B. Forrás, K. Müller *Res. Number Theory (2025)11:56*
https://doi.org/10.1007/s40993-025-00635-9

Research in Number Theory

RESEARCH

On the cohomology of plus/minus Selmer groups of supersingular elliptic curves in weakly ramified base fields

Ben Forrás* and Katharina Müller

*Correspondence:
ben.forras@unibw.de
Institut für Theoretische Informatik, Mathematik und Operations Research, Universität der Bundeswehr München, Werner-Heisenberg-Weg 39, Neubiberg 85577, Germany

Abstract

Let $E/\mathbb{Q}$ be an elliptic curve and let $p \geq 5$ be a prime of good supersingular reduction. We generalize results due to Meng Fai Lim proving Kida's formula and integrality results for characteristic elements of signed Selmer groups along the cyclotomic $\mathbb{Z}_p$-extension of weakly ramified base fields $K/\mathbb{Q}_p$.

1 Introduction

The Iwasawa theory of elliptic curves at good supersingular primes with $a_p = 0$ was initiated by Kobayashi in his seminal work [29], where $a_p = 1 + p - |\widetilde{E}(\mathbb{F}_p)|$, and $|\widetilde{E}(\mathbb{F}_p)|$ is the the number of points in the reduction of the curve modulo p. Working with the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$, he defined plus/minus norm subgroups as well as a corresponding signed Selmer group, and used Coleman theory to prove that it is cotorsion over the Iwasawa algebra. This involved writing down an explicit power series, and using Honda theory to associate with it a formal group law which turns out to be isomorphic to the formal group of the elliptic curve. Crucially, this formal group law has no p-torsion over the cyclotomic tower. Moreover, one can explicitly construct a norm coherent sequence of points along the tower generating the corresponding even/odd norm subgroups.

This strategy was generalised, first by Iovita–Pollack [22] to extensions of $\mathbb{Q}$ where p splits completely, then by Kim to extensions of $\mathbb{Q}$ with p unramified [25,27]. Torsion properties and finite submodules of the Pontryagin dual of the signed Selmer groups were further studied by Kitajima–Otsuki [28] and Lei–Lim [31], among others.

In a recent work, Lim [30] established cohomological triviality of the plus/minus subgroups, studied projectivity of signed Selmer groups, and used these results to deduce a Kida formula as well as to prove an integrality result for characteristic elements for the Pontryagin dual of signed Selmer groups. The aim of this paper is to generalise these results by allowing tame ramification at supersingular primes under certain assumptions.

Before we state our main results, let us fix some notation. Let p be an odd rational prime, $F/F'/\mathbb{Q}$ number fields with p splitting completely in F', K/F a finite Galois extension. Let K_∞/K by the cyclotomic $\mathbb{Z}_p$-extension. Let $G := \mathrm{Gal}(K_\infty/F_\infty)$ and $\Gamma := \mathrm{Gal}(F_\infty/F)$.

© The Author(s) 2025. This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

Then we have an isomorphism $\mathcal{G} := \mathrm{Gal}(K_\infty/F) = G \rtimes \Gamma$. We fix once and for all a lift Γ' of Γ in $\mathcal{G}$ such that the restriction induces an isomorphism $\Gamma' \cong \Gamma$ (not necessarily $\mathrm{Gal}(K_\infty/K)$). By abuse of notation we denote Γ' by Γ. Let $\Lambda := \mathbb{Z}_p[\![\Gamma]\!]$ and $\Lambda(\mathcal{G}) := \mathbb{Z}_p[\![\mathcal{G}]\!]$ be the relevant Iwasawa algebras. Recall that a finite Galois extension of local fields is called weakly ramified if its second ramification group vanishes—so wild ramification is allowed, but only in the first ramification group. Let E/F' be an elliptic curve satisfying the following assumptions:

(S1) E has good reduction at all p-adic places of F';
(S2) there is a p-adic place with supersingular reduction;
(S3) each p-adic supersingular place u
  (i) has ramification index $e_u(K/F')$ that is not divisible by $p^2 - 1$ in K/F',
  (ii) fulfills the following condition: K_u is contained in the compositum of an at most weakly ramified extension $\mathcal{K}'/\mathbb{Q}_p$ and the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_{p,\infty}$, such that $\mathcal{K}'$ does not intersect the cyclotomic extension $\mathbb{Q}_{p,\infty}$,
  (iii) satisfies $a_u = 0$, where $a_u = 1 + p - |\widetilde{E}_u(\mathbb{F}_p)|$ and $\widetilde{E}_u$ is the reduction of E at u.

Furthermore, we fix a finite set of places Σ of F subject to certain standard conditions, as well as a subset $\Sigma' \subset \Sigma$ consisting only of some non-p-adic places. Let $\vec{s}$ be a tuple consisting of a sign in $\{+,-\}$ for each p-adic supersingular place in Σ. Analogously to the works cited above, we may define signed Selmer groups $\mathrm{Sel}^{\vec{s}}(E/K_\infty)$ as well as non-primitive versions $\mathrm{Sel}^{\vec{s}}_{\Sigma'}(E/K_\infty)$ thereof; for the precise definitions, we refer to Sections 4.1 and 4.4.

Our first main result is the following:

Theorem (Kida formula, Theorem 6.3) *Assume that* $\mathrm{Sel}^{\vec{s}}(E/K_\infty)$ *is* Λ*-cotorsion and that* $\theta(X^{\vec{s}}(E/K_\infty)) \leq 1$. *Let* $P_1 \subset \Sigma'$ *be the primes where* E *has split multiplicative reduction and let* P_2 *be the set of primes in* Σ' *where* E *has good reduction and* $E(K)[p] \neq 0$.

Let L *be a number field contained in* K *such that the extensions* L/F *and* K/F *satisfy conditions (S1)–(S3) above, and such that* K/L *is Galois and* $\mathrm{Gal}(K/L)$ *is a p-group.*

Then the Iwasawa λ*- resp.* μ*-invariants of the* Λ*-modules* $X^{\vec{s}}(E/K_\infty)$ *and* $X^{\vec{s}}(E/L_\infty)$ *are related as follows:*

$$\lambda\left(X^{\vec{s}}(E/K_\infty)\right) = [K_\infty : L_\infty]\lambda\left(X^{\vec{s}}(E/L_\infty)\right) + \sum_{v\in P_1}(e_v - 1) + 2\sum_{w\in P_2}(e_v - 1),$$

$$\mu\left(X^{\vec{s}}(E/K_\infty)\right) = [K_\infty : L_\infty]\mu\left(X^{\vec{s}}(E/L_\infty)\right).$$

Here $\theta(X^{\vec{s}}(E/K_\infty))$ denotes the largest exponent in the standard decomposition of the maximal p-power-torsion submodule of $X^{\vec{s}}(E/K_\infty)$, that is, if $X^{\vec{s}}(E/K_\infty)[p^\infty] \to \bigoplus_{i\in I}\Lambda/p^{m_i}\Lambda$ is a pseudo-isomorphism, then $\theta(X^{\vec{s}}(E/K_\infty)[p^\infty]) := \max\{m_i : i \in I\}$. The proof of this Kida formula is by calculating certain Herbrand quotients: this is a method due to Iwasawa [23, §9]. The method was used by Hachimori–Matsuno [20] to prove a Kida formula for elliptic curves with good ordinary reduction and $\mu = 0$. The weakening of the $\mu = 0$ assumption to $\theta \leq 1$ above is along the lines of Hachimori–Sharifi's Kida formula for CM fields [21]. Our result is a direct generalisation of Lim's Kida formula [30, Proposition 5.2].

We come to our second main result. Let Γ_0 be an open subgroup of Γ that is central in $\mathcal{G}$. Recall that an ordinary p-adic place v of F is called non-anomalous if for all places w of

K above v, we have $p \nmid |\widetilde{E}(k_w)|$, where k_w is the residue field of the local field K_w, and $\widetilde{E}$ is the reduction of E.

Theorem (Integrality of characteristic elements, Theorem 7.1) *Suppose that Σ' contains all non-p-adic places in Σ whose inertia degree in K/F is divisible by p. Further suppose that $X^{\vec{s}}(E/K_\infty)$ is Λ-torsion, and that every ordinary p-adic place is either non-anomalous or ramifies tamely in K/F. Then there exists a characteristic element $\xi_{E,\Sigma'}$ of $X^{\vec{s}}_{\Sigma'}(E/K_\infty)$. For every graduated $\Lambda(\Gamma_0)$-order $\mathfrak{M}$ of $\mathcal{Q}(\mathcal{G})$ containing $\Lambda(\mathcal{G})$, the characteristic element $\xi_{E,\Sigma'}$ is in the image of the natural map $\mathfrak{M} \cap \mathcal{Q}(\mathcal{G})^\times \to K_1(\mathcal{Q}(\mathcal{G}))$.*

Graduated orders constitute a generalisation of maximal orders; the precise definition will be recalled in Sect. 7. The characteristic elements above are essential for the main conjecture of Coates et al. [5]. An integrality result for maximal orders was established by Nichifor–Palvannan [36, §5] for elliptic curves with good ordinary or split multiplicative reduction admitting a cyclic isogeny of order p^2. They also developed an algebraic tool for studying characteristic elements of $\Lambda(\mathcal{G})$-modules admitting a projective resolution of length 1 in the case when $\mathcal{G}$ is a direct product of Γ and a finite group; this method was generalised to semidirect products by the first named author in [9,11].

In the process of establishing the results above, we make extensive use of the properties of p-torsion freeness and cohomological triviality mentioned above, which are easy consequences of our assumptions (S1–S3). An important distinction between the present article and preexisting work is that we don't have access to a norm compatible system of points, as these are only known to exist in the unramified setting. While the outline of our proofs rely heavily on the work of Lim in the unramified case, our computation of the relevant cohomology groups is a more laborious endeavour. Indeed, if $\mathcal{K}/\mathbb{Q}_p$ is a finite unramified extension with cyclotomic $\mathbb{Z}_p$-extension $\mathcal{K}_\infty$, then the existence of a norm coherent sequence gives rise to a short exact sequence $\widehat{E}(\mathcal{K}) \hookrightarrow \widehat{E}^+(\mathcal{K}_\infty) \oplus \widehat{E}^-(\mathcal{K}_\infty) \twoheadrightarrow \widehat{E}(\mathcal{K}_\infty)$, whereas we make no claim of such a sequence existing, and compute the relevant cohomology groups by studying the module-theoretic properties of certain plus/minus Iwasawa cohomology groups. Note that there is no apparent way of directly generalising the construction of norm coherent points to the ramified setting. Indeed, using Kobayashi's approach would involve Honda theory, which requires working over an unramified extension. On the other hand, lifting a norm coherent sequence from the cyclotomic tower over an unramified extension to a ramified extension thereof would not preserve the desired norm relations.

We remark that recently, Kataoka has constructed a framework for deriving Kida formulæ via Selmer complexes [24]. This differs from the present work in its setting: indeed, §4.5 of op.cit. treats supersingular elliptic curves for abelian extensions only, whereas §5.2 of op.cit. treats some non-abelian cases, but only for λ-invariants. It would be interesting to see if the results of the present article can be interpreted in Kataoka's framework.

It is a natural question to ask whether our results could be generalised to modular forms. Indeed, several elements of the theory recalled above, such as Coleman maps, have been constructed for modular forms by Lei–Loeffler–Zerbes [32] using p-adic Hodge theory and Wach modules, with the relationship to Kobayashi's signed Selmer groups explained in [33].

The paper is structured as follows. Section 2 consists of a collection of general facts related to Galois cohomology. We treat local cohomology groups in Sect. 3. In Sect. 4,

we define signed Selmer groups in the above setting, and study torsion properties as well as finite submodules of their Pontryagin duals. We establish projectivity results in Sect. 5. The Kida formula and the integrality result stated above are proven in Sects. 6 and 7, respectively. Finally in Sect. 8, we study the relationship between the Iwasawa invariants of elliptic curves whose p-torsion points are isomorphic as Galois modules.

2 Preliminaries on Galois cohomology

Let $\mathcal{G} := G \rtimes \Gamma$, where $\Gamma \cong \mathbb{Z}_p$ and G is a finite group. We fix once and for all a lift Γ' of Γ in $\mathcal{G}$ such that $\Gamma' \cong \Gamma$ by restriction. Let M be a $\mathbb{Z}_p[\![\mathcal{G}]\!]$-module. Note that the action of $\mathcal{G}$ on M_G factors through Γ and coincides with the action of Γ'. By abuse of notation we will frequently write Γ instead of Γ'. Let $\Lambda := \mathbb{Z}_p[\![\Gamma]\!]$ and $\Lambda(\mathcal{G}) := \mathbb{Z}_p[\![\mathcal{G}]\!]$. If G is a cyclic group and M is a G-module with finite cohomology groups, we write $h_G(M) := |H^2(G, M)|/|H^1(G, M)|$ for the Herbrand quotient.

Lemma 2.1 *Assume that M is an $\mathbb{F}_p[G]$-module and that G is a cyclic p-group. Assume furthermore that $H^i(G, M)$ is finite for all $i \geq 1$. Then the Herbrand quotient $h_G(M)$ is trivial.*

Proof This is a straightforward generalization of [21, Lemma 2.2].

For a finitely generated Λ-module M, let $\theta(M)$ denote the largest exponent in the standard decomposition of the maximal p-power-torsion submodule $M[p^\infty]$ of M up to pseudo-isomorphism. In formulæ: there is a pseudo-isomorphism $M[p^\infty] \to \bigoplus_{i\in I} \Lambda/p^{m_i}\Lambda$, and $\theta(M) = \max\{m_i : i \in I\}$.

Lemma 2.2 *Assume that G is a cyclic p-group. Let M be a finitely generated $\Lambda(\mathcal{G})$-module that is torsion as a Λ-module. Assume that $H^i(G, M)$ is finitely generated over $\mathbb{Z}_p$ for all $i \geq 1$ and that $\theta(M) \leq 1$. Then $h_G(M[p^\infty]) = 1$ and $\mu(M) = |G|\mu(M_G)$.*

Proof This is basically [21, Lemma 2.4], but there it's assumed that the actions of Γ and G commute. Consider the short exact sequence

$$0 \to M[p^\infty] \to M \to Z \to 0,$$

where Z is $\mathbb{Z}_p$-free and finitely generated over $\mathbb{Z}_p$. Taking cohomology with respect to G, and using that $H^i(G, Z)$ is finitely generated over $\mathbb{Z}_p$ for all i, we obtain that $H^i(G, M[p^\infty])$ is finitely generated over $\mathbb{Z}_p$ for all $i \geq 1$. As $\theta(M) \leq 1$, we see that the natural map $M[p^\infty] \to M[p^\infty]/pM[p^\infty]$ is actually a surjective pseudo-isomorphism. Therefore $h_G(M[p^\infty]) = h_G(M[p^\infty]/pM[p^\infty])$, and $H^i(G, M[p^\infty]/pM[p^\infty]))$ is finitely generated over $\mathbb{Z}_p$ for all $i \geq 1$. This implies that $H^i(G, M[p^\infty]/pM[p^\infty])$ is finite for all $i \geq 1$, and Lemma 2.1 shows that $h_G(M[p^\infty]/pM[p^\infty]) = 1$.

It remains to show the claim on μ-invariants. As $H^i(G, M[p^\infty]/pM[p^\infty])$ is finite for all $i \geq 1$, we see that the three modules $(M[p^\infty]/pM[p^\infty])_G$, $(M[p^\infty]/pM[p^\infty])^G$ and $N_G(M[p^\infty]/pM[p^\infty])$ are pseudo-isomorphic as Λ-modules, where $N_G := \sum_{g\in G} g \in \mathbb{Z}_p[G]$. In particular, they have the same μ-invariant. Let τ be a generator of G, and let $I_G := \Lambda(\mathcal{G})(\tau - 1)$. As G is a normal subgroup of $\mathcal{G}$, the ideal I_G^k is generated by $(\tau - 1)^k$. The μ-invariant can then be expressed as the sum of the μ-invariants of the quotients in the filtration induced by I_G. Each μ-invariant in this sum can be estimated from below by

the μ-invariant in the last module in the filtration:

$$\begin{aligned}\mu(M) = \mu(M[p^\infty]/pM[p^\infty]) &= \sum_{k=0}^{|G|-1} \mu\big(I_G^k(M[p^\infty]/pM[p^\infty])\big/I_G^{k+1}\big(M[p^\infty]/pM[p^\infty]\big)\\ &\geq |G|\cdot\mu\Big(I_G^{|G|-1}(M[p^\infty]/pM[p^\infty])\Big) = |G|\cdot\mu\big(N_G(M[p^\infty]/pM[p^\infty])\big)\\ &= |G|\cdot\mu\big((M[p^\infty]/pM[p^\infty])_G\big) = |G|\cdot\mu(M_G).\end{aligned}$$

The last equality follows from the fact that $\theta(M_G) \leq 1$. Thus, $\mu(M_G) = \mu(M_G/pM_G)$. Furthermore, $M_G/pM_G \cong M/(\tau-1,p)M \cong (M/pM)_G$. We have an exact sequence

$$Z^G \to (M[p^\infty]/pM[p^\infty])_G \to (M/pM)_G \to (Z/pZ)_G.$$

The first and last term are finite. Therefore, $\mu((M/pM)_G) = \mu((M[p^\infty]/pM[p^\infty])_G)$.

On the other hand, $\big(M[p^\infty]/pM[p^\infty]\big)\big/\big(I_G(M[p^\infty]/pM[p^\infty])\big)$ surjects onto $N_G\big(M[p^\infty]/pM[p^\infty]\big)$ with finite kernel. Once again writing $\mu(M)$ as a sum, each summand can therefore be estimated from above:

$$\begin{aligned}\mu(M) = \mu\big(M[p^\infty]/pM[p^\infty]\big) &= \sum_{k=0}^{|G|-1} \mu\big(I_G^k(M[p^\infty]/pM[p^\infty])\big/I_G^{k+1}(M[p^\infty]/pM[p^\infty])\big)\\ &\leq |G|\cdot\mu\big(N_G(M[p^\infty]/pM[p^\infty])\big) = |G|\cdot\mu\big((M[p^\infty]/pM[p^\infty])_G\big) = |G|\cdot\mu(M_G).\end{aligned}$$

We obtain the desired equality. □

Lemma 2.3 *Let E be an elliptic curve over $\mathbb{Q}_p$ that is supersingular at p. Let $\mathcal{K}/\mathbb{Q}_p$ be a finite extension and $\mathcal{K}_\infty$ its cyclotomic $\mathbb{Z}_p$-extension, and assume that for all $n \geq 0$, the group $E(\mathcal{K}_n)$ has no p-torsion. Then*

$$H^1(\mathcal{K}_\infty, E[p^\infty]) = E(\mathcal{K}_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p.$$

Later on, we will assume $a_p = 0$; note that for $p \geq 5$, this already follows from $p \mid a_p$ by the Hasse bound. In our applications of the Lemma, the p-torsion freeness assumption will be satisfied by Lemma 3.1.

