Rubin – A. Silverberg, Families of elliptic curves with constant mod p representations. In *Elliptic curves, modular forms, & Fermat's last theorem* (Hong Kong, 1993), pp. 148–161, Ser. Number Theory 1, International Press, Cambridge, MA, 1995. Zbl 0856.11027 MR 1363500

[33] P. Schneider, p-adic height pairings. II. *Invent. Math.* **79** (1985), no. 2, 329–374. Zbl 0571.14021 MR 778132

[34] J.-P. Serre, *Cohomologie galoisienne*. Fifth edn., Lecture Notes in Math. 5, Springer, Berlin, 1994. Zbl 0812.12002 MR 1324577

[35] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*. Grad. Texts in Math. 151, Springer, New York, 1994. Zbl 0911.14015 MR 1312368

[36] F. E. I. Sprung, Iwasawa theory for elliptic curves at supersingular primes: a pair of main conjectures. *J. Number Theory* **132** (2012), no. 7, 1483–1506. Zbl 1284.11147 MR 2903167

[37] R. Sujatha, Elliptic curves and Iwasawa's $\mu = 0$ conjecture. In *Quadratic forms, linear algebraic groups, and cohomology*, pp. 125–135, Dev. Math. 18, Springer, New York, 2010. Zbl 1232.11116 MR 2648723

Manoscritto pervenuto in redazione il 16 luglio 2020.