Proof Let k be the residue field of $\mathcal{K}$. As E is a supersingular elliptic curve, p-rank$(E(k)) = 0$, where the p-rank is defined as in [40]. It follows from [40, Theorem 2] that the group of universal norms $\bigcap_n N_{\mathcal{K}_n/\mathcal{K}}(E(\mathcal{K}_n))$ is trivial. In particular, local duality [34, I.3.4] implies that

$$H^1(\mathcal{K}_\infty, E)[p^\infty] = \varinjlim_n H^1(\mathcal{K}_n, E)[p^\infty] = \mathrm{Hom}\left(\varprojlim_n E(\mathcal{K}_n), \mathbb{Q}_p/\mathbb{Z}_p\right) = 0,$$

which in turn implies that $H^1(\mathcal{K}_\infty, E[p^\infty]) = E(\mathcal{K}_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p$. □

Recall that a finitely generated $\mathbb{Z}_p[G]$-module is called strictly quasi-projective if it admits a pseudo-isomorphism $X \to Y$ to a projective $\mathbb{Z}_p[G]$-module Y. A finitely generated $\mathbb{Z}_p[G]$-module is called quasi-projective if there exist finitely generated strictly quasi-projective $\mathbb{Z}_p[G]$-modules X_1, X_2 such that there is an exact sequence $0 \to X_1 \to X_2 \to X \to 0$ of $\mathbb{Z}_p[G]$-modules.

Let Q be a finite cyclic group of order coprime to p. Let $\mathbb{Q}_p(\mu_{|Q|})$ denote the field obtained by adjoining all roots of unity of order $|Q|$ to $\mathbb{Q}_p$, and let $\mathcal{O}_{\mathbb{Q}_p(\mu_{|Q|})}$ denote its ring of integers. For a (necessarily 1-dimensional) character ε of Q, we have an associated idempotent

$$e(\varepsilon) = |Q|^{-1} \sum_{q \in Q} \varepsilon(q^{-1}) q \in \mathcal{O}_{\mathbb{Q}_p(\mu_{|Q|})}[Q].$$

If X is a finitely generated $\mathbb{Z}_p[G]$-module and $Q \leq G$ is a finite cyclic subgroup of order coprime to p, then the ε-component of X is defined as $X^\varepsilon := e(\varepsilon)(X \otimes_{\mathbb{Z}_p} \mathcal{O}_{\mathbb{Q}_p(\mu_{|Q|})})$. We similarly define the ε-component of the Pontryagin dual $S = X^\vee = \mathrm{Hom}(X, \mathbb{Q}_p/\mathbb{Z}_p)$ by $S^\varepsilon := e(\varepsilon)(S \otimes_{\mathbb{Z}_p} \mathcal{O}_{\mathbb{Q}_p(\mu_{|Q|})})$.

Proposition 2.4 *Let S be a discrete $\Lambda(\mathcal{G})$-module, and let X be its Pontryagin dual. Assume that X is finitely generated and torsion over Λ, and that $\theta(X) \leq 1$. Suppose that for all cyclic subgroups $C = PQ$ of G, where P is a p-group and Q has order coprime to p, the cohomology groups $H^i(P, X)$ are finite for all $i \geq 1$, and $h_P(S^\varepsilon) = 1$ for all (one-dimensional) characters ε of Q. Then $X/X[p]$ is quasi-projective as $\mathbb{Z}_p[G]$-module.*

Proof This is [12, Proposition 2.2.1] in the case that G commutes with Γ. The only place where this assumption is used is while proving $h_P(S^\varepsilon) = h_P(pS^\varepsilon)$. We now prove this without assuming that G and Γ commute.

Let $M := S[p]^\varepsilon$. Then M is a $\mathbb{F}_p[G]$-module and $M^\vee = X^\varepsilon/pX^\varepsilon$. As $\theta(X) \leq 1$, the module pX is finitely generated over $\mathbb{Z}_p$. We have a long exact sequence

$$\ldots \to H^i(P, X^\varepsilon) \to H^i(P, X^\varepsilon/pX^\varepsilon) \to H^{i+1}(P, pX^\varepsilon) \to \ldots$$

The first and the last term are finitely generated over $\mathbb{Z}_p$ for all $i \geq 1$. Thus the middle term is finite for all $i \geq 1$. We can now apply Lemma 2.1 to conclude that $1 = h_P(M^\vee) = h_P(M)^{-1}$, which in turn implies that $1 = h_P(S^\varepsilon) = h_P(pS^\varepsilon)$ as desired. □

For a local field $\mathcal{K}$, we write $\mathcal{O}_\mathcal{K}$ resp. $m_\mathcal{K}$ for its ring of integers resp. maximal ideal. If $\mathcal{L}/\mathcal{K}$ is a finite Galois extension of local fields, and $\mathfrak{F}$ is a formal group defined over $\mathcal{O}_\mathcal{K}$, we let $\mathrm{Tr}^\mathfrak{F} : \mathfrak{F}(m_\mathcal{L}) \to \mathfrak{F}(m_\mathcal{K})$ denote the norm with respect to $\mathfrak{F}$, as defined in [16, 2.2.3]. In the following special case, the $\mathfrak{F}$-norm is surjective:

Proposition 2.5 *Let $\mathcal{L}/\mathcal{K}$ be a cyclic extension of local fields, and let $\mathfrak{F}$ be a formal group defined over $\mathcal{O}_\mathcal{K}$ of height at least 2. Let t be the last ramification jump (i.e. $G_t \neq 1$ and $G_{t+1} = 1$), and assume that $t \leq 1$ (i.e. $\mathcal{L}/\mathcal{K}$ is at most weakly ramified). Then $\mathfrak{F}(m_\mathcal{K}) = \mathrm{Tr}^\mathfrak{F}(\mathfrak{F}(m_\mathcal{L}))$.*

Proof It suffices to consider the case where $[\mathcal{L} : \mathcal{K}] = \ell$ is a prime. If $\mathcal{L}/\mathcal{K}$ is at most tamely ramified, this is handled in [7, Proposition 3.10]. Thus we will assume $t = 1$ for the rest of the proof.

By [7, Proposition 3.5], for every $n \geq 1$ there are well defined maps

$$\alpha_n \colon \mathfrak{F}\left(m_\mathcal{L}^{\psi(n)}\right) \Big/ \mathfrak{F}\left(m_\mathcal{L}^{\psi(n)+1}\right) \to \mathfrak{F}\left(m_\mathcal{K}^{n}\right) \Big/ \mathfrak{F}\left(m_\mathcal{K}^{n+1}\right)$$

where ψ is as in [41, IV§3]. It follows from [7, Corollary 3.6] that these maps are isomorphisms for $n \geq t+1$. We want to show that it is also an isomorphism for $n = t = 1$; . So assume $t = 1$. By [16, Corollary 2.4.2], there are coefficients $a_i \in \mathcal{O}_\mathcal{K}$ such that

$$\mathrm{Tr}^{\mathfrak{F}}(x) \equiv \mathrm{Tr}(x) + \sum_{i=1}^{\infty} a_i \mathrm{Nm}(x)^i \pmod{\mathrm{Tr}(x^2)}$$

and the coefficient a_1 has positive valuation as $\mathfrak{F}$ has height at least 2; Hazewinkel's result is valid in the case $\ell = p$, which is the case for $t = 1$. It follows that α_n is surjective for $n = 1$ if and only if $\mathrm{Tr}_{\mathcal{L}/\mathcal{K}}(m_\mathcal{L}) = m_\mathcal{K}$. By [41, V§3, Lemma 4], this is always the case if

$$2 > \frac{2(\ell-1)+1}{\ell} \geq 1,$$

This chain of inequalities is trivially true and the map α_n is an isomorphism for all $n \geq 1$. Now [41, V§1, Lemma 2] implies the desired claim for $t = 0$ and for $t = 1$. □

Corollary 2.6 *Keep the assumptions of Proposition 2.5. Then* $H^i(\mathrm{Gal}(\mathcal{L}/\mathcal{K}), \mathfrak{F}(m_\mathcal{L})) = 0$ *for all* $i > 0$.

Proof Let $H := \mathrm{Gal}(\mathcal{L}/\mathcal{K})$, and let $\widehat{H}^i(H, \mathfrak{F}(m_\mathcal{L}))$ denote the Tate cohomology groups. By Proposition 2.5, we know that $\widehat{H}^0(H, \mathfrak{F}(m_\mathcal{L})) = 0$. By [7, Lemma 3.9], the Herbrand quotient of $\mathfrak{F}(m_\mathcal{L})$ vanishes. Thus, $\widehat{H}^i(H, \mathfrak{F}(m_\mathcal{L})) = 0$ for all i, which implies the desired claim. □

Remark 2.7 For determining whether an extension is weakly ramified, one may use Hilbert's formula [41, IV§1, Proposition 4]. This states that if $\mathcal{L}/\mathcal{K}$ is a Galois extension of local fields, and v denotes the valuation on L, then the different $\mathfrak{D}_{\mathcal{L}/\mathcal{K}}$ has valuation

$$v(\mathfrak{D}_{L/K}) = \sum_{i=0}^{\infty} (|G_i| - 1),$$

where G_i are the higher ramification groups (in lower numbering). In particular, a totally ramified extension of degree p resp. p^2 is weakly ramified if and only if $v(\mathfrak{D}_{L/K}) = 2p-2$ resp. $2p^2-2$.

Lemma 2.8 *Let* $\mathcal{L}/\mathcal{K}$ *and* $\mathcal{K}'/\mathcal{K}$ *be Galois extensions of local fields of degree* $[\mathcal{L} : \mathcal{K}] = [\mathcal{K}' : \mathcal{K}] = p$. *Assume that* $\mathcal{L} \cap \mathcal{K}' = \mathcal{K}$ *and that* $\mathcal{L}/\mathcal{K}$ *is weakly ramified. Then* $\mathcal{L}\mathcal{K}'/\mathcal{K}'$ *is weakly ramified.*

Proof If $\mathcal{L}\mathcal{K}'/\mathcal{K}$ is at most weakly ramified, there is nothing to prove. It remains to treat the case when $\mathcal{K}'\mathcal{L}/\mathcal{K}$ is totally but not weakly ramified. Let v be the valuation on $\mathcal{K}'\mathcal{L}$. As $\mathcal{K}'\mathcal{L}/\mathcal{K}$ is a $(\mathbb{Z}/p\mathbb{Z})^2$-extension that is not weakly ramified, Remark 2.7 yields

$$2p^2 - 2 \neq v(\mathfrak{D}_{\mathcal{L}\mathcal{K}'/\mathcal{K}}) = v(\mathfrak{D}_{\mathcal{L}\mathcal{K}'/\mathcal{L}}) + v(\mathfrak{D}_{\mathcal{L}/\mathcal{K}}) = v(\mathfrak{D}_{\mathcal{K}'\mathcal{L}/\mathcal{L}}) + p(2p-2).$$

It follows that $v(\mathfrak{D}_{\mathcal{K}'\mathcal{L}/\mathcal{L}}) \neq 2p-2$. In particular, $\mathcal{K}'\mathcal{L}/\mathcal{L}$ is not weakly ramified by Remark 2.7. By [35, Theorem 10.7] and the fact that $\mathcal{L}/\mathcal{K}$ is weakly ramified, we obtain

$$1 = G_2(\mathcal{L}/\mathcal{K}) = G_2(\mathcal{L}\mathcal{K}'/\mathcal{K})\mathrm{Gal}(\mathcal{L}\mathcal{K}'/\mathcal{L})/\mathrm{Gal}(\mathcal{L}\mathcal{K}'/\mathcal{L}).$$

This implies $G_2(\mathcal{L}\mathcal{K}'/\mathcal{K}) = \mathrm{Gal}(\mathcal{L}\mathcal{K}'/\mathcal{L})$. By [35, Theorem 10.3] we obtain

$$G_2(\mathcal{L}\mathcal{K}'/\mathcal{K}') = G_2(\mathcal{L}\mathcal{K}'/\mathcal{K}) \cap \mathrm{Gal}(\mathcal{L}\mathcal{K}'/\mathcal{K}') = \mathrm{Gal}(\mathcal{L}\mathcal{K}'/\mathcal{L}) \cap \mathrm{Gal}(\mathcal{L}\mathcal{K}'/\mathcal{K}') = \{0\},$$

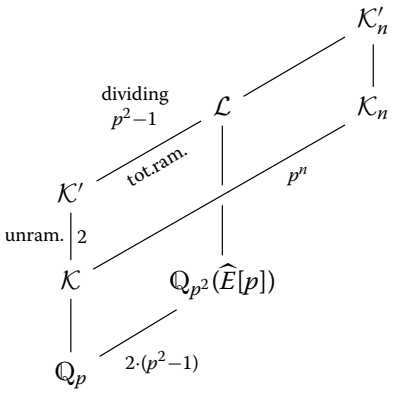
as claimed. □

3 Local considerations

Let $E/\mathbb{Q}_p$ be an elliptic curve with good supersingular reduction and $a_p = 0$, and let $\widehat{E}$ denote the formal group associated with E. Let $\mathcal{K}/\mathbb{Q}_p$ be a finite extension with ramification index $e(\mathcal{K}/\mathbb{Q}_p)$ not divisible by $p^2 - 1$. Let $\mathcal{K}_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathcal{K}$ and let $\mathcal{K}_n$ be the intermediate field of degree p^n over $\mathcal{K}$.

Lemma 3.1 *If $p^2 - 1 \nmid e(\mathcal{K}/\mathbb{Q}_p)$, then for all $n \geq 0$, the group $\widehat{E}(\mathcal{K}_n)$ is p-torsion free. In particular, $E(\mathcal{K}_n)$ is also p-torsion free.*

Proof Let $\mathcal{K}'$ be the unramified quadratic extension of $\mathcal{K}$, and let $\mathcal{K}'_n := \mathcal{K}_n\mathcal{K}'$. Assume that $\widehat{E}(\mathcal{K}'_n)[p] \neq 0$. Recall from the proof of [29, Proposition 8.7] that this implies that $\mathcal{K}'_n$ contains all p-torsion points. In particular, $\mathcal{K}'_n$ contains $\mathcal{L} := \mathcal{K}'(\widehat{E}[p])$.



Let $\mathbb{Q}_{p^2}$ be the unique unramified extension of $\mathbb{Q}_p$ of degree 2. As $\mathbb{Q}_{p^2}(\widehat{E}[p])/\mathbb{Q}_{p^2}$ is a totally ramified extension of degree $p^2 - 1$, it follows that $p^2 - 1 \mid e(\mathcal{K}'_n/\mathcal{K}')e(\mathcal{K}'/\mathbb{Q}_p)$. The first factor is a power of p and the second one is equal to $e(\mathcal{K}/\mathbb{Q}_p)$. By assumption, $e(\mathcal{K}/\mathbb{Q}_p)$ is not divisible by $p^2 - 1$, yielding a contradiction, which shows that indeed $\widehat{E}(\mathcal{K}_n)[p] = 0$. The p-torsion freeness of $E(\mathcal{K}_n)$ follows by the same argument as in [30, Lemma 3.1]. □

Definition 3.2 For $n \geq 0$, we define the two subgroups of $\widehat{E}(\mathcal{K}_n)$:

$$\widehat{E}^+(\mathcal{K}_n) := \left\{x \in \widehat{E}(\mathcal{K}_n) \mid \mathrm{Tr}_{\mathcal{K}_n/\mathcal{K}_{m+1}}(x) \in \widehat{E}(\mathcal{K}_m), 2 \mid m, 0 \leq m \leq n-1\right\}$$

$$\widehat{E}^-(\mathcal{K}_n) := \left\{x \in \widehat{E}(\mathcal{K}_n) \mid \mathrm{Tr}_{\mathcal{K}_n/\mathcal{K}_{m+1}}(x) \in \widehat{E}(\mathcal{K}_m), 2 \nmid m, 0 \leq m \leq n-1\right\}$$

Fix a (non-canonical) topological generator γ of Γ, which gives rise to an isomorphism $\Lambda = \mathbb{Z}_p[\![\Gamma]\!] \xrightarrow{\sim} \mathbb{Z}_p[[X]]$ given by $\gamma \mapsto 1 + X$. For $n \geq 0$, let Φ_n be the p^n-th cyclotomic polynomial. We define

$$\omega_n^+(X) := X \prod_{\substack{1 \leq m \leq n \\ m \text{ even}}} \Phi_m(X+1), \quad \omega_n^-(X) := X \prod_{\substack{1 \leq m \leq n \\ m \text{ odd}}} \Phi_m(X+1).$$

Note that $\omega_n^+(X)\omega_n^-(X) = X\omega_n(X)$.

Lemma 3.3 *The group $\widehat{E}^+(\mathcal{K}_n) + \widehat{E}^-(\mathcal{K}_n)$ has finite index in $\widehat{E}(\mathcal{K}_n)$.*

Proof By the definitions we have

$$\widehat{E}(\mathcal{K}_n)[\omega_n^\pm] \subset \widehat{E}^\pm(\mathcal{K}_n). \tag{1}$$

As $\omega_n^+(X)$ and $\omega_n^-(X)/X$ are coprime in $\mathbb{Z}[X]$ and thus in $\mathbb{Z}_p[X]$, there exists a p-adic integer $c \in \mathbb{Z}_p$ and elements $a(X), b(X) \in \mathbb{Z}_p[X]$ such that

$$c = a(X) \cdot \omega_n^+(X) + b(X) \cdot \frac{\omega_n^-(X)}{X}.$$

Let $y \in \widehat{E}(\mathcal{K}_n)$. Multiplying by c, we get a decomposition

$$cy = a(X) \cdot \omega_n^+(X) \cdot y + b(X) \cdot \frac{\omega_n^-(X)}{X} \cdot y.$$

Write y^- resp. y^+ for the first resp. second term on the right hand side. By definition, we have $y^- \in \widehat{E}(\mathcal{K}_n)[\omega_n^-]$ and $y^+ \in \widehat{E}(\mathcal{K}_n)[\omega_n^+]$. Using (1), we obtain

$$cy \in \widehat{E}^+(\mathcal{K}_n) + \widehat{E}^-(\mathcal{K}_n).$$

As $\widehat{E}(\mathcal{K}_n)$ has finite rank, the lemma follows. □

Lemma 3.4 *If $p^2 - 1 \nmid e(\mathcal{K}/\mathbb{Q}_p)$, then $\widehat{E}(\mathcal{K}) = \widehat{E}^+(\mathcal{K}_n) \cap \widehat{E}^-(\mathcal{K}_n)$.*

Proof We may reproduce the first half of the proof in [29, Proposition 8.12]. Indeed, let $x \in \widehat{E}^+(\mathcal{K}_n) \cap \widehat{E}^-(\mathcal{K}_n)$. Distinguishing by parity, we show that for all $0 \le m \le n-1$, $x \in \widehat{E}(\mathcal{K}_m)$ implies $x \in \widehat{E}(\mathcal{K}_{m-1})$; since $\widehat{E}(\mathcal{K}_{-1}) = \widehat{E}(\mathcal{K})$, this clearly implies the assertion. We have $p^{n-m}x = \mathrm{Tr}_{\mathcal{K}_n/\mathcal{K}_m}(x) \in \widehat{E}(\mathcal{K}_{m-1})$, and thus for all $\sigma \in \mathrm{Gal}(\mathcal{K}_m/\mathcal{K}_{m-1})$ we have $p^{n-m}(\sigma(x) - x) = 0$, and now Lemma 3.1 shows $\sigma(x) = x$, that is, $x \in \widehat{E}(\mathcal{K}_{m-1})$. □

Corollary 3.5 *If $p^2 - 1 \nmid e(\mathcal{K}/\mathbb{Q}_p)$, then for all $n \ge 0$ we have*

$$\mathbb{Z}_p\text{-rank}(\widehat{E}^\pm(\mathcal{K}_n)) = [\mathcal{K} : \mathbb{Q}_p] \deg(\omega_n^\pm).$$

Proof We prove the claim by induction on n. If $n = 0$, we have $\widehat{E}^-(\mathcal{K}) = \widehat{E}(\mathcal{K}) = \widehat{E}^+(\mathcal{K})$, which is of rank $[\mathcal{K} : \mathbb{Q}_p]$. Let us now assume that the claim is proved for $n-1$ and that n is even (the case of odd n can be treated similarly). In this case $\widehat{E}^-(\mathcal{K}_n) = \widehat{E}^-(\mathcal{K}_{n-1})$ and $\omega_n^- = \omega_{n-1}^-$. Thus, for the minus sign there is nothing to prove. By Lemmas 3.3 and 3.4, we have

$$\begin{aligned}\mathbb{Z}_p\text{-rank}\left(\widehat{E}^+(\mathcal{K}_n)\right) &= [\mathcal{K}_n : \mathbb{Q}_p] - \mathbb{Z}_p\text{-rank}\left(\widehat{E}^-(\mathcal{K}_n)\right) + \mathbb{Z}_p\text{-rank}\left(\widehat{E}(\mathcal{K})\right) \\ &= [\mathcal{K} : \mathbb{Q}_p](p^n - \deg(\omega_n^-) + 1) = [\mathcal{K} : \mathbb{Q}_p] \deg(\omega_n^+),\end{aligned}$$

which proves the claim. □

3.1 Corank computations

Assume that $\mathcal{K}/\mathbb{Q}_p$ is Galois, at most weakly ramified and that $\mathcal{K}\cap\mathbb{Q}_{p,\infty}=\mathbb{Q}_p$. Let $\mathcal{F}\subset\mathcal{K}$ be a subfield $G=\mathrm{Gal}(\mathcal{K}_\infty/\mathcal{F}_\infty)$. Then $\mathrm{Gal}(\mathcal{K}_\infty/\mathcal{F})=\Gamma\times G$. Let $\Lambda=\mathbb{Z}_p[[\Gamma]]$.

Lemma 3.6 *If $p^2-1\nmid e(\mathcal{K}/\mathbb{Q}_p)$, then*

$$\Lambda\text{-corank}(E^{\pm}(\mathcal{K}_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p)\geq[\mathcal{K}:\mathbb{Q}_p].$$

Proof By Corollary 3.5 we have

$$\mathbb{Z}_p\text{-corank}(E^{\pm}(\mathcal{K}_n)\otimes\mathbb{Q}_p/\mathbb{Z}_p)=\left(1+\sum_{\substack{k=1\\ k\text{ even/odd}}}^{p^n}\varphi(p^k)\right)[\mathcal{K}:\mathbb{Q}_p].$$

As $E(\mathcal{K}_\infty)[p]=\{0\}$, there is a natural embedding

$$E^{\pm}(\mathcal{K}_n)\otimes\mathbb{Q}_p/\mathbb{Z}_p\hookrightarrow(E^{\pm}(\mathcal{K}_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p)[\omega_n^{\pm}].$$

As $\deg(\omega_n^{\pm})=1+\sum_{k=1,k\text{ even/odd}}^{p^n}\varphi(p^k)$, we obtain

$$\Lambda\text{-corank}(E^{\pm}(\mathcal{K}_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p)\geq[\mathcal{K}:\mathbb{Q}_p].$$

□

Corollary 3.7 *If $p^2-1\nmid e(\mathcal{K}/\mathbb{Q}_p)$, then*

$$\Lambda\text{-corank}(E^{\pm}(\mathcal{K}_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p)=[\mathcal{K}:\mathbb{Q}_p].$$

In the proof, we will use the following plus/minus subgroups of $H^1(\mathcal{K}_n,T)$; the definition is analogous to [29, Definition 6.1].

Definition 3.8 Let $H_\pm(\mathcal{K}_n,T)\subset H^1(\mathcal{K}_n,T)$ be the orthogonal complement of $\widehat{E}^{\pm}(\mathcal{K}_n)\otimes\mathbb{Q}_p/\mathbb{Z}_p$ under the Tate pairing $H^1(\mathcal{K}_n,E[p^\infty])\times H^1(\mathcal{K}_n,T)\to\mathbb{Q}_p/\mathbb{Z}_p$, where $T=T_pE$ is the Tate module.

Proof of Corollary 3.7 We know that

$$\Lambda\text{-corank}(E(\mathcal{K}_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p)=\Lambda\text{-corank}(H^1(\mathcal{K}_\infty,E[p^\infty]))=2[\mathcal{K}:\mathbb{Q}_p],$$

where the first equality is Lemma 2.3, and the second one is due to Greenberg, see [14, 94] or [13, Proposition 1]. Note that $\widehat{E}^{\pm}(\mathcal{K}_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p=E^{\pm}(\mathcal{K}_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p$ as $E(\mathcal{K}_\infty)[p]=\{0\}$ by Lemma 3.1.

By Lemma 3.3 we see that $\widehat{E}^{+}(\mathcal{K}_n)\otimes\mathbb{Q}_p/\mathbb{Z}_p+\widehat{E}^{-}(\mathcal{K}_n)\otimes\mathbb{Q}_p/\mathbb{Z}_p=\widehat{E}(\mathcal{K}_n)\otimes\mathbb{Q}_p/\mathbb{Z}_p$. Therefore, $H_+(\mathcal{K}_n,T)\cap H_-(\mathcal{K}_n,T)$ is the orthogonal complement of $\widehat{E}(\mathcal{K}_n)\otimes\mathbb{Q}_p/\mathbb{Z}_p$. By definition,

$$\varprojlim_n H_+(\mathcal{K}_n,T)\cap\varprojlim_n H_-(\mathcal{K}_n,T)=\varprojlim_n(H_+(\mathcal{K}_n,T)\cap H_-(\mathcal{K}_n,T))$$

is the orthogonal complement of $\widehat{E}(\mathcal{K}_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p$, which is in turn equal to $H^1(\mathcal{K}_\infty,E[p^\infty])$ by Lemma 2.3. Thus,

$$\varprojlim_n H_+(\mathcal{K}_n,T)\cap\varprojlim_n H_-(\mathcal{K}_n,T)=0. \tag{2}$$

By Lemma 3.3 we have the following exact sequence

$$\widehat{E}(\mathcal{K}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \widehat{E}^+(\mathcal{K}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \oplus \widehat{E}^-(\mathcal{K}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \widehat{E}(\mathcal{K}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to 0,$$

which shows that

$$\big(\widehat{E}^+(\mathcal{K}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p\big) \cap \big(\widehat{E}^-(\mathcal{K}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p\big)$$

is annihilated by the variable X of $\mathbb{Z}_p[[X]]$. This implies that

$$\Lambda\text{-rank}\Big(\varprojlim_n H_+(\mathcal{K}_n, T) + \varprojlim_n H_-(\mathcal{K}_n, T)\Big) = \Lambda\text{-rank}\Big(\varprojlim_n H^1(\mathcal{K}_n, T)\Big).$$

Using (2), we obtain

$$\begin{aligned}&\Lambda\text{-rank}\Big(\varprojlim_n H_+(\mathcal{K}_n, T)\Big) + \Lambda\text{-rank}\Big(\varprojlim_n H_-(\mathcal{K}_n, T)\Big)\\ &\quad = \Lambda\text{-rank}\Big(\varprojlim_n H^1(\mathcal{K}_n, T)\Big) = 2[\mathcal{K} : \mathbb{Q}_p].\end{aligned}$$

Without loss of generality we can assume that

$$\Lambda\text{-rank}\Big(\varprojlim_n H_+(\mathcal{K}_n, T)\Big) \geq \Lambda\text{-rank}\Big(\varprojlim_n H_-(\mathcal{K}_n, T)\Big).$$

Therefore,

$$\begin{aligned}[\mathcal{K} : \mathbb{Q}_p] &\leq \Lambda\text{-rank}\Big(\varprojlim_n H_+(\mathcal{K}_n, T)\Big)\\ &= 2[\mathcal{K} : \mathbb{Q}_p] - \Lambda\text{-corank}\Big(\widehat{E}^+(\mathcal{K}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p\Big) \leq [\mathcal{K} : \mathbb{Q}_p].\end{aligned}$$

As $\varprojlim_n H_+(\mathcal{K}_n, T)$ is the Tate dual of $\widehat{E}^+(\mathcal{K}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p$, we obtain

$$[\mathcal{K} : \mathbb{Q}_p] = \Lambda\text{-corank}\Big(\widehat{E}^+(\mathcal{K}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p\Big) = \Lambda\text{-rank}\Big(\varprojlim_n H_+(\mathcal{K}_n, T)\Big). \tag{3}$$

As a consequence we obtain $\Lambda\text{-rank}(\varprojlim_n H_-(\mathcal{K}_n, T)) = [\mathcal{K} : \mathbb{Q}_p]$ and

$$\begin{aligned}[\mathcal{K} : \mathbb{Q}_p] &= \Lambda\text{-rank}\Big(\varprojlim_n H_-(\mathcal{K}_n, T)\Big)\\ &= 2[\mathcal{K} : \mathbb{Q}_p] - \Lambda\text{-corank}\Big(\widehat{E}^-(\mathcal{K}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p\Big) \leq [\mathcal{K} : \mathbb{Q}_p],\end{aligned}$$

which completes the proof. □

3.2 Freeness of Iwasawa cohomology

In this subsection, we study the Iwasawa cohomology groups $H^1_{\mathrm{Iw}}(\mathcal{K}, T) := \varprojlim H^1(\mathcal{K}_n, T)$ and $H^{\pm}_{\mathrm{Iw}}(\mathcal{K}, T) := \varprojlim H_{\pm}(\mathcal{K}_n, T)$ as modules over Λ and $\Lambda[G]$.

Lemma 3.9 *The module $H^1_{\mathrm{Iw}}(\mathcal{K}, T) = \varprojlim H^1(\mathcal{K}_n, T)$ is Λ-free.*

Proof Note that $(\varprojlim H^1(\mathcal{K}_n, T))_\Gamma$ is the dual of $H^1(\mathcal{K}_\infty, E[p^\infty])^\Gamma = H^1(\mathcal{K}, E[p^\infty])$ under the Tate pairing. Thus, $(\varprojlim H^1(\mathcal{K}_n, T))_\Gamma$ is $\mathbb{Z}_p$-free. As

$$\Lambda\text{-corank}(H^1(\mathcal{K}_\infty, E[p^\infty]) = [K : \mathbb{Q}_p] = \mathbb{Z}_p\text{-corank}(H^1(\mathcal{K}, E[p^\infty])),$$

the claim follows. □

Lemma 3.10 *If $p^2 - 1 \nmid e(\mathcal{K}/\mathbb{Q}_p)$, then $H^{\pm}_{\mathrm{Iw}}(\mathcal{K}, T) = \varprojlim H_{\pm}(\mathcal{K}_n, T)$ is Λ-free.*[1]

Proof According to [37, 5.3.19(ii)] it suffices to show that $H^{\pm}_{\mathrm{Iw}}(\mathcal{K}, T)^\Gamma = 0$ and that $H^{\pm}_{\mathrm{Iw}}(\mathcal{K}, T)_\Gamma$ is $\mathbb{Z}_p$-free. By Lemma 3.9 and the result just cited, we see that $H^{\pm}_{\mathrm{Iw}}(\mathcal{K}, T)^\Gamma \subset H^1_{\mathrm{Iw}}(\mathcal{K}, T)^\Gamma = 0$. It remains to prove that $H^{\pm}_{\mathrm{Iw}}(\mathcal{K}, T)_\Gamma$ is $\mathbb{Z}_p$-free.

Consider the tautological exact sequence

$$0 \to H^{\pm}_{\mathrm{Iw}}(\mathcal{K}, T) \to H^1_{\mathrm{Iw}}(\mathcal{K}, T) \to H^1_{\mathrm{Iw}}(\mathcal{K}, T)\big/H^{\pm}_{\mathrm{Iw}}(\mathcal{K}, T) \to 0.$$

The snake lemma gives us

$$0 \to \left(H^1_{\mathrm{Iw}}(\mathcal{K}, T)/H^{\pm}_{\mathrm{Iw}}(\mathcal{K}, T)\right)^\Gamma \to H^{\pm}_{\mathrm{Iw}}(\mathcal{K}, T)_\Gamma \to H^1_{\mathrm{Iw}}(\mathcal{K}, T)_\Gamma.$$

The last term is $\mathbb{Z}_p$-free by Lemma 3.9. It remains to show that $(H^1_{\mathrm{Iw}}(\mathcal{K}, T)/H^{\pm}_{\mathrm{Iw}}(\mathcal{K}, T))^\Gamma$ is $\mathbb{Z}_p$-free. Note that the dual with respect to the Tate pairing agrees with the Pontryagin dual. To prove the desired freeness, consider the following chain of equalities:

$$\begin{aligned}\left(\left(H^1_{\mathrm{Iw}}(\mathcal{K}, T)\Big/H^{\pm}_{\mathrm{Iw}}(\mathcal{K}, T)\right)^\Gamma\right)^\vee &= \left(\left(H^1_{\mathrm{Iw}}(\mathcal{K}, T)\Big/H^{\pm}_{\mathrm{Iw}}(\mathcal{K}, T)\right)^\vee\right)_\Gamma \\ &= \left(\left(\varprojlim_n H^1(\mathcal{K}_n, T)\Big/H_{\pm}(\mathcal{K}_n, T)\right)^\vee\right)_\Gamma \\ &= \left(\varinjlim_n \widehat{E}^{\pm}(\mathcal{K}_n, T) \otimes \mathbb{Q}_p/\mathbb{Z}_p\right)_\Gamma = \left(\widehat{E}^{\pm}(\mathcal{K}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p\right)_\Gamma.\end{aligned}$$

Thus,

$$\begin{aligned}\left(H^1_{\mathrm{Iw}}(\mathcal{K}, T)\Big/H^{\pm}_{\mathrm{Iw}}(\mathcal{K}, T)\right)^\Gamma &= \left(\left(\widehat{E}^{\pm}(\mathcal{K}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p\right)_\Gamma\right)^\vee \\ &= \left(\left(E^{\pm}(\mathcal{K}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p\right)_\Gamma\right)^\vee = \left(\widehat{E}^{\pm}(\mathcal{K}_\infty)^\iota \otimes \mathbb{Z}_p\right)^\Gamma,\end{aligned}$$

where ι means that elements $\gamma \in \Gamma$ act via γ^{-1} on $\widehat{E}^{\pm}(\mathcal{K}_\infty) \otimes \mathbb{Z}_p$. We obtain

$$\left(\widehat{E}^{\pm}(\mathcal{K}_\infty)^\iota \otimes \mathbb{Z}_p\right)^\Gamma = \widehat{E}^{\pm}(\mathcal{K}) \otimes \mathbb{Z}_p,$$

which is clearly $\mathbb{Z}_p$-free. □

[1] We thank Andreas Nickel for pointing out the proof of this fact given below.

Remark 3.11 By definition, $(\widehat{E}^{\pm}(\mathcal{K}_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p)^\vee = H^1_{\mathrm{Iw}}(\mathcal{K},T)/H^{\pm}_{\mathrm{Iw}}(\mathcal{K},T)$. By Lemmas 3.9 and 3.10, both modules $H^1_{\mathrm{Iw}}(\mathcal{K},T)$ and $H^{\pm}_{\mathrm{Iw}}(\mathcal{K},T)$ are Λ-free. This, however, does not imply that the quotient is Λ-free as well, as one can easily see from the following example.

Consider the following two Λ-homomorphisms

$$\psi\colon \Lambda\to\Lambda^2,\quad 1\mapsto(p,-T)$$

and

$$\phi\colon \Lambda^2\mapsto(p,T)\Lambda,\quad (1,0)\mapsto T,\quad (0,1)\mapsto p.$$

It is easy to see that $\ker(\phi)=\Lambda(p,-T)=\mathrm{Im}(\psi)$. Thus we obtain a short exact sequence

$$0\to\Lambda\to\Lambda^2\to(p,T)\Lambda\to 0$$

The first two modules are clearly free over Λ, while the third one is not.

Corollary 3.12 *If $p^2-1\nmid e(\mathcal{K}/\mathbb{Q}_p)$, then $\left(\frac{H^1(\mathcal{K}_\infty,E[p^\infty])}{E^{\pm}(\mathcal{K}_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p}\right)^{\Gamma_n}$ is $\mathbb{Z}_p$-divisible for all $n\geq 0$.*

Proof It suffices to prove that $\varprojlim H_{\pm}(\mathcal{K}_n,T)/\omega_n$ is $\mathbb{Z}_p$-free. By Lemma 3.10 we know that $\varprojlim H_{\pm}(\mathcal{K}_n,T)$ is Λ-free. Thus, taking Γ_n-coinvariants results in a $\mathbb{Z}_p$-free module. □

Lemma 3.13 *Let G be a cyclic group of order p that commutes with Γ. Let M be a finitely generated $\Lambda[G]$-module that is free as a Λ-module. Let $M_{\Gamma,G}$ denote the module of coinvariants under Γ and G. Suppose that $M_{\Gamma,G}$ is free as a $\mathbb{Z}_p$-module and $\mathbb{Z}_p$-rank$(M_{\Gamma,G})\cdot|G|=\Lambda$-rank$(M)$.[2] Then M is $\Lambda[G]$-free.*

Proof Since M is free as a Λ-module, we may choose a $\mathbb{Z}_p$-basis $x_1,\dots,x_r$ of $M_{\Gamma,G}$, where $r=\mathbb{Z}_p$-rank$(M_{\Gamma,G})$. Applying Nakayama's lemma, we obtain that these generate M as a $\Lambda[G]$-module: $\langle x_1,\dots,x_r\rangle_{\Lambda[G]}=M$. We have Λ-rank$(\langle x_1,\dots,x_r\rangle_{\Lambda[G]})\leq r\cdot|G|=\Lambda$-rank$(M)$ by the assumption. It follows that there can be no $\Lambda[G]$-relations between the generators $x_1,\dots,x_r$, so they form a $\Lambda[G]$-basis of M. □

Corollary 3.14 *Let $G\subset\mathrm{Gal}(\mathcal{K}/\mathbb{Q}_p)$ be cyclic of order p. If $p^2-1\nmid e(\mathcal{K}/\mathbb{Q}_p)$, and if $\mathcal{K}/\mathcal{K}^G$ is at most weakly ramified, then $H^{\pm}_{\mathrm{Iw}}(\mathcal{K},T)$ is a free $\Lambda[G]$-module.*

Proof This follows by applying Lemma 3.13 to $M:=H^{\pm}_{\mathrm{Iw}}(\mathcal{K},T)$. The module $H^{\pm}_{\mathrm{Iw}}(\mathcal{K},T)$ is Λ-free by Lemma 3.10. To verify the rank condition, recall that $H^{\pm}_{\mathrm{Iw}}(\mathcal{K},T)_{\Gamma,G}=H_{\pm}(\mathcal{K},T)_G$ is, by definition, the Tate dual of $H^1(\mathcal{K},E[p^\infty])/(\widehat{E}^{\pm}(\mathcal{K})\otimes\mathbb{Q}_p/\mathbb{Z}_p)^G$. We show that this quotient is $\mathbb{Z}_p$-cofree: for this, first consider the tautological exact sequence

$$0\to E(\mathcal{K})\otimes\mathbb{Q}_p/\mathbb{Z}_p\to H^1(\mathcal{K},E[p^\infty])\to\frac{H^1(\mathcal{K},E[p^\infty])}{E(\mathcal{K})\otimes\mathbb{Q}_p/\mathbb{Z}_p}\to 0.$$

We claim that $\widehat{E}(\mathcal{K})$ is $\mathbb{Z}_p[G]$-free. The module $\widehat{E}(\mathcal{K}^G)$ is $\mathbb{Z}_p$-free of rank $[\mathcal{K}^G:\mathbb{Q}_p]$. As G is cyclic of order p and $\mathcal{K}/\mathcal{K}^G$ is at most weakly ramified, Corollary 2.6 implies

$$\widehat{E}\left(\mathcal{K}^G\right)=\mathrm{Tr}_{\mathcal{K}/\mathcal{K}^G}\left(\widehat{E}(\mathcal{K})\right)\simeq\widehat{E}(\mathcal{K})\Big/\ker\left(\mathrm{Tr}_{\mathcal{K}/\mathcal{K}^G}\right)=\widehat{E}(\mathcal{K})\Big/\mathrm{aug}\left(\mathcal{K}/\mathcal{K}^G\right)\widehat{E}(\mathcal{K}),$$

[2] The authors thank Eva Brenner for pointing out a missing condition in an earlier version of this statement.

where $\mathrm{aug}(\mathcal{K}/\mathcal{K}^G) \subset \mathbb{Z}_p[G]$ denotes the augmentation ideal. It follows from Nakayama's Lemma that $\widehat{E}(\mathcal{K})$ is generated by $[\mathcal{K}^G : \mathbb{Q}_p]$ elements as a $\mathbb{Z}_p[G]$-module. But $\widehat{E}(\mathcal{K})$ has $\mathbb{Z}_p$-rank $[\mathcal{K} : \mathbb{Q}_p]$, so it must in fact be free over $\mathbb{Z}_p[G]$. (Compare this with [30, Lemma 3.2].)

Note that $E(\mathcal{K}) \otimes \mathbb{Q}_p/\mathbb{Z}_p = \widehat{E}(\mathcal{K}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$. We take G-invariants in the short exact sequence above. Since $\widehat{E}(\mathcal{K})$ is $\mathbb{Z}_p[G]$-free, the first term in the resulting long exact sequence is $\widehat{E}(\mathcal{K}^G) \otimes \mathbb{Q}_p/\mathbb{Z}_p = E(\mathcal{K}^G) \otimes \mathbb{Q}_p/\mathbb{Z}_p$. The inflation-restriction sequence shows that the second term is $H^1(\mathcal{K}^G, E[p^\infty])$. The fourth term is $H^1(G, E(\mathcal{K}) \otimes \mathbb{Q}_p/\mathbb{Z}_p) = H^1(G, \widehat{E}(\mathcal{K}) \otimes \mathbb{Q}_p/\mathbb{Z}_p) = 0$. Hence the third term is the quotient of the first two, that is, the long sequence of G-invariants becomes:

$$0 \to E(\mathcal{K}^G) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to H^1(\mathcal{K}^G, E[p^\infty]) \to \frac{H^1(\mathcal{K}^G, E[p^\infty])}{E(\mathcal{K}^G) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \to 0$$

The middle term is divisible, hence $\mathbb{Z}_p$-cofree, and thus so is the quotient, as claimed. The rank condition now follows from (3). □

3.3 Computation of cohomology groups

In this subsection, we compute the cohomology groups which will be relevant for studying signed Selmer groups. Most of our computations follow along the lines of Lim's work [30], with the crucial exception of Proposition 3.19, the proof of which relies on the freeness of Iwasawa cohomology.

From now on, we assume that $\mathcal{K}/\mathbb{Q}_p$ is a Galois extension. Let $\mathcal{F} \subset \mathcal{K}$ be a subfield such that $\mathcal{K}$ is Galois over $\mathcal{F}$. We set $G := \mathrm{Gal}(\mathcal{K}_\infty/\mathcal{F}_\infty)$. Then G is canonically isomorphic to a subgroup of $\mathrm{Gal}(\mathcal{K}/\mathcal{F})$, and it makes sense to consider the Galois action of (subgroups of) G on $\widehat{E}(\mathcal{K})$.

Recall that a finite extension of local fields is called weakly ramified if the second ramification group vanishes.

Remark 3.15 The assumption $\mathbb{Q}_{p,\infty} \cap \mathcal{K} = \mathbb{Q}_p$ ensures that there is a well-defined action of H on $\mathcal{K}_n$. If $\mathcal{K}/\mathbb{Q}_p$ is tamely ramified, the condition $\mathbb{Q}_{p,\infty} \cap \mathcal{K} = \mathbb{Q}_p$ is trivially satisfied. Cohomological triviality in the tamely ramified case was also established in [7, Proposition 3.10].

Lemma 3.16 *Assume that $\mathcal{K}/\mathbb{Q}_p$ is at most weakly ramified and that $\mathbb{Q}_{p,\infty} \cap \mathcal{K} = \mathbb{Q}_p$. For each subgroup H of $\mathrm{Gal}(\mathcal{K}/\mathbb{Q}_p)$ and each $i \geq 1$ we have*

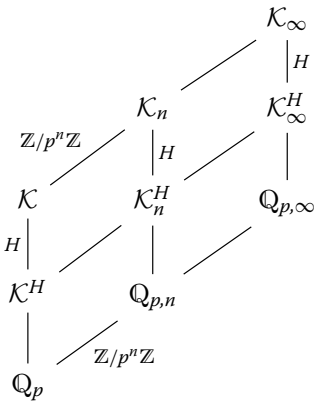
$$H^i(H, \widehat{E}(\mathcal{K}_n)) = \{0\}.$$

Proof Note that $\mathrm{Gal}(\mathcal{K}/\mathbb{Q}_p)$ is the semidirect product of cyclic groups. It therefore suffices to consider the case that H is cyclic. If the order of H is coprime to p, the claim follows from [7, Proposition 3.10]. It remains the case that $|H| = p$. By Lemma 2.8 the extension $\mathcal{K}_n/\mathcal{K}_n^H$ is weakly ramified. As E is supersingular and therefore $\widehat{E}$ is of height 2, this follows from Corollary 2.6. □

Using Lemma 3.16 instead of [30, Lemma 3.2], we can work along the lines of [30, proof of Proposition 3.4] to prove the following:

Lemma 3.17 *Assume that $\mathcal{K}/\mathbb{Q}_p$ is at most weakly ramified, and that $\mathbb{Q}_{p,\infty} \cap \mathcal{K} = \mathbb{Q}_p$ and $p^2 - 1 \nmid e(\mathcal{K}/\mathbb{Q}_p)$. For every subgroup of $\mathrm{Gal}(\mathcal{K}/\mathbb{Q}_p)$ we have*

$$H^i(H, \widehat{E}(\mathcal{K}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p) = \begin{cases} \widehat{E}(\mathcal{K}_n^H) \otimes \mathbb{Q}_p/\mathbb{Z}_p & i = 0, \\ 0 & i > 0. \end{cases} \square$$



The infinite level version of Lemma 3.17 is the following:

Lemma 3.18 *If $p^2 - 1 \nmid e(\mathcal{K}/\mathbb{Q}_p)$, then for every subgroup H of $\mathrm{Gal}(\mathcal{K}/\mathbb{Q}_p)$ we have*

$$H^i(H, \widehat{E}(\mathcal{K}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p) = \begin{cases} \widehat{E}(\mathcal{K}_\infty^H) \otimes \mathbb{Q}_p/\mathbb{Z}_p & i = 0, \\ 0 & i > 0. \end{cases}$$

Proof The proof follows along the lines of [30, Proposition 3.6]. We restate it here for the convenience of the reader. By Lemma 3.1, we have a short exact sequence

$$0 \to \widehat{E}(\mathcal{K}_\infty) \to \widehat{E}(\mathcal{K}_\infty) \otimes \mathbb{Q}_p \to \widehat{E}(\mathcal{K}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to 0$$

By [4, Theorem 3.1] we have $H^i(H, \widehat{E}(\mathcal{K}_\infty)) = 0$ for all $i > 0$. Thus, we obtain

$$0 \to \widehat{E}(\mathcal{K}_\infty^H) \to \widehat{E}(\mathcal{K}_\infty^H) \otimes \mathbb{Q}_p \to (\widehat{E}(\mathcal{K}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^H \to 0$$

and

$$H^i(H, \widehat{E}(\mathcal{K}_\infty) \otimes \mathbb{Q}_p) \cong H^i(H, \widehat{E}(\mathcal{K}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p)$$

for $i \geq 1$. The claim for $i = 0$ follows from the exact sequence. As H is a finite group and $\widehat{E}(\mathcal{K}_\infty) \otimes \mathbb{Q}_p$ is torsion free, we see that $H^i(H, \widehat{E}(\mathcal{K}_\infty) \otimes \mathbb{Q}_p) = 0$ for all $i > 0$, which implies the second claim by the above isomorphism. $\square$

Proposition 3.19 *Assume that $\mathcal{K}/\mathbb{Q}_p$ is at most weakly ramified, that $\mathbb{Q}_{p,\infty} \cap \mathcal{K} = \mathbb{Q}_p$ and $p^2 - 1 \nmid e(\mathcal{K}/\mathbb{Q}_p)$. For every subgroup H of $\mathrm{Gal}(\mathcal{K}/\mathbb{Q}_p)$ we have*

$$H^i\left(H, \frac{H^1(\mathcal{K}_\infty, E[p^\infty])}{\widehat{E}^\pm(\mathcal{K}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p}\right) = \begin{cases} \frac{H^1(\mathcal{K}_\infty^H, E[p^\infty])}{\widehat{E}^\pm(\mathcal{K}_\infty^H) \otimes \mathbb{Q}_p/\mathbb{Z}_p} & i = 0, \\ 0 & i > 0. \end{cases}$$

Proof We will first assume that H is cyclic of prime order ℓ. If ℓ is coprime to p, there is nothing to prove. Thus, we will assume that H is cyclic of order p. By Corollary 3.14, the module $H^{\pm}_{\mathrm{Iw}}(\mathcal{K}, T)$ is $\Lambda[H]$-free. In particular,

$$H^i(H, H^{\pm}_{\mathrm{Iw}}(\mathcal{K}, T)) = 0 \quad i > 0.$$

As $H^{\pm}_{\mathrm{Iw}}(\mathcal{K}, T)$ is the Tate dual of $\frac{H^1(\mathcal{K}_\infty, E[p^\infty])}{\widehat{E}^{\pm}(\mathcal{K}_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p}$, the claim for $i > 0$ follows. It remains to prove the claim for $i = 0$. As H is cyclic, we obtain

$$\widehat{H}^0\left(H, \frac{H^1(\mathcal{K}_\infty, E[p^\infty])}{\widehat{E}^{\pm}(\mathcal{K}_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p}\right) = H^2\left(H, \frac{H^1(\mathcal{K}_\infty, E[p^\infty])}{\widehat{E}^{\pm}(\mathcal{K}_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p}\right) = 0,$$

where $\widehat{H}^0$ denotes the 0th Tate cohomology group. In particular,

$$\left(\frac{H^1(\mathcal{K}_\infty, E[p^\infty])}{\widehat{E}^{\pm}(\mathcal{K}_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p}\right)^H = \mathrm{Tr}_H\left(\left(\frac{H^1(\mathcal{K}_\infty, E[p^\infty])}{\widehat{E}^{\pm}(\mathcal{K}_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p}\right)\right) \subset \frac{H^1(\mathcal{K}_\infty^H, E[p^\infty])}{\widehat{E}^{\pm}(\mathcal{K}_\infty^H)\otimes\mathbb{Q}_p/\mathbb{Z}_p}.$$

The last inclusion follows from the fact that

$$\mathrm{Tr}_H(H^1(\mathcal{K}_\infty, E[p^\infty])) \subset H^1(\mathcal{K}_\infty, E[p^\infty])^H = H^1(\mathcal{K}_\infty^H, E[p^\infty])$$

and

$$\mathrm{Tr}_H(\widehat{E}^{\pm}(\mathcal{K}_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p) \subset \widehat{E}^{\pm}(\mathcal{K}_\infty)^H\otimes\mathbb{Q}_p/\mathbb{Z}_p = \widehat{E}^{\pm}(\mathcal{K}_\infty^H)\otimes\mathbb{Q}_p/\mathbb{Z}_p.$$

This completes the proof for cyclic groups of prime order.

For the general case, note that $\mathrm{Gal}(\mathcal{K}/\mathbb{Q}_p)$ is solvable and that each subfield of $\mathcal{K}$ is again at most weakly ramified and such that $\mathbb{Q}_{p,\infty}\cap\mathcal{K} = \mathbb{Q}_p$. It therefore suffices to prove the claim for cyclic groups. □

Corollary 3.20 *Assume that $\mathcal{K}/\mathbb{Q}_p$ is at most weakly ramified, and that $\mathbb{Q}_{p,\infty}\cap\mathcal{K} = \mathbb{Q}_p$ and $p^2-1\nmid e(\mathcal{K}/\mathbb{Q}_p)$. For every cyclic subgroup $C = PQ$ of $\mathrm{Gal}(\mathcal{K}/\mathbb{Q}_p)$ and every character ε of Q we have*

$$h_P\left(\left(\frac{H^1(\mathcal{K}_\infty, E[p^\infty])}{\widehat{E}^{\pm}(\mathcal{K}_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p}\right)^{\varepsilon}\right) = 1.\square$$

3.4 *p*-primary part

Lemma 3.21 *If $p^2-1\nmid e(\mathcal{K}/\mathbb{Q}_p)$, then there is a natural isomorphism*

$$\frac{H^1(\mathcal{K}_\infty, E[p])}{\widehat{E}^{\pm}(\mathcal{K}_\infty)/p\widehat{E}^{\pm}(\mathcal{K}_\infty)} \longrightarrow \frac{H^1(\mathcal{K}_\infty, E[p^\infty])}{\widehat{E}^{\pm}(\mathcal{K}_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p}[p].$$

Proof Consider the following commutative diagram; the first row is tautologically exact, with the vertical arrows being the natural maps.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \widehat{E}^{\pm}(\mathcal{K}_\infty)/p\widehat{E}^{\pm}(\mathcal{K}_\infty) & \longrightarrow & H^1(\mathcal{K}_\infty, E[p]) & \longrightarrow & \frac{H^1(\mathcal{K}_\infty, E[p])}{\widehat{E}^{\pm}(\mathcal{K}_\infty)/p\widehat{E}^{\pm}(\mathcal{K}_\infty)} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & (\widehat{E}^{\pm}(\mathcal{K}_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p)[p] & \longrightarrow & H^1(\mathcal{K}_\infty, E[p^\infty])[p] & \longrightarrow & \frac{H^1(\mathcal{K}_\infty, E[p^\infty])}{\widehat{E}^{\pm}(\mathcal{K}_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p}[p] & \longrightarrow & 0
\end{array}$$

The second row is exact as $\widehat{E}^{\pm} \otimes \mathbb{Q}_p/\mathbb{Z}_p$ is $\mathbb{Z}_p$-divisible The left most and the middle vertical map are isomorphisms as $E(\mathcal{K}_\infty)[p] = 0$ by Lemma 3.1. Thus, the right vertical map is an isomorphism. □

4 Global considerations

We fix the following: p is a rational prime, $F/F'/\mathbb{Q}$ are number fields with p completely split in F', K/F is a finite Galois extension, and E/F' is an elliptic curve. We assume that

(S1) E has good reduction at all p-adic places of F';
(S2) there is a p-adic place with supersingular reduction;
(S3) each p-adic supersingular place u
  (i) has ramification index $e_u(K/F')$ that is not divisible by $p^2 - 1$ in K/F',
  (ii) fulfills the following condition: K_u is contained in the compositum of an at most weakly ramified extension $\mathcal{K}'/\mathbb{Q}_p$ and the cyclotomic extension $\mathbb{Q}_{p,\infty}$, where $\mathcal{K}' \cap \mathbb{Q}_{p,\infty} = \mathbb{Q}_p$.
  (iii) satisfies $a_u = 0$.

Conditions (S3.i) and (S3.ii) are weaker than those put in place by [30, §4]: indeed, there the condition is $e_u(K/F') = 1$, whereas we require $e_u(K/F')$ not to be divisible by $p^2 - 1$ and that wild ramification only come from the cyclotomic $\mathbb{Z}_p$-extension.

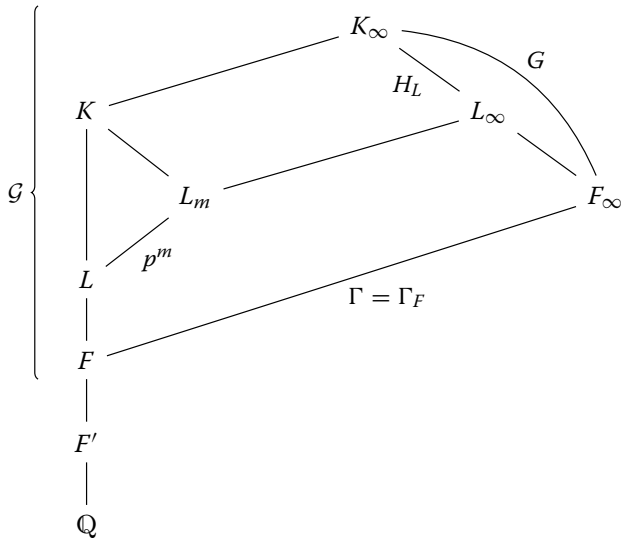
Remark 4.1 Let $E/\mathbb{Q}$ be an elliptic curve and $p \geq 5$ a supersingular prime. Let s, l be a non-negative integers and let $\alpha_1, \ldots, \alpha_s$ be integers that are independent in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^{p^l}$. Assume that the α_i are p^l-th powers in $\mathbb{Q}_p$. Let $K = \mathbb{Q}(\zeta_{p^l}, \alpha_1^{1/p^l}, \ldots, \alpha_s^{1/p^l})$. Then E, p and K satisfy the above conditions with $F = F' = \mathbb{Q}$.

Fix the following finite sets of places of F. We write Σ^{ord} resp. Σ^{ss} resp. Σ^{bad} for the set of places of F at which E has ordinary resp. supersingular resp. bad reduction. Let Σ_p resp. Σ_∞ be the set of p-adic resp. infinite places of F. Let Σ be a finite set of places of F satisfying

$$\Sigma \supseteq \Sigma_p \cup \Sigma_{\mathrm{ram}(F/F')} \cup \Sigma_{\mathrm{ram}(K/F)} \cup \Sigma^{\mathrm{bad}} \cup \Sigma_\infty, \tag{4}$$

and let $\Sigma_1 := \Sigma - \Sigma_p$ be the subset of non-p-adic places. We decompose Σ_p into the disjoint sets Σ_p^{ord} of ordinary places and Σ_p^{ss} of supersingular places. For an extension $\widetilde{F}/F$, let $\Sigma(\widetilde{F})$ denote the places of $\widetilde{F}$ above those in Σ.

Let K_∞/K by the cyclotomic $\mathbb{Z}_p$-extension, and let K/L be a subextension of K/F. If $L_\infty = LF_\infty$ is the cyclotomic $\mathbb{Z}_p$-extension of L and L_m/L is the unique degree p^m extension of L in L_∞, then there is an $m \geq 0$ such that $K \cap L_\infty = L_m$. Write $H_L := \mathrm{Gal}(K_\infty/L_\infty)$ and $\Gamma_L := \mathrm{Gal}(L_\infty/L)$. Let $G = \mathrm{Gal}(K_\infty/F_\infty)$ and denote Γ_F by Γ. Then we have an isomorphism $\mathcal{G} := \mathrm{Gal}(K_\infty/F) = G \rtimes \Gamma$. We fix once and for all a lift Γ' of Γ in $\mathcal{G}$ such that the restriction induces an isomorphism $\Gamma' \cong \Gamma$. By abuse of notation we will denote Γ' by Γ in the following. Let $\Lambda := \mathbb{Z}_p[\![\Gamma_K]\!]$ and $\Lambda(\mathcal{G}) := \mathbb{Z}_p[\![\mathcal{G}]\!]$ be the relevant Iwasawa algebras.



Note that conditions (S2) and (S3) imply that $H^0(G_\Sigma(K_\infty, E[p^\infty]) = 0$ by Lemma 3.1. We will frequently use this fact without further mentioning it.

4.1 Definition of signed Selmer groups

For each supersingular place $v \in \Sigma_p^{\mathrm{ss}}$, fix a sign $s_v \in \{+, -\}$, thus defining a vector $\vec{s} \in \{\pm\}^{\Sigma_p^{\mathrm{ss}}}$. Let $v(L_n)$ denote the set of primes lying above v in L_n; note that there may be more than one such prime. For $u \in v(L_n)$, let $s_u := s_v$: this defines a vector $\vec{s}(L_n) \in \{\pm\}^{\Sigma_p^{\mathrm{ss}}(L_n)}$.

Let $L_{n,\Sigma}/L_n$ be the maximal Σ-ramified extension of L_n. Note that the assumption $\Sigma \supseteq \Sigma_p \cup \Sigma_{\mathrm{ram}(K/F)}$ implies $L_\Sigma = K_\Sigma$ and $L_{\infty,\Sigma} = K_{\infty,\Sigma}$. Let the signed Selmer group $\mathrm{Sel}^{\vec{s}}(E/L_n)$ be defined as the kernel of the following natural global-to-local map:

$$H^1\left(L_{n,\Sigma}/L_n, E[p^\infty]\right) \to \bigoplus_{u \in \Sigma_p^{\mathrm{ord}}(L_n)} \frac{H^1(L_{n,u}, E[p^\infty])}{E(L_{n,u}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \oplus \oplus \bigoplus_{u \in \Sigma_p^{\mathrm{ss}}(L_n)} \frac{H^1(L_{n,u}, E[p^\infty])}{E^{s_u}(L_{n,u}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \oplus \bigoplus_{u \in \Sigma_1(L_n)} H^1(L_{n,u}, E[p^\infty])$$

Let $\mathrm{Sel}^{\vec{s}}(E/L_\infty) := \varinjlim_n \mathrm{Sel}^{\vec{s}}(E/L_n)$. For $n \leq \infty$ and $u \in \Sigma(L_n)$, we introduce the notation

$$B_{n,u} := \begin{cases} E(L_{n,u}) \otimes \mathbb{Q}_p/\mathbb{Z}_p & u \in \Sigma_p^{\mathrm{ord}}(L_n) \\ E^{s_u}(L_{n,u}) \otimes \mathbb{Q}_p/\mathbb{Z}_p & u \in \Sigma_p^{\mathrm{ss}}(L_n) \\ 0 & u \in \Sigma_1(L_n) \end{cases} \tag{5}$$

and let $J_u(E/L_n) := H^1(L_{n,u}, E[p^\infty])/B_{n,u}$, so that

$$\mathrm{Sel}^{\vec{s}}(E/L_n) = \ker\left(H^1\left(L_{n,\Sigma}/L_n, E[p^\infty]\right) \to \bigoplus_{u \in \Sigma(L_n)} J_u(E/L_n)\right). \tag{6}$$

Note that for $u \in \Sigma_p^{\mathrm{ord}}(L_\infty)$, we have

$$J_u(E/L_\infty) \simeq H^1(L_{\infty,u}, E)[p^\infty] \tag{7}$$

Lemma 4.2 *The restriction map $H^1(K_{\infty,\Sigma}/L_\infty, E[p^\infty]) \to H^1(K_{\infty,\Sigma}/K_\infty, E[p^\infty])$ induces a map $\mathrm{Sel}^{\vec{s}}(E/L_\infty) \to \mathrm{Sel}^{\vec{s}}(E/K_\infty)^{H_L}$, which has trivial kernel and finite cokernel.*

Proof The idea is the same as in the proof of [20, Lemma 3.3]. Reformulating (6), we find that there is a commutative diagram with exact rows:

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Sel}^{\vec{s}}(E/L_\infty) & \longrightarrow & H^1(K_{\infty,\Sigma}/L_\infty, E[p^\infty]) & \longrightarrow & \bigoplus_{u\in\Sigma(L_\infty)} J_u(E/L_\infty) \\
 & & \downarrow & & \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle l=\oplus_u l_u} \\
0 & \longrightarrow & \mathrm{Sel}^{\vec{s}}(E/K_\infty)^{H_L} & \longrightarrow & H^1(K_{\infty,\Sigma}/K_\infty, E[p^\infty])^{H_L} & \longrightarrow & \bigoplus_{w\in\Sigma(K_\infty)} J_w(E/K_\infty)^{H_L}
\end{array}$$

This is referred to as the 'fundamental diagram' in [33, §6.2]. Consider the restriction map. By Lemma 3.1, we have $E(K_{\infty,w})[p^\infty] = 0$ for all $w \in \Sigma_p^{\mathrm{ss}}(K_\infty)$. Writing $G_\Sigma(K_\infty) := \mathrm{Gal}(K_{\infty,\Sigma}/K_\infty)$, the inflation–restriction exact sequence implies that

$$\ker(\mathrm{res}) = H^1\left(H_L, E[p^\infty]^{G_\Sigma(K_\infty)}\right) = 0 \quad \mathrm{coker}(\mathrm{res}) = H^2\left(H_L, E[p^\infty]^{G_\Sigma(K_\infty)}\right) = 0.$$

In particular, res is an isomorphism. We turn to the map l. Local considerations show that l_u is an isomorphism for all supersingular primes above p: indeed, Proposition 3.19 with $i = 0$ shows $J_u(E/L_\infty) = J_w(E/K_\infty)^{H_L}$. For non-supersingular places, the map l_u has finite kernel: for $u \in \Sigma_p^{\mathrm{ord}}(L_\infty)$, this is the last sentence of [20, Lemma 3.3] together with the observation (7), and for $u \in \Sigma_1(L_\infty)$, this is shown in loc.cit. Modding out by the cokernels on the right in both rows, the assertion follows by invoking the snake lemma. □

4.2 Torsion properties of $X^{\vec{s}}(E/K_\infty)$

We want to generalise a well-known characterisation of being Λ-cotorsion for signed Selmer groups, see [30, Proposition 4.2], [31, Proposition 2.8].

Let $n \geq 0$ be fixed. Let $T = T_pE$ denote the Tate module, and write $V = T_p \otimes \mathbb{Q}_p$ and $T^*(1) = \mathrm{Hom}_{\mathbb{Z}_p}(T, \mathbb{Z}_p(1))$. Noting that $V/T \simeq E[p^\infty]$, the Cassels–Poitou–Tate exact sequence [6, Theorem 1.5] reads as follows:

$$\begin{aligned}
0 \to \mathrm{Sel}^{\vec{s}}(E/K_n) \to H^1(G_\Sigma(K_n), E[p^\infty]) \to \bigoplus_{w\in\Sigma(K_n)} J_w(E/K_n) \to \\
\to H^1_A(K_n, T^*(1))^\vee \to H^2(G_\Sigma(K_n), E[p^\infty]) \to \bigoplus_{w\in\Sigma(K_n)} H^2(K_{n,w}, E[p^\infty]) \to \\
\to H^0(K_n, T^*(1))^\vee \to 0
\end{aligned} \tag{8}$$

The group $H^1_A(K_n, T^*(1)) \subseteq H^1(G_\Sigma(K_n), T^*(1))$ consists of cocycles whose restrictions at w satisfy local conditions $A_w \subseteq H^1(K_{n,w}, T^*(1))$, where $A_{n,w}$ is the orthogonal complement of $B_{n,w}$ under local Tate duality, where $B_{n,w}$ is as in (5). As explained in the paragraph preceding (4) in op.cit., Tate duality gives an isomorphism $H^2(K_{n,w}, E[p^\infty]) \simeq$

$\left(\varprojlim_m H^0(K_{n,w}, E[p^m])\right)^\vee = 0$ for all $w \in \Sigma(K_n)$. Going up the tower, it follows that for any place $w \in \Sigma(K_\infty)$, we have

$$H^2(K_{\infty,w}, E[p^\infty]) = 0. \tag{9}$$

This last assertion can also be seen through more direct means.[3] Letting v denote the place beneath w in K, the field $K_{\infty,w}$ is an extension of the local field K_v of degree p^∞, and therefore the absolute Galois group of $K_{\infty,w}$ has p-cohomological dimension 1 by [37, Theorem 7.1.8.(i)].

The following is a generalization of [31, Proposition 2.8].

Proposition 4.3 *The module $X^{\vec{s}}(E/K_\infty)$ is Λ-torsion if and only if $H^2(G_\Sigma(K_\infty), E[p^\infty]) = 0$ and the following sequence is exact:*

$$0 \to \mathrm{Sel}^{\vec{s}}(E/K_\infty) \to H^1(G_\Sigma(K_\infty), E[p^\infty]) \to \bigoplus_{w \in \Sigma(K_\infty)} J_w(E/K_\infty) \to 0. \tag{10}$$

Proof Taking direct limits in (8) and using (9), we obtain an exact sequence:

$$0 \to \mathrm{Sel}^{\vec{s}}(E/K_\infty) \to H^1(G_\Sigma(K_\infty), E[p^\infty]) \to \bigoplus_{w \in \Sigma(K_\infty))} J_w(E/K_\infty) \to$$
$$\to \left(\varprojlim_n H^1_A(K_n, T^*(1))\right)^\vee \to H^2(G_\Sigma(K_\infty), E[p^\infty]) \to 0.$$

The Λ-module $\varprojlim_n H^1(G_\Sigma(K_n), T)$ is torsion-free by [31, Lemma 2.6]. As the module $\varprojlim_n H^1_A(K_n, T^*(1))$ is a submodule of $\varprojlim_n H^1(G_\Sigma(K_n), T)$ by definition, it does not contain any non-zero Λ-torsion submodule. Thus, $\varprojlim_n H^1_A(K_n, T^*(1)) = 0$ if and only if $\Lambda\text{-corank}\left(\varprojlim_n H^1_A(K_n, T^*(1))\right)^\vee = 0$.

Fix a lift of Γ to $\mathrm{Gal}(K_\infty/F)$, and let K_∞^Γ denote its fixed field (a subfield of K).Note that this lift can be chosen to be Γ_K. By abuse of notation we will write Γ for Γ_K in the following. By [13, Proposition 3] we have

$$\Lambda\text{-corank}\left(H^1(G_\Sigma(K_\infty), E[p^\infty])\right) - \Lambda\text{-corank}\left(H^2(G_\Sigma(K_\infty), E[p^\infty]\right) = [K_\infty^\Gamma : \mathbb{Q}]$$

If w is a place coprime to p, [13, Proposition 2] implies that $H^1(K_{\infty,w}, E[p^\infty])$ is of Λ-corank zero. If $w \mid p$ and p is an ordinary prime [20, section 4] implies that $J_w(E/K_\infty)$ is of Λ-corank $[K^\Gamma_{\infty,w} : \mathbb{Q}_p]$. For $w \mid p$ a supersingular prime, Corollary 3.7 implies that $J_w(E/K_\infty)$ has Λ-corank $[K^\Gamma_{\infty,w} : \mathbb{Q}_p]$. Thus we obtain

$$\Lambda\text{-corank}\left(H^1(G_\Sigma(K_\infty), E[p^\infty])\right) - \Lambda\text{-corank}\left(H^2(G_\Sigma(K_\infty), E[p^\infty]\right)$$
$$= \Lambda\text{-corank}\left(\bigoplus_{w \in \Sigma(K_\infty)} J_w(E/K_\infty)\right).$$

It now follows that $\mathrm{Sel}^{\vec{s}}(E/K_\infty)$ is Λ-cotorsion if an only if $\Lambda\text{-corank}(H^2(G_\Sigma(K_\infty), E)) = \Lambda\text{-corank}((\varprojlim_n H^1_A(K_n, T^*(1)))^\vee) = 0$. By [13, proposition 4] this is the case if and only if both modules vanish which is in turn equivalent to the vanishing of $H^2(G_\Sigma(K_\infty), E[p^\infty])$ and the validity of the short exact sequence in the statement of the proposition. □

[3] The authors thank the referee for pointing this out.

Proposition 4.4 *If $X^{\vec{s}}(E/K_\infty)$ is Λ-torsion, then $H^i(H, \mathrm{Sel}^{\vec{s}}(E/K_\infty))$ is finite for all $H \leq G$ and $i \geq 1$.*

Proof We follow [30, Proposition 4.4]. As before, let $H_L \leq G$ be a finite subgroup with fixed field L_∞. Consider the commutative diagram in the proof of Lemma 4.2: the first row becomes a short exact sequence due to Proposition 4.3, and the second row can be extended to a long exact sequence:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Sel}^{\vec{s}}(E/L_\infty) & \longrightarrow & H^1(G_\Sigma(L_\infty), E[p^\infty]) & \longrightarrow & \bigoplus_{u\in\Sigma(L_\infty)} J_u(E/L_\infty) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle =\oplus l_u} & & \\
0 & \longrightarrow & \mathrm{Sel}^{\vec{s}}(E/K_\infty) & \longrightarrow & H^1(G_\Sigma(K_\infty), E[p^\infty])^{H_L} & \longrightarrow & \left(\bigoplus_{w\in\Sigma(K_\infty)} J_w(E/K_\infty)\right)^{H_L} & &
\end{array}$$

$$\to H^1\left(H_L, \mathrm{Sel}^{\vec{s}}(E/K_\infty)\right) \to H^1\left(H_L, H^1(G_\Sigma(K_\infty), E[p^\infty])\right) \to H^1\left(H_L, \bigoplus_{w\in\Sigma(K_\infty)} J_w(E/K_\infty)\right) \to \cdots$$

We compute the middle terms in the long exact sequence. For $i = 0$, we have seen in the proof of Lemma 4.2 that res is an isomorphism. For $i \geq 1$, we use the degeneration of the Hochschild–Serre spectral sequence. For this, we make the following observations. Firstly, Proposition 4.3 implies $H^2(G_\Sigma(K_\infty), E[p^\infty]) = 0$. Furthermore, it follows from Lemma 4.2 that $X^{\vec{s}}(E/L_\infty)$ is torsion whenever $X^{\vec{s}}(E/K_\infty)$ is, and so Proposition 4.3 applies with L_∞ in place of K_∞ as well, showing that $H^2(G_\Sigma(L_\infty), E[p^\infty]) = 0$. We have $H^0(G_\Sigma(K_\infty), E[p^\infty]) = E(K_{\infty,\Sigma})[p^\infty] = 0$ and $H^0(G_\Sigma(L_\infty), E[p^\infty]) = 0$: this is because locally at supersingular primes $w \in \Sigma_p^{\mathrm{ss}}(K_\infty)$—which exist by our assumption (S2)—we have $E(K_{\infty,w})[p^\infty] = 0$ due to Lemma 3.1. The vanishing of these cohomology groups together shows degeneration, and we conclude that

$$H^i(H_L, H^1(G_\Sigma(K_\infty), E[p^\infty])) = \begin{cases} H^1(G_\Sigma(L_\infty), E[p^\infty]) & i = 0; \\ 0 & i \geq 1. \end{cases} \tag{11}$$

We turn to the rightmost terms in the long exact sequence. At supersingular primes w, Proposition 3.19 shows that l_u is surjective and $H^i(H_L, J_w(E/K_\infty)) = 0$ for $i \geq 1$. For ordinary primes and at places away from p, we have that $\mathrm{coker}\, l_u$ and $H^i(H_L, J_w(E/K_\infty))$ are all finite by [20, §4].

The assertion about finiteness of the leftmost terms in the sequence follows. □

4.3 Finite submodules of $X^{\vec{s}}(E/K_\infty)$

For the remainder of this subsection, we assume that $\mathrm{Sel}^{\vec{s}}(E/K_\infty)$ is Λ-cotorsion.

Definition 4.5 Let $\Sigma_0 = \Sigma_1 \cup \{v \mid p, E \text{ is ordinary at } v\}$ and let M be a G_K-module. We define

$$\mathrm{Sel}^{\Sigma_0}(M/K_n) = \ker\left(H^1(G_\Sigma(K_n), M[p^\infty]) \to \bigoplus_{v\in\Sigma_0(K_n)} H^1(K_{n,v}, M)[p^\infty]\right)$$

Lemma 4.6 *Assume that* $\mathrm{Sel}^{\vec{s}}(E/K_\infty)$ *is* Λ*-cotorsion. Then we have*

$$\Lambda\text{-corank}(\mathrm{Sel}^{\Sigma_0}(E/K_\infty)) = \Lambda\text{-corank}\left(\bigoplus_{v\in\Sigma(K_\infty)\setminus\Sigma_0(K_\infty)} J_v(E/K_\infty)\right)$$

Proof We have a tautological exact sequence

$$0 \to \mathrm{Sel}^{\vec{s}}(E/K_\infty) \to \mathrm{Sel}^{\Sigma_0}(E/K_\infty) \to \bigoplus_{v\in\Sigma(K_\infty)\setminus\Sigma_0(K_\infty)} J_v(E/K_\infty).$$

As $\mathrm{Sel}^{\vec{s}}(E/K_\infty)$ is Λ-cotorsion by assumption, we obtain

$$\Lambda\text{-corank}(\mathrm{Sel}^{\Sigma_0}(E/K_\infty)) \le \Lambda\text{-corank}\left(\bigoplus_{v\in\Sigma(K_\infty)\setminus\Sigma_0(K_\infty)} J_v(E/K_\infty)\right). \tag{12}$$

By Proposition 4.3 we know that $H^2(G_\Sigma(K_\infty), E[p^\infty]) = 0$. Thus, [13, Proposition 3] implies

$$\Lambda\text{-corank}(H^1(G_\Sigma(K_\infty), E[p^\infty]) = [K_\infty^\Gamma : \mathbb{Q}].$$

Therefore,

$$\begin{aligned}\Lambda\text{-corank}(\mathrm{Sel}^{\Sigma_0}(E/K_\infty)) &\ge [K_\infty^\Gamma : \mathbb{Q}] - \Lambda\text{-corank}\left(\bigoplus_{v\in\Sigma_0(K_\infty)} J_v(E/K_\infty)\right)\\ &= \Lambda\text{-corank}\left(\bigoplus_{v\in\Sigma(K_\infty)\setminus\Sigma_0(K_\infty)} J_v(E/K_\infty)\right). \end{aligned}\tag{13}$$

Combining (12) with (13) gives the desired claim. □

Fix an isomorphism $\kappa : \Gamma \simeq 1+p\mathbb{Z}_p$. For any Γ-module M, let us write $M(t) := M\otimes\kappa^t$ for the Γ-module with κ^t-twisted Γ-action. We have $\mathrm{Sel}^{\vec{s}}(E(t)/K_\infty) = \mathrm{Sel}^{\vec{s}}(E/K_\infty)(t)$; see [14, 89] and [39, §6.2]. Let $d := \Lambda\text{-corank}\left(\bigoplus_{v\in\Sigma(K_\infty)\setminus\Sigma_0(K_\infty)} J_v(E/K_\infty)\right)$. We now choose t such that the following conditions are satisfied for all n.

$$\mathbb{Z}_p\text{-corank}\left((\mathrm{Sel}^{\Sigma_0}(E/K_\infty)\otimes\kappa^t)^{\Gamma_n}\right) = dp^n \tag{14}$$

$$\mathbb{Z}_p\text{-corank}\left((\mathrm{Sel}^{\vec{s}}(E/K_\infty)\otimes\kappa^t)^{\Gamma_n}\right) = 0 \tag{15}$$

$$\mathbb{Z}_p\text{-corank}\left(\left(\bigoplus_{v\in\Sigma_0(K_\infty)} J_v(E/K_\infty)\otimes\kappa^t\right)^{\Gamma_n}\right) = ([K_\infty^\Gamma : \mathbb{Q}] - d)p^n \tag{16}$$

$$\mathbb{Z}_p\text{-corank}\left(H^1(G_\Sigma(K_\infty), E[p^\infty])\otimes\kappa^t)^{\Gamma_n}\right) = [K_\infty^\Gamma : \mathbb{Q}]p^n. \tag{17}$$

The compact Λ-module $(\mathrm{Sel}^{\Sigma_0}(E/K_\infty))^\vee$ is pseudo-isomorphic to $\Lambda^d \oplus W$, where W is a torsion Λ-module. For all but finitely many t the quotients $(W(\kappa^t))_{\Gamma_n}$ are finite for all n. Thus all but finitely many choices of t satisfy (14). Similarly, the other conditions are satisfied for all but finitely many t.

Lemma 4.7 *We have an exact sequence*

$$0 \to \mathrm{Sel}^{\Sigma_0}(E(t)/K_n) \to H^1(G_\Sigma(K_n), E(t)[p^\infty]) \xrightarrow{\varphi_n} \bigoplus_{v\in\Sigma_0(K_n)} J_v(E(t)/K_{n,v})$$

where the rightmost map has finite cokernel.

Proof Note that $H^0(G_\Sigma(K_\infty), E(t)[p^\infty]) = H^0(G_\Sigma(K_\infty), E[p^\infty]) = 0$. Thus, the inflation–restriction exact sequence implies that we have an isomorphism

$$H^1(G_\Sigma(K_n), E(t)[p^\infty]) \cong H^1(G_\Sigma(K_\infty), E(t)[p^\infty])^{\Gamma_n}.$$

It follows that we have a natural embedding $\mathrm{Sel}^{\Sigma_0}(E(t)/K_n) \to \mathrm{Sel}^{\Sigma_0}(E(t)/K_\infty)^{\Gamma_n}$, which in turn implies

$$\mathbb{Z}_p\text{-corank}\left(\mathrm{Sel}^{\Sigma_0}(E(t)/K_n)\right) \le dp^n.$$

we obtain

$$\mathbb{Z}_p\text{-corank}(\mathrm{coker}(\varphi_n)) \le ([K_\infty^\Gamma : \mathbb{Q}] - d)p^n - [K_\infty^\Gamma : \mathbb{Q}]p^n + dp^n = 0.$$

This is only possible if $\mathrm{coker}(\varphi_n)$ is finite. □

Consider now the natural maps

$$\alpha_n \colon H^1(G_\Sigma(K_n), E(t)[p^\infty]) \to \bigoplus_{v\in\Sigma_0(K_n)} H^1(K_{n,v}, E(t)[p^\infty])$$
$$\beta_n \colon H^1(G_\Sigma(K_n), T(-t)) \to \bigoplus_{v\in\Sigma_0(K_n)} H^1(K_{n,v}, T(-t)),$$

where T is the Tate module of $E[p^\infty]$. Note that the images of α and β are orthogonal complements of each other by global Poitou–Tate duality. Let $G_{\alpha_n} \subset \prod_{v\in\Sigma_0(K_n)} H^1(K_{n,v}, E(t)[p^\infty])$ be the smallest subgroup containing $\mathrm{Im}(\alpha_n)$ and $\prod_{v\in\Sigma_0(K_n)} E(t)(K_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$. Let $G_{\beta_n} \subset \prod_{v\in\Sigma_0(K_n)} H^1(K_{n,v}, T(-t))$ be the orthogonal complement of G_{α_n}.

Lemma 4.8 *G_{β_n} lies in $\mathrm{Im}(\beta_n)$, and $\beta_n^{-1}(G_{\beta_n})$ is finite.*

Proof The orthogonal complement of G_{α_n} is contained in the orthogonal complement of $\mathrm{Im}(\alpha_n)$, which is $\mathrm{Im}(\beta_n)$. This proves the first claim. By Lemma 4.7, G_{α_n} has finite index in the direct product $\prod_{v\in\Sigma_0(K_n)} H^1(K_{n,v}, E(t)[p^\infty])$. Thus, G_{β_n} is finite. By global Poitou–Tate duality, the kernel of β_n is isomorphic to

$$\ker\left(H^2(G_\Sigma(K_n), E(t)[p^\infty]) \to \bigoplus_{v\in\Sigma_0(K_n)} H^2(K_{n,v}, E(t)[p^\infty])\right).$$

By (17) and [13, Equation (29)],

$$|H^2(G_\Sigma(K_n), E(t)[p^\infty])| < \infty. \tag{18}$$

Thus, the kernel of β_n is finite and we obtain that $\beta_n^{-1}(G_{\beta_n})$ is finite. □

Lemma 4.9 $\beta_n^{-1}(G_{\beta_n}) = 0$.

Proof By Lemma 4.8 we know that $\beta_n^{-1}(G_{\beta_n}) \subset H^1(G_\Sigma(K_n), T(t))_{\text{tors}}$. We repeat a standard argument from [15]: Consider the tautological exact sequence

$$0 \to T(-t) \to T(-t) \otimes \mathbb{Q}_p \to E(-t)[p^\infty] \to 0.$$

Taking $G_\Sigma(K_n)$ cohomology and using that $H^0(G_\Sigma(K_n), E(-t)[p^\infty]) \subset H^0(G_\Sigma, E[p^\infty]) = 0$, we see that $H^1(G_\Sigma(K_n), T(-t))$ embeds into $H^1(G_\Sigma(K_n), T(-t) \otimes \mathbb{Q}_p)$, which is torsion-free. Therefore, $\beta_n^{-1}(G_{\beta_n})$ has to be trivial. □

Corollary 4.10 *The map φ_n defined in Lemma 4.7 is surjective.*

Proof By Lemma 4.9 we know that $\beta_n^{-1}(G_{\beta_n})$ is trivial. By Lemma 4.8 $G_{\beta_n} \subset \mathrm{Im}(\beta_n)$. Thus, G_{β_n} has to be trivial, hence its complement is $G_{\alpha_n} = \prod_{v \in \Sigma_0(K_n)} H^1(K_{n,v}, E(t)[p^\infty])$, which in turn implies that φ_n has to be surjective by definition. □

Proposition 4.11 *Assume that* $\mathrm{Sel}^{\vec{s}}(E/K_\infty)$ *is* Λ*-cotorsion. Let*

$$\psi_n^{\vec{s}} \colon H^1(G_\Sigma(K_\infty), E(t)[p^\infty])^{\Gamma_n} \to \left(\prod_{v \in \Sigma(K_\infty)} J_v(E(t)/K_\infty) \right)^{\Gamma_n}.$$

Then the cokernel of $\psi_n^{\vec{s}}$ is $\mathbb{Z}_p$-cofree for all n large enough.

Proof The inflation–restriction exact sequence together with Corollary 4.10 implies that we have a surjection

$$\varphi_n^{\Gamma_n} \colon H^1(G_\Sigma(K_\infty), E(t)[p^\infty])^{\Gamma_n} \to \left(\bigoplus_{v \in \Sigma_0(K_\infty)} J_v(E(t)/K_\infty) \right)^{\Gamma_n}.$$

Indeed, for $n \gg 0$ we have

$$\begin{aligned} H^1(G_\Sigma(K_\infty), E[p^\infty]) &= H^1(G_\Sigma(K_n), E[p^\infty])^{\Gamma_n} \\ H^1(K_{n,v}, E[p^\infty]) &\to \bigoplus_{w|v} (H^1(K_{\infty,n}, E[p^\infty]))^{\Gamma_n} \quad \forall v \in \Sigma_0 \\ \widehat{E}(K_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p &= (\bigoplus_{w|v} K_{\infty,v} \otimes \mathbb{Q}_p/\mathbb{Z}_p))^{\Gamma_n} \quad \forall v \in \Sigma_0 \setminus \Sigma_1 \end{aligned}$$

We obtain the following commutative diagram

$$\begin{array}{ccc} H^1(G_\Sigma(K_n), E[p^\infty]) & \xrightarrow{\varphi_n} & \bigoplus_{v \in \Sigma_0(K_n)} J_v(E(t)/K_{n,v}) \\ \downarrow & & \downarrow \\ H^1(G_\Sigma(K_\infty), E[p^\infty])^{\Gamma_n} & \xrightarrow{\varphi_n^{\Gamma_n}} & \left(\bigoplus_{v \in \Sigma_0(K_\infty)} J_v(E(t)/K_\infty) \right)^{\Gamma_n} \end{array}$$

The two vertical arrows and the upper horizontal one are surjective. Thus, the lower vertical map is surjective. We have a tautological exact sequence

$$0 \to \left(\bigoplus_{v \in \Sigma(K_\infty) \setminus \Sigma_0(K_\infty)} J_v(E(t)/K_\infty) \right)^{\Gamma_n} \to \left(\bigoplus_{v \in \Sigma(K_\infty)} J_v(E(t)/K_\infty) \right)^{\Gamma_n} \to \left(\bigoplus_{v \in \Sigma_0(K_\infty)} J_v(E(t)/K_\infty) \right)^{\Gamma_n} \to 0.$$

By Corollary 3.12, the leftmost term is divisible for all n. As $\varphi_n^{\Gamma_n}$ is surjective, we obtain a surjection

$$\left(\bigoplus_{v\in\Sigma(K_\infty)\setminus\Sigma_0(K_\infty)} J_v(E(t)/K_\infty)\right)^{\Gamma_n} \to \operatorname{coker}(\psi_n^{\vec{s}}).$$

As the image of a divisible module is divisible, we obtain a surjection

$$\left(\bigoplus_{v\in\Sigma(K_\infty)} J_v(E(t)/K_\infty)\right)^{\Gamma_n}_{\mathrm{div}} \to \operatorname{coker}(\psi_n^{\vec{s}}),$$

where M_{div} denotes the maximal divisible submodule. As the quotient of divisible submodules is again divisible, the desired claim follows. □

Proposition 4.12 *If $X^{\vec{s}}(E/K_\infty)$ is torsion over Λ, then it has no nonzero finite Λ-submodules.*

Proof Let t be as above. According to Proposition 4.11, there is an exact sequence

$$0 \to \left(\mathrm{Sel}^{\vec{s}}(E(t)/K_\infty)\right)^{\Gamma_n} \to \left(H^1(G_\Sigma(K_\infty), E(t)[p^\infty])\right)^{\Gamma_n} \xrightarrow{\psi_n^{\vec{s}}} \left(\bigoplus_{v\in\Sigma(K_\infty)} J_v(E(t)/K_\infty)\right)^{\Gamma_n}$$

with $\mathbb{Z}_p$-cofree cokernel on the right for every n. For each n, the long exact cohomology sequence associated with taking Γ_n-invariants of the t-twist of the short exact sequence in Proposition 4.3 shows that in particular, the following sequence is exact:

$$0 \to \operatorname{coker}(\psi_n^{\vec{s}}) \to H^1\left(\Gamma_n, \mathrm{Sel}^{\vec{s}}(E(t)/K_\infty)\right) \to H^1\left(\Gamma_n, H^1(G_\Sigma(K_\infty), E(t)[p^\infty])\right).$$

The group on the right vanishes. Indeed, following Ahmed and Lim [2, Lemma 2.5], we have that the Hochschild–Serre spectral sequence $H^i(\Gamma_n, H^j(G_\Sigma(K_\infty), E(t)[p^\infty])) \Rightarrow H^{i+j}(G_\Sigma(K_n), E(t)[p^\infty])$ implies, by the fact that $\mathrm{cd}_p\,\Gamma_n = 1$, that the group in question embeds into $H^2(G_\Sigma(K_n), E(t)[p^\infty])$, which is finite by (18). Then as in [13, 114], we have that $\mathrm{cd}_p\, G_\Sigma(K_n) = 2$ implies that $H^2(G_\Sigma(K_n), E(t)[p^\infty])$ is also divisible, and thus it must be trivial.

In particular, we have that $H^1\left(\Gamma_n, \mathrm{Sel}^{\vec{s}}(E(t)/K_\infty)\right)$ is $\mathbb{Z}_p$-cofree, so its Pontryagin dual $H^0\left(\Gamma_n, \mathrm{Sel}^{\vec{s}}(E(t)/K_\infty)^\vee\right)$ is $\mathbb{Z}_p$-free, which is equivalent to $\mathrm{Sel}^{\vec{s}}(E(t)/K_\infty)^\vee$ having no nonzero finite Λ-submodules by [37, Proposition 5.3.19(i)]. Therefore $\mathrm{Sel}^{\vec{s}}(E/K_\infty)^\vee = X^{\vec{s}}(E/K_\infty)$ has no nonzero finite Λ-submodules either. □

Remark 4.13 The proof of Proposition 4.12 follows that of [30, Proposition 4.5], which in turn relies on ideas of Greenberg [14, Proposition 4.14]. The salient difference in our approach is that the argument in [30] uses an argument involving a local norm compatible sequence and plus/minus Coleman maps constructed in the unramified case by Kim [27, Lemma 3.9ff.], an analogue of which is not known for ramified extensions. This necessitates establishing cofreeness in another way, namely through Proposition 4.11.

4.4 Non-primitive Selmer groups

Let $\Sigma' \subseteq \Sigma_1$ be a subset of the non-p-adic places in Σ. As in Sect. 4.1, let $H_L \leq G$ be a finite subgroup with fixed field L_∞. We define the non-primitive signed Selmer group with respect to Σ' over L_n as

$$\mathrm{Sel}^{\vec{s}}_{\Sigma'}(E/L_n) := \ker\left(H^1(G_\Sigma(L_n), E[p^\infty]) \to \bigoplus_{w\in(\Sigma-\Sigma')(L_n)} J_w(E/L_n)\right).$$

On infinite level, we set $\mathrm{Sel}^{\vec{s}}_{\Sigma'}(E/L_\infty) := \varinjlim_n \mathrm{Sel}^{\vec{s}}_{\Sigma'}(E/L_n)$, so that the previous formula holds for all $n \leq \infty$. We write $X^{\vec{s}}_{\Sigma'}(E/L_\infty)$ for the Pontryagin dual of $\mathrm{Sel}^{\vec{s}}_{\Sigma'}(E/L_\infty)$.

For a finitely generated Λ-module M, let $\theta(M)$ denote the maximal p-exponent in the decomposition into elementary modules. Following [30, Proposition 4.6], we have that non-primitive signed Selmer groups inherit the following properties of signed Selmer groups:

Proposition 4.14 *Assume that* $\mathrm{Sel}^{\vec{s}}(E/K_\infty)$ *is* Λ*-cotorsion.*

(i) $0 \to \mathrm{Sel}^{\vec{s}}(E/K_\infty) \to \mathrm{Sel}^{\vec{s}}_{\Sigma'}(E/K_\infty) \to \bigoplus_{w\in\Sigma'(K_\infty)} H^1(K_{\infty,w}, E[p^\infty]) \to 0.$

(ii) $0 \to \mathrm{Sel}^{\vec{s}}_{\Sigma'}(E/K_\infty) \to H^1(G_\Sigma(K_\infty), E[p^\infty]) \to \bigoplus_{w\in(\Sigma-\Sigma')(K_\infty)} J_w(E/K_\infty) \to 0.$

(iii) $\theta(X^{\vec{s}}_{\Sigma'}(E/K_\infty)) = \theta(X^{\vec{s}}(E/K_\infty))$.

(iv) For every subgroup $H \leq G$ *and* $i \geq 1$*, the group* $H^i\left(H, \mathrm{Sel}^{\vec{s}}_{\Sigma'}(E/K_\infty)\right)$ *is finite.*

(v) $X^{\vec{s}}_{\Sigma'}(E/K_\infty)$ *has no nontrivial finite* Λ*-submodules.*

Proof We have the following commutative diagram with exact rows; the top row is Proposition 4.3, and the bottom row is the definition of the non-primitive Selmer group.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Sel}^{\vec{s}}(E/K_\infty) & \longrightarrow & H^1(G_\Sigma(K_\infty), E[p^\infty]) & \xrightarrow{\psi^{\vec{s}}} & \bigoplus_{w\in\Sigma(K_\infty)} H^1(K_{\infty,w}, E[p^\infty]) & \longrightarrow & 0 \\
 & & \downarrow & & \| & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Sel}^{\vec{s}}_{\Sigma'}(E/K_\infty) & \longrightarrow & H^1(G_\Sigma(K_\infty), E[p^\infty]) & \xrightarrow{\psi^{\vec{s}}_{\Sigma'}} & \bigoplus_{w\in(\Sigma-\Sigma')(K_\infty)} H^1(K_{\infty,w}, E[p^\infty]) & &
\end{array}$$

The sequence (i) follows from the snake lemma. Sequence (ii) is equivalent to surjectivity of $\psi^{\vec{s}}_{\Sigma'}$, which follows from the surjectivity of the other three maps in the right square and commutativity.

Equation (iii) has the same proof as in [30].

For (iv), we take H-invariants of (i), thus obtaining a long exact sequence

$$\ldots \to H^i\left(H, \mathrm{Sel}^{\vec{s}}(E/K_\infty)\right) \to H^i\left(H, \mathrm{Sel}^{\vec{s}}_{\Sigma'}(E/K_\infty)\right) \to H^i\left(H, \bigoplus_{w\in\Sigma'(K_\infty)} H^1(K_{\infty,w}, E[p^\infty])\right) \to \ldots$$

The first term here is finite by Proposition 4.4, and the third one is also finite by [20, §4] (recall that Σ' only contains non-p-adic places). The assertion follows.

Let $t \in \mathbb{Z}$ satisfy the conditions in Section 4.3, and let n be large enough as in the proof of Proposition 4.12. Then (i) is applicable to the twist $E(t)$ of the elliptic curve E, and the long exact sequence associated with taking Γ_n-invariants reads

$$\ldots \to H^i\left(\Gamma_n, \mathrm{Sel}^{\vec{s}}(E/K_\infty)\right) \to H^i\left(\Gamma_n, \mathrm{Sel}^{\vec{s}}_{\Sigma'}(E/K_\infty)\right) \to H^i\left(\Gamma_n, \bigoplus_{w\in\Sigma'(K_\infty)} H^1(K_{\infty,w}, E[p^\infty])\right) \to \ldots$$

The first term is $\mathbb{Z}_p$-cofree, as seen in the last paragraph of the proof of Proposition 4.12, and the third term vanishes. (By the Hochschild–Serre spectral sequence, the group in question embeds into $H^2(K_v, E[p^\infty])$ which is trivial by [34, I.3.4]). Hence the middle term is also $\mathbb{Z}_p$-cofree, and the same argument as used in the end of the proof of Proposition 4.12 shows the claim (v). □

5 Projectivity results

Let

$$\Phi := \{v \in \Sigma_1 \mid \text{the inertia degree of } v \text{ in } K/F \text{ is divisible by } p\}.$$

Theorem 5.1 *Assume that $\Phi \subset \Sigma'$, and that $X^{\vec{s}}(E/K_\infty)$ is Λ-torsion with $\theta(X^{\vec{s}}(E/K_\infty)) \leq 1$. Then $X^{\vec{s}}_{\Sigma'}(E/K_\infty)/X^{\vec{s}}_{\Sigma'}(E/K_\infty)[p]$ is quasi-projective as $\mathbb{Z}_p[G]$-module.*

Proof This proof follows [30, Theorem 4.7]. By Proposition 4.14(iv) $H^i(H, \mathrm{Sel}^{\vec{s}}_{\Sigma'}(E/K_\infty))$ is finite for all subgroups $H \leq G$ and for all $i \geq 1$. In particular, let $C = PQ$ be a cyclic subgroup of G, and ε a character of Q. By Proposition 4.14(ii) and the fact that $|Q|$ is coprime to p, we have a short exact sequence

$$0 \to \mathrm{Sel}^{\vec{s}}_{\Sigma'}(E/K_\infty)^\varepsilon \to H^1(G_\Sigma(K_\infty), E[p^\infty])^\varepsilon \to \left(\bigoplus_{v\in(\Sigma-\Sigma')(K_\infty)} J_w(E/K_\infty)\right)^\varepsilon \to 0.$$

For the middle term, using [14, 3.2 A and 3.2 B], we have

$$h_P(H^1(G_\Sigma(K_\infty), E[p^\infty])^\varepsilon) = h_P\left(\left(\bigoplus_{v\in(\Sigma_1\cup\Sigma_{\mathrm{ord}}-\Sigma')(K_\infty)} J_w(E/K_\infty)\right)^\varepsilon\right) = 1.$$

For the rightmost term, Corollary 3.20 shows

$$h_P\left(\left(\bigoplus_{v\in\Sigma_{\mathrm{ss}}(K_\infty)} J_v(E/K_\infty)\right)^\varepsilon\right) = 1$$

Consequently,

$$h_P(\mathrm{Sel}^{\vec{s}}_{\Sigma'}(E/K_\infty)^\varepsilon) = 1.$$

The claim now follows from Proposition 2.4. □

We recall the following cohomological criterion of Greenberg [12, Proposition 2.4.1] for checking whether an Iwasawa module admits a free resolution of length 1. See also [36, §4] and [30, Proposition 2.14].

Proposition 5.2 *Let Y be a finitely generated $\Lambda(\mathcal{G})$-module that is torsion over Λ and contains no nonzero finite Λ-submodules. Then Y admits a free resolution of length 1 of $\Lambda(\mathcal{G})$-modules if for all subgroups $H \leq G$, the cohomology groups $H^1(H, Y^\vee)$ and $H^2(H, Y^\vee)$ vanish.*

Proposition 5.3 *Assume that $\Phi \subset \Sigma'$, that $X^{\vec{s}}(E/K_\infty)$ is Λ-torsion, and that every ordinary p-adic place $v \in \Sigma_p^{\mathrm{ord}}$ is either non-anomalous (i.e. if $w \mid v$ for w a place of K, then $p \nmid |\tilde{E}(k_w)|$) or ramifies tamely in K/F. Then $X^{\vec{s}}_{\Sigma'}(E/K_\infty)$ admits a free resolution of $\Lambda(\mathcal{G})$-modules of length 1.*

Proof The proof consists of verifying the condition in Greenberg's criterion in the same fashion as in [30, Theorem 4.8]. Let $H_L \leq G$ be a finite subgroup with fixed field L_∞. As in the proof of Proposition 4.4, the short exact sequence of Proposition 4.3 induces a commutative diagram with exact rows:

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Sel}^{\vec{s}}_{\Sigma'}(E/L_\infty) & \longrightarrow & H^1(G_\Sigma(L_\infty), E[p^\infty]) & \longrightarrow & \bigoplus_{u \in (\Sigma-\Sigma')(L_\infty)} J_u(E/L_\infty) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle l=\oplus l_u} & & \\
0 & \longrightarrow & \mathrm{Sel}^{\vec{s}}_{\Sigma'}(E/K_\infty)^{H_L} & \longrightarrow & H^1(G_\Sigma(K_\infty), E[p^\infty])^{H_L} & \longrightarrow & \left(\bigoplus_{w \in (\Sigma-\Sigma')(K_\infty)} J_w(E/K_\infty)\right)^{H_L} & & \\
 & & & & & & & & \\
 & & H^1\left(H_L, \mathrm{Sel}^{\vec{s}}_{\Sigma'}(E/K_\infty)\right) & \longrightarrow & 0 & \longrightarrow & H^1\left(H_L, \bigoplus_{w \in (\Sigma-\Sigma')(K_\infty)} J_w(E/K_\infty)\right) & & \\
 & & & & & & & & \\
 & & H^2\left(H_L, \mathrm{Sel}^{\vec{s}}_{\Sigma'}(E/K_\infty)\right) & \longrightarrow & 0 & & & &
\end{array}
$$

The middle terms in the long exact sequence vanish by (11).

We have $H^1(H_L, J_w(E/K_\infty)) = 0$: for good ordinary p-adic places and for non-p-adic places, this is [12, Proposition 3.1.1], and for supersingular p-adic places, this was shown in Proposition 3.19. Hence $H^2\left(H_L, \mathrm{Sel}^{\vec{s}}_{\Sigma'}(E/K_\infty)\right) = 0$. The cited statements also show that l_u is surjective for all u, and thus $0 = \mathrm{coker}(l)$. Commutativity of the diagram shows $\mathrm{coker}(l) = H^1\left(H_L, \mathrm{Sel}^{\vec{s}}_{\Sigma'}(E/K_\infty)\right)$. Hence Greenberg's criterion applies. □

6 Kida's formula

Let L be a number field contained in K such that the extensions L/F and K/F satisfy conditions (S1)–(S3) of Sect. 4. Assume furthermore that K/L is Galois and that $\mathrm{Gal}(K/L)$ is a p-group. Let Σ' be the set of all places $v \nmid p$ in L such that the ramification index of v in K/L is divisible by p.

Lemma 6.1 *Let $v \in \Sigma'$. Then $\mu_p \subset L_v$.*

Proof The proof is the same as [30, Lemma 5.1]. □

Proposition 6.2 *Assume that* $\mathrm{Sel}^{\vec{s}}(E/K_\infty)$ *is* Λ*-cotorsion. Assume that* $\theta(X^{\vec{s}}_{\Sigma'}(E/K_\infty)) \leq 1$. *Then we have*

$$\lambda(X^{\vec{s}}_{\Sigma'}(E/K_\infty)) = [K_\infty : L_\infty] \cdot \lambda(X^{\vec{s}}_{\Sigma'}(E/L_\infty))$$
$$\mu(X^{\vec{s}}_{\Sigma'}(E/K_\infty)) = [K_\infty : L_\infty] \cdot \mu(X^{\vec{s}}_{\Sigma'}(E/L_\infty)).$$

Proof The proof of this proposition is analogous to [21, Theorem 2.1]. Note that it suffices to prove the proposition for the case that $[K_\infty : L_\infty] = p$. Proposition 4.14(i) implies that $\mathrm{Sel}^{\vec{s}}_{\Sigma'}(E/K_\infty)$ is Λ-cotorsion. As before, let $H_L \leq G$ be a finite subgroup with fixed field L_∞, and consider the following commutative diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Sel}^{\vec{s}}_{\Sigma'}(E/L_\infty) & \longrightarrow & H^1(G_\Sigma(L_\infty), E[p^\infty]) & \longrightarrow & \bigoplus_{u\in(\Sigma-\Sigma')(L_\infty)} J_u(E/L_\infty) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle l=\oplus l_u} & & \\
0 & \longrightarrow & \mathrm{Sel}^{\vec{s}}_{\Sigma'}(E/K_\infty)^{H_L} & \longrightarrow & H^1(G_\Sigma(K_\infty), E[p^\infty])^{H_L} & \longrightarrow & \bigoplus_{u\in(\Sigma-\Sigma')(K_\infty)} J_u(E/K_\infty)^{H_L} & &
\end{array}$$

Note that the top row is exact by Proposition 4.14(ii). As the middle vertical map is an isomorphism and the right vertical map is surjective (compare with the proof of Proposition 5.3), the restriction

$$\mathrm{Sel}^{\vec{s}}_{\Sigma'}(E/L_\infty) \to \mathrm{Sel}^{\vec{s}}_{\Sigma'}(E/K_\infty)^{H_L}$$

is injective with finite cokernel. In particular,

$$\lambda((X^{\vec{s}}_{\Sigma'}(E/K_\infty))^{H_L}) = \lambda(X^{\vec{s}}_{\Sigma'}(E/L_\infty)), \quad \mu((X^{\vec{s}}_{\Sigma'}(E/K_\infty))^{H_L}) = \mu(X^{\vec{s}}_{\Sigma'}(E/L_\infty)).$$

Proposition 4.14(iii) implies that $H^i(H_L, \mathrm{Sel}^{\vec{s}}_{\Sigma'}(E/K_\infty))$ is finite for all $i > 0$. Therefore, $H^i(H_L, X^{\vec{s}}_{\Sigma'}(E/K_\infty))$ is finite for all $i > 0$. In particular it has vanishing μ-invariant. We can now apply Lemma 2.2 to conclude that

$$h(X^{\vec{s}}_{\Sigma'}(E/K_\infty)[p^\infty]) = 1, \quad \mu(X^{\vec{s}}_{\Sigma'}(E/K_\infty)) = p\mu(X^{\vec{s}}_{\Sigma'}(E/L_\infty)) \tag{19}$$

which proves the claim on μ-invariants.

It remains to show the claim on λ-invariants. Using again Proposition 4.14(ii) we deduce that

$$h(\mathrm{Sel}^{\vec{s}}_{\Sigma'}(E/K_\infty)) = \frac{h(H^1(G_\Sigma(K_\infty), E[p^\infty]))}{h\left(\bigoplus_{v\in(\Sigma-\Sigma')(K_\infty)} J_v(E/K_\infty)\right)}$$

By [14, 3.2 A und B], $h(H^1(G_\Sigma(K_\infty), E[p^\infty])) = h(J_v(E/K_\infty)) = 1$ for all places in $(\Sigma_1 - \Sigma')(K_\infty)$ and for all ordinary primes above p. For the supersingular primes $h(J_v(E/K_\infty)) = 1$ by Corollary 3.20. Thus,

$$1 = h(X^{\vec{s}}_{\Sigma'}(E/K_\infty)). \tag{20}$$

Let $Z = X^{\vec{s}}_{\Sigma'}(E/K_\infty)/X^{\vec{s}}_{\Sigma'}(E/K_\infty)[p^\infty]$. Then Z is $\mathbb{Z}_p$-free and $\lambda(Z) = \lambda(X^{\vec{s}}_{\Sigma'}(E/K_\infty))$. For the H_L-coinvariants Z_{H_L}, we have $\lambda(Z_{H_L}) = \lambda(X^{\vec{s}}_{\Sigma'}(E/L_\infty))$ and $h(Z) = 1$ by (19) and (20). We can now conclude as in [21] that

$$\lambda(Z) = p(\lambda(Z_{H_L}) - v_p(h(Z))) + v_p(h(Z)) = p\lambda(Z_{H_L}),$$

which concludes the proof. □

Theorem 6.3 *Assume that* $\mathrm{Sel}^{\vec{s}}(E/K_\infty)$ *is* Λ*-cotorsion and that* $\theta(X^{\vec{s}}(E/K_\infty)) \leq 1$. *Let* $P_1 \subset \Sigma'$ *be the primes where E has split multiplicative reduction and let* P_2 *be the set of primes in* Σ' *where E has good reduction and* $E(K)[p] \neq 0$. *Then we have*

$$\lambda(X^{\vec{s}}(E/K_\infty)) = [K_\infty : L_\infty]\lambda(X^{\vec{s}}(E/L_\infty)) + \sum_{v\in P_1}(e_v - 1) + 2\sum_{w\in P_2}(e_v - 1)$$

and

$$\mu(X^{\vec{s}}(E/K_\infty)) = [K_\infty : L_\infty]\mu(X^{\vec{s}}(E/L_\infty)).$$

Proof By Proposition 4.14(i) we have that $\mathrm{Sel}^{\vec{s}}_{\Sigma'}(E/K_\infty)$ is Λ-cotorsion and that

$$\lambda(X^{\vec{s}}(E/K_\infty)) = \lambda(X^{\vec{s}}_{\Sigma'}(E/K_\infty)) - \sum_{v\in\Sigma'(K_\infty)}\lambda(J_v(E/K_\infty))$$

and

$$\mu(X^{\vec{s}}(E/K_\infty)) = \mu(X^{\vec{s}}_{\Sigma'}(E/K_\infty)) - \sum_{v\in\Sigma'(K_\infty)}\mu(J_v(E/K_\infty)).$$

By Proposition 4.14(iii) we can apply Proposition 6.2 and obtain

$$\begin{aligned}\lambda(X^{\vec{s}}(E/K_\infty)) &= [K_\infty : L_\infty]\lambda(X^{\vec{s}}(E/L_\infty)) \\ &\quad + [K_\infty : L_\infty]\sum_{v\in\Sigma'(L_\infty)}\lambda(J_v(E/L_\infty)) - \sum_{v\in\Sigma'(K_\infty)}\lambda(J_v(E/K_\infty))\end{aligned}$$

and

$$\begin{aligned}\mu(X^{\vec{s}}(E/K_\infty)) &= [K_\infty : L_\infty]\mu(X^{\vec{s}}(E/L_\infty)) \\ &\quad + [K_\infty : L_\infty]\sum_{v\in\Sigma'(L_\infty)}\mu(J_v(E/L_\infty)) - \sum_{v\in\Sigma'(K_\infty)}\mu(J_v(E/K_\infty)).\end{aligned}$$

The claim now follows by analysing the terms $\lambda(J_v(E/K_\infty))$ as in [30, proof of Proposition 5.2] using [13] and [20] and from the fact that $\mu(J_w(E/K_\infty)) = 0$ [14, Proposition 2]. □

7 Integrality of characteristic elements

In this section, we generalise Lim's integrality results on characteristic elements of signed Selmer groups [30, §5.2].

Let $\mathcal{Q}(\mathcal{G})$ denote the total ring of quotients of the Iwasawa algebra $\Lambda(\mathcal{G})$. Let $\partial : K_1(\mathcal{Q}(\mathcal{G})) \to K_0(\Lambda(\mathcal{G}), \mathcal{Q}(\mathcal{G}))$ denote the connecting homomorphism in the localisation exact sequence of relative K-theory; for details, we refer to [42, p. 29ff.]. For a finitely generated $\Lambda(\mathcal{G})$-module Y that is torsion over Λ and has projective dimension $\mathrm{pd}_{\Lambda(\mathcal{G})} Y \leq 1$, a characteristic element is an element $\xi_Y \in K_1(\mathcal{Q}(\mathcal{G}))$ whose image $\partial(\xi_Y) \in K_0(\Lambda(\mathcal{G}), \mathcal{Q}(\mathcal{G}))$ agrees with the class of Y in the relative K_0-group.

Let n_0 be a large enough integer such that $\Gamma_0 := \Gamma^{p^{n_0}}$ is central in $\mathcal{G}$, and let $\Lambda(\Gamma_0) := \mathbb{Z}_p[\![\Gamma_0]\!] \subset \Lambda(\mathcal{G})$ denote the corresponding Iwasawa algebra. Recall that a $\Lambda(\Gamma_0)$-order $\mathfrak{M}$ in $\mathcal{Q}(\mathcal{G})$ is called a graduated order if there exist orthogonal indecomposable idempotents $e_1, \ldots, e_t \in \mathfrak{M}$ such that $e_i \mathfrak{M} e_i$ is a maximal order in $e_i \mathcal{Q}(\mathcal{G}) e_i$ for each $i = 1, \ldots t$. In particular, every maximal order is graduated [38, Theorem 10.5.(i)]. Graduated orders over Iwasawa algebras have been studied in [10].

Theorem 7.1 *Let E be an elliptic curve satisfying (S1), (S2) and (S3), and suppose that the conditions of Proposition 5.3 hold. Let $\xi_{E,\Sigma'}$ denote a characteristic element of $X^{\vec{s}}_{\Sigma'}(E/K_\infty)$. Then for every graduated $\Lambda(\Gamma_0)$-order $\mathfrak{M}$ of $\mathcal{Q}(\mathcal{G})$ containing $\Lambda(\mathcal{G})$, we have*

$$\xi_{E,\Sigma'} \in \mathrm{Im}\left(\mathfrak{M} \cap \mathcal{Q}(\mathcal{G})^\times \to K_1(\mathcal{Q}(\mathcal{G}))\right).$$

Proof The skew fields occurring in the Wedderburn decomposition of $\mathcal{Q}(\mathcal{G})$ are given explicitly in [11, Theorem 4.12]. This shows that $\mathcal{Q}(\mathcal{G})$ meets the conditions of [10, Proposition 2.7], which provides a description of graduated orders. Moreover, it is shown in [9, Proposition 6.2] that Nichifor–Palvannan's dimension reduction argument [36, Proposition 2.13] can be generalised to such rings.

Since Proposition 5.3 shows that $X^{\vec{s}}_{\Sigma'}(E/K_\infty)$ admits a free resolution of length 1, the assertion can be proven by the same argument as in [10, Corollary 4.3], which follows along the lines of [36, Theorem 1] and [9, Corollary 7.6]. □

Corollary 7.2 *Keep the assumptions of Theorem 7.1, and further assume that Φ contains no places at which E has either split multiplicative reduction or good reduction with $E(K_{\infty,w})[p] \neq 0$ (i.e. $P_1 = P_2 = \emptyset$ in the notation of Theorem 6.3). Let ξ_E denote a characteristic element of $X^{\vec{s}}(E/K_\infty)$. Then for every graduated $\Lambda(\Gamma_0)$-order $\mathfrak{M}$ containing $\Lambda(\mathcal{G})$, we have*

$$\xi_E \in \mathrm{Im}\left(\mathfrak{M} \cap \mathcal{Q}(\mathcal{G})^\times \to K_1(\mathcal{Q}(\mathcal{G}))\right).$$

Proof The proof is identical to [30, Proposition 5.5]: indeed, the short exact sequence of Proposition 4.14(i) combined with the corank analysis in the proof of [30, Proposition 5.2] shows that

$$\left[X^{\vec{s}}(E/K_\infty)\right] = \left[X^{\vec{s}}_{\Sigma'}(E/K_\infty)\right] \in K_0(\Lambda(\mathcal{G}), \mathcal{Q}(\mathcal{G}))$$

under setting $\Sigma' := \Phi$. The claim now follows from Theorem 7.1. □

8 Behavior of Iwasawa invariants under congruences

Let E_1 and E_2 be elliptic curves defined over F and assume that $E_1[p] \cong E_2[p]$ as G_K-modules. Let Σ be a finite set of places of F satisfying (4), containing the places at which E_1 or E_2 has bad reduction. Recall that $\Sigma_1 = \Sigma - \Sigma_p$ is the set of non-p-adic places in Σ.

Definition 8.1 Assume that $X^{\vec{s}}(E_i/K_\infty)$ is Λ-torsion for $1 \leq i \leq 2$. For $E \in \{E_1, E_2\}$, we define the p-primary signed Selmer group as

$$\mathrm{Sel}^{\vec{s}}(E[p]/K_\infty) = \ker\left(H^1(G_\Sigma(K_\infty), E[p]) \to \bigoplus_{v \in \Sigma(K_\infty)} J_v(E[p]/K_\infty)\right),$$

where $J_v(E[p]/K_\infty)$ is defined by case distinction:

$$J_v(E[p]/K_\infty) = \begin{cases} H^1(K_{\infty,v}, E[p]) & \text{if } v \in \Sigma_1(K_\infty), \\ \frac{H^1(K_{\infty,v}, E[p])}{E(K_{\infty,v})/pE(K_{\infty,v})} & \text{if } v \in \Sigma^{\mathrm{ord}}(K_\infty), \\ \frac{H^1(K_{\infty,v}, E[p])}{\widehat{E^\pm}(K_{\infty,v})/p\widehat{E^\pm}(K_{\infty,v})} & \text{if } v \in \Sigma^{\mathrm{ss}}(K_\infty). \end{cases}$$

We define the non-primitive version as

$$\mathrm{Sel}^{\vec{s}}_{\Sigma_1}(E[p]/K_\infty) = \ker\left(H^1(G_\Sigma(K_\infty), E[p]) \to \bigoplus_{v \in (\Sigma - \Sigma_1)(K_\infty)} J_v(E[p]/K_\infty)\right),$$

Lemma 8.2 *Then there is a natural isomorphism*

$$\mathrm{Sel}^{\vec{s}}_{\Sigma_1}(E_i[p]/K_\infty) \cong \mathrm{Sel}^{\vec{s}}_{\Sigma_1}(E_i/K_\infty)[p].$$

Proof We have a commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Sel}^{\vec{s}}_{\Sigma_1}(E_i[p]/K_\infty) & \longrightarrow & H^1(G_\Sigma(K_\infty), E_i[p]) & \longrightarrow & \bigoplus_{v \in (\Sigma - \Sigma_1)(K_\infty)} J_v(E_i[p]/K_\infty) \\ & & \downarrow & & \| & & \downarrow{\scriptstyle \oplus_v d_v} \\ 0 & \longrightarrow & \mathrm{Sel}^{\vec{s}}_{\Sigma_1}(E_i/K_\infty)[p] & \longrightarrow & H^1(G_\Sigma(K_\infty), E_i[p^\infty])[p] & \longrightarrow & \bigoplus_{v \in (\Sigma - \Sigma_1)(K_\infty)} J_v(E_i[p^\infty]/K_\infty) \end{array}$$

Here $J_v(E_i[p^\infty]/K_\infty)$ is defined analogously to Definition 8.1. One can easily check that d_v is injective for ordinary primes v (see also [15, proof of Proposition 2.8]). For supersingular v, Lemma 3.21 implies that d_v is injective. Thus, the left vertical map is surjective by the snake Lemma. □

Proposition 8.3 *Assume that $E_1[p] \cong E_2[p]$ as G_K-modules. Assume that $X^{\vec{s}}_{\Sigma_1}(E_1/K_\infty)$ is Λ-torsion and finitely generated over $\mathbb{Z}_p$. Then the same is true for $X^{\vec{s}}_{\Sigma_1}(E_2/K_\infty)$ and the λ-invariants are the same.*

Proof As $E_1[p] \cong E_2[p]$, we obtain an isomorphism

$$X^{\vec{s}}_{\Sigma_1}(E_1[p]/K_\infty) \cong X^{\vec{s}}_{\Sigma_1}(E_2[p]/K_\infty).$$

By Lemma 8.2 we have isomorphisms

$$X^{\vec{s}}_{\Sigma_1}(E_i[p]/K_\infty) \cong X^{\vec{s}}_{\Sigma_1}(E_i/K_\infty)\big/pX^{\vec{s}}_{\Sigma_1}(E_i/K_\infty)$$

for $1 \leq i \leq 2$. Thus, if $X^{\vec{s}}_{\Sigma_1}(E_1/K_\infty)$ is finitely generated over $\mathbb{Z}_p$, the same is true for $X^{\vec{s}}_{\Sigma_1}(E_2/K_\infty)$.

It remains to prove the claim concerning λ-invariants. By Proposition 4.14(v) $X^{\vec{s}}_{\Sigma_1}(E_i/K_\infty)$ does not contain a non-trivial finite submodule. Thus, if it is finitely generated over $\mathbb{Z}_p$, we have

$$\lambda(X^{\vec{s}}_{\Sigma_1}(E/K_\infty)) = \nu_p\left(\left|X^{\vec{s}}_{\Sigma_1}(E/K_\infty)\big/pX^{\vec{s}}_{\Sigma_1}(E/K_\infty)\right|\right).$$

The claim now follows from the two isomorphisms above. □

Theorem 8.4 *Assume that $E_1[p] \cong E_2[p]$ as G_K-modules. Assume that $X^{\vec{s}}(E_1/K_\infty)$ is Λ-torsion and finitely generated over $\mathbb{Z}_p$. Then the same is true for $X^{\vec{s}}(E_2/K_\infty)$ and we get the following equality of λ-invariants*

$$\lambda(X^{\vec{s}}(E_1/K_\infty)) + \sum_{v\in\Sigma_1}\lambda(J_v(E_1/K_\infty)^\vee) = \lambda(X^{\vec{s}}(E_2/K_\infty)) + \sum_{v\in\Sigma_1}\lambda(J_v(E_2/K_\infty)^\vee).$$

Similar results have been achieved by a number of authors. Greenberg–Vatsal compared algebraic and analytic Iwasawa invariants of modular elliptic curves under the assumption that $E_1[p] \cong E_2[p]$ is irreducible [15, Theorem 1.4]. B.D. Kim established equality of λ-invariants of non-primitive plus/minus Selmer groups of congruent elliptic curves over $\mathbb{Q}$ [26, Corollary 2.13]. Ahmed–Aribam–Shekhar studied the parity of λ-invariants and root numbers of congruent elliptic curves defined over $\mathbb{Q}$ while assuming irreducibility [1]. Ahmed–Lim compared λ-invariants of signed Selmer groups under an unramifiedness assumption at supersingular places [3]. Our Theorem 8.4 can be seen as a generalisation of these results on algebraic Iwasawa invariants to our setting.

The question has also been studied for anticyclotomic Selmer groups by Hatley–Lei [18, Proposition 5.4] [19, Theorem 4.6]. In the context of ordinary modular forms, a similar result is due to Emerton–Pollack–Weston [8, Theorem 2]. In the supersingular case, Hatley–Lei compared λ-invariants of signed Selmer groups of two modular forms of the same even weight that are congruent modulo p [17, Theorem 4.6].

Proof of Theorem 8.4 By [13, Proposition 2] the modules $J_v(E_i/K_\infty)^\vee$ are finitely generated over $\mathbb{Z}_p$. Therefore Proposition 4.14(i) implies that $X^{\vec{s}}_{\Sigma_1}(E_i/K_\infty)$ is finitely generated over $\mathbb{Z}_p$ if and only if the same is true for $X^{\vec{s}}(E_i/K_\infty)$. In this case we obtain the following equality of Iwasawa invariants:

$$\lambda(X^{\vec{s}}(E_i/K_\infty)) + \sum_{v\in\Sigma_1}\lambda(J_v(E_i/K_\infty)^\vee) = \lambda(X^{\vec{s}}_{\Sigma_1}(E_i/K_\infty)).$$

The desired claim now follows from Proposition 8.3. □

Acknowledgements
The authors would like to thank Andreas Nickel for various and extensive comments on a draft version of this paper, as well as Cornelius Greither for helpful remarks. They also thank the referees for insightful comments and useful suggestions.

Funding Open Access funding enabled and organized by Projekt DEAL.

Data availability All relevant data are contained within the manuscript.

Received: 11 November 2024 Accepted: 6 May 2025
Published online: 20 May 2025

References

1. Ahmed, S., Aribam, C., Shekhar, S.: Root numbers and parity of local Iwasawa invariants. J. Number Theory **177**, 285–306 (2017). https://doi.org/10.1016/j.jnt.2017.01.019
2. Ahmed, S., Lim, M.F.: On the Euler characteristics of signed Selmer groups. Bull. Aust. Math. Soc. **101**(2), 238–246 (2020). https://doi.org/10.1017/s0004972719000704
3. Ahmed, S.: On the signed Selmer groups of congruent elliptic curves with semistable reduction at all primes above *p*. Acta Arith. **197**(4), 353–377 (2021). https://doi.org/10.4064/aa190711-21-6
4. Coates, J., Greenberg, R.: Kummer theory for abelian varieties over local fields. Invent. Math. **124**(1–3), 129–174 (1996). https://doi.org/10.1007/s002220050048
5. Coates, J., et al.: The GL_2 main conjecture for elliptic curves without complex multiplication. Publ. Math. Inst. Hautes Études Sci. **101**, 163–208 (2005). https://doi.org/10.1007/s10240-004-0029-3
6. Coates, J., Sujatha, R.: Galois Cohomology of Elliptic Curves. Second. Narosa Publishing House, New Delhi; for the Tata Institute of Fundamental Research, Mumbai, p. xii+98 (2010). ISBN: 978-81-8487-023-7
7. Ellerbrock, N., Nickel, A.: On formal groups and Tate cohomology in local fields. Acta Arith. **182**(3), 285–299 (2018). https://doi.org/10.4064/aa170509-5-12
8. Emerton, M., Pollack, R., Weston, T.: Variation of Iwasawa invariants in Hida families. Invent. Math. **163**(3), 523–580 (2006). https://doi.org/10.1007/s00222-005-0467-7
9. Forrás, B.: An equivariant *p*-adic Artin conjecture. arXiv:2404.15078 [math.NT] (2024)
10. Forrás, B.: Graduated orders over completed group rings and conductor formulælig. arXiv:2502.15560 [math.RA] (2025)
11. Forrás, B.: On the Wedderburn decomposition of the total ring of quotients of certain Iwasawa algebras. arXiv:2403.04663 [math.RA] (2025)
12. Greenberg, R.: Iwasawa theory, projective modules, and modular representations. Mem. Am. Math. Soc. **211**(992), vi+185 (2011). https://doi.org/10.1090/S0065-9266-2010-00608-2
13. Greenberg, R.: Iwasawa theory for *p*-adic representations. In: Algebraic Number Theory. Advanced Studies in Pure Mathematics, vol. 17, pp. 97–137. Academic Press, Boston (1989). https://doi.org/10.2969/aspm/01710097
14. Greenberg, R.: Iwasawa theory for elliptic curves. In: Viola, C. (ed.) Arithmetic Theory of Elliptic Curves: Lectures Given at the 3rd Session of the Centro Internazionale Matematico Estivo (C.I.M.E.) Held in Cetraro, Italy, July 12–19, 1997, pp. 51–144. Springer, Berlin, Heidelberg (1999). https://doi.org/10.1007/BFb0093453
15. Greenberg, R., Vatsal, V.: On the Iwasawa invariants of elliptic curves. Invent. Math. **142**(1), 17–63 (2000). https://doi.org/10.1007/s002220000080
16. Hazewinkel, M.: On norm maps for one dimensional formal groups. I. The cyclotomic Γ-extension. J. Algebra **32**, 89–108 (1974). https://doi.org/10.1016/0021-8693(74)90173-2
17. Hatley, J., Lei, A.: Arithmetic properties of signed Selmer groups at non-ordinary primes. Ann. Inst. Fourier (Grenoble) **69**(3), 1259–1294 (2019). https://doi.org/10.5802/aif.3270
18. Hatley, J., Lei, A.: Comparing anticyclotomic Selmer groups of positive coranks for congruent modular forms. Math. Res. Lett. **26**(4), 1115–1144 (2019). https://doi.org/10.4310/MRL.2019.v26.n4.a7
19. Hatley, J., Lei, A.: Comparing anticyclotomic Selmer groups of positive coranks for congruent modular forms—part II. J. Number Theory **229**, 342–363 (2021). https://doi.org/10.1016/j.jnt.2021.05.004
20. Hachimori, Y., Matsuno, K.: An analogue of Kida's formula for the Selmer groups of elliptic curves. J. Algebr. Geom. **8**(3), 581–601 (1999)
21. Hachimori, Y., Sharifi, R.T.: On the failure of pseudo-nullity of Iwasawa modules. J. Algebr. Geom. **14**(3), 567–591 (2005). https://doi.org/10.1090/S1056-3911-05-00396-6
22. Iovita, A., Pollack, R.: Iwasawa theory of elliptic curves at supersingular primes over $\mathbb{Z}_p$-extensions of number fields. J. Reine Angew. Math. **598**, 71–103 (2006). https://doi.org/10.1515/CRELLE.2006.069
23. Iwasawa, K.: Riemann-Hurwitz formula and *p*-adic Galois representations for number fields. Tohoku Math. J. (2) **33**(2), 263–288 (1981). https://doi.org/10.2748/tmj/1178229453
24. Kataoka, T.: Kida's formula via Selmer complexes. arXiv:2401.07036 [math.NT] (2024)
25. Kim, B.D.: The parity conjecture for elliptic curves at supersingular reduction primes. Compos. Math. **143**(1), 47–72 (2007). https://doi.org/10.1112/S0010437X06002569
26. Kim, B.D.: The Iwasawa invariants of the plus/minus Selmer groups. Asian J. Math. **13**(2), 181–190 (2009). https://doi.org/10.4310/AJM.2009.v13.n2.a2
27. Kim, B.D.: The plus/minus Selmer groups for supersingular primes. J. Aust. Math. Soc. **95**(2), 189–200 (2013). https://doi.org/10.1017/S1446788713000165
28. Kitajima, T., Otsuki, R.: On the plus and the minus selmer groups for elliptic curves at supersingular primes. Tokyo J. Math. **41**(1), 273–303 (2018). https://doi.org/10.3836/tjm/1502179270
29. Kobayashi, S.: Iwasawa theory for elliptic curves at supersingular primes. Invent. Math. **152**, 1–36 (2003). https://doi.org/10.1007/s00222-002-0265-4
30. Lim, M.F.: On the cohomology of Kobayashi's plus/minus norm groups and applications. Math. Proc. Camb. Philos. Soc. **173**(1), 1–24 (2022). https://doi.org/10.1017/S0305004121000396
31. Lei, A., Lim, M.F.: Mordell-Weil ranks and Tate-Shafarevich groups of elliptic curves with mixed-reduction type over cyclotomic extensions. Int. J. Number Theory **18**(2), 303–330 (2022). https://doi.org/10.1142/S1793042122500208

32. Lei, A., Loeffler, D., Zerbes, S.L.: Wach modules and Iwasawa theory for modular forms. Asian J. Math. **14**(4), 475–528 (2010). https://doi.org/10.4310/AJM.2010.v14.n4.a2
33. Lei, A., Zerbes, S.L.: Signed Selmer groups over *p*-adic Lie extensions. J. Théor. Nombres Bordeaux **24**(2), 377–403 (2012)
34. Milne, J.S.: Arithmetic Duality Theorems, 2nd edn., p. viii+339. BookSurge, LLC (2006). ISBN: 1-4196-4274-X
35. Neukirch, J.: Algebraische Zahlentheorie, p. xiii+595. Springer-Verlag, Berlin (1992). https://doi.org/10.1007/978-3-540-37663-7
36. Nichifor, A., Palvannan, B.: On free resolutions of Iwasawa modules. Doc. Math. **24**, 609–662 (2019)
37. Neukirch, J., Schmidt, A., Wingberg, K.: Cohomology of Number Fields, 2.3 electronic edn. Springer, Berlin (2020)
38. Reiner, I.: Maximal orders. In: London Mathematical Society Monographs. New Series, vol. 28. Corrected Reprint of the 1975 Original, with a Foreword by M. J. Taylor, p. xiv+395. The Clarendon Press, Oxford University Press, Oxford (2003). ISBN: 0-19-852673-3
39. Rubin, K.: Euler systems. In: Annals of Mathematics Studies. Hermann Weyl Lectures. The Institute for Advanced Study, vol. 147, p. xii+227. Princeton University Press, Princeton (2000). ISBN: 0-691-05076-7. https://doi.org/10.1515/9781400865208
40. Schneider, P.: Arithmetic of formal groups and applications. I. Universal norm subgroups. Invent. Math. **87**(3), 587–602 (1987). https://doi.org/10.1007/BF01389244
41. Serre, J.-P.: Local fields. In: Graduate Texts in Mathematics, vol. 67. Translated from the French by Marvin Jay Greenberg, p. viii+241. Springer-Verlag, New York-Berlin (1979). ISBN: 0-387-90424-7
42. Sujatha, R.: Reductions of the main conjecture. In: Springer Proceedings in Mathematics and Statistics 29 (2013). https://doi.org/10.1007/978-3-642-32199-3_2

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.