JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Antonio LEI et Meng Fai LIM

Akashi series and Euler characteristics of signed Selmer groups of elliptic curves with semistable reduction at primes above p

Tome 33, n° 3.2 (2021), p. 997-1019.

<http://jtnb.centre-mersenne.org/item?id=JTNB_2021__33_3.2_997_0>

Journal de Théorie des Nombres
de Bordeaux **33** (2021), 997–1019

Akashi series and Euler characteristics of signed Selmer groups of elliptic curves with semistable reduction at primes above p

par Antonio LEI et Meng Fai LIM

Résumé. Soit p un nombre premier impair, et soit E une courbe elliptique définie sur un corps des nombres F' ayant réduction semi-stable en chaque premier de F' sur p et ayant réduction supersingulière en au moins un premier sur p. Sous des hypothèses appropriées, nous calculons la série d'Akashi des groupes de Selmer signés de E sur une $\mathbb{Z}_p^d$-extension d'une extension finie F de F'. Comme un sous-produit, nous calculons aussi le caractéristique d'Euler de ces groupes de Selmer.

Abstract. Let p be an odd prime number, and let E be an elliptic curve defined over a number field F' such that E has semistable reduction at every prime of F' above p and is supersingular at least one prime above p. Under appropriate hypotheses, we compute the Akashi series of the signed Selmer groups of E over a $\mathbb{Z}_p^d$-extension over a finite extension F of F'. As a by-product, we also compute the Euler characteristics of these Selmer groups.

1. Introduction

Throughout this article, p will always denote an odd prime number. Let E be an elliptic curve defined over a number field F'. If E has good ordinary reduction at every prime of F' above p and F is a finite extension of F', the p-primary Selmer group of E over the cyclotomic $\mathbb{Z}_p$-extension F^{cyc} of F is conjectured to be cotorsion over $\mathbb{Z}_p[\![\Gamma]\!]$ (meaning that its Pontryagin dual is torsion over $\mathbb{Z}_p[\![\Gamma]\!]$; see [29]), where $\Gamma = \mathrm{Gal}(F^{\mathrm{cyc}}/F)$. Granted this conjecture, Perrin-Riou [33] and Schneider [36, 37] computed the Γ-Euler characteristics of the aforementioned Selmer group and showed that its value is related to the p-part of the algebraic invariants appearing in the formula of the Birch and Swinnerton-Dyer conjecture. Their calculations

Manuscrit reçu le 26 janvier 2020, révisé le 11 août 2020, accepté le 18 septembre 2020.
2010 *Mathematics Subject Classification.* 11G05, 11R23.
Mots-clefs. Akashi series, signed Selmer groups, Euler characteristics.
We would like to thank the anonymous referee for constructive comments on an earlier version of this article. The authors' research is partially supported by: the NSERC Discovery Grants Program RGPIN-2020-04259 and RGPAS-2020-00096 (Lei) and the National Natural Science Foundation of China under Grant numbers 11550110172 and 11771164 (Lim).

have since then been extended to higher dimensional p-adic Lie extensions (see [6, 7, 10, 39, 40, 41]).

If E has supersingular reduction at one prime above p, then the p-primary Selmer group of E over F^{cyc} is not expected to be cotorsion over $\mathbb{Z}_p[\![\Gamma]\!]$ (see [6, 37]). When $F = F' = \mathbb{Q}$, Kobayashi [20] defined the plus and minus Selmer groups of E over $\mathbb{Q}^{\mathrm{cyc}}$ by constructing the plus and minus norm groups $\widehat{E}^{\pm}(\mathbb{Q}_p^{\mathrm{cyc}})$, which are subgroups of the formal group of E at p. He was able to describe the algebraic structure of these plus and minus norm groups precisely and show that the plus and minus Selmer groups are cotorsion over $\mathbb{Z}_p[\![\Gamma]\!]$. These Selmer groups have been extended to different settings by various authors (see [1, 2, 3, 15, 16, 17, 18, 19, 21, 23, 24, 25, 31]). When E is defined over $\mathbb{Q}$ and F is a number field where p is unramified, Kim [15, 16] studied the structure of plus and minus Selmer groups over F^{cyc}. In particular, he showed that these Selmer groups do not contain non-trivial submodules of finite index. This led to a formula of the Γ-Euler characteristics of these Selmer groups under the assumption that the p-primary Selmer group of E over F is finite (see [16]). Remarkably, the Euler characteristics of the plus and minus Selmer groups turn out to be the same as the usual Selmer group in the ordinary case.

One of the key ingredients in Kim's works is a precise description of the algebraic structure of Kobayashi's plus and minus norm groups over K^{cyc}, where K is a finite unramified extension of $\mathbb{Q}_p$. For the minus norm group, Kim's result is unconditional, whereas the plus norm group is studied under the hypothesis that 4 does not divide $|K : \mathbb{Q}_p|$ (see [15, 17]). In [19], Kitajima and Otsuki were able to describe the plus norm groups even when 4 divides $|K : \mathbb{Q}_p|$. Furthermore, they relaxed the hypothesis that the elliptic curve E is defined over $\mathbb{Q}$ and allowed E to have mixed reduction types at primes above p. In their setting, E is defined over a number field F' with good reduction at all primes above p and that if u is a prime of F' above p where E has supersingular reduction, then $F'_u = \mathbb{Q}_p$. Let F be a finite extension of F' where the supersingular primes of E above p are unramified and let Σ_{ss} denote the set of primes of F lying above these supersingular primes. On choosing one of the two plus and minus norm subgroups for each prime of Σ_{ss}, we may define $2^{|\Sigma_{\mathrm{ss}}|}$ signed Selmer groups. Such mixed signed Selmer groups were first considered by Kim in [17]. In [1], the Γ-Euler characteristics of these mixed signed Selmer groups have been computed. In a different vein, we may consider a $\mathbb{Z}_p^d$-extensions of F, which we denote by F_∞ and write $G = \mathrm{Gal}(F_\infty/F)$. We may define plus and minus Selmer groups of E over F_∞ (see [17, 24]). In [24], assuming that p splits completely in F, the G-Euler characteristics of the plus and minus (no mixed signs) Selmer groups have been computed.

In this article, we assume that our elliptic curve E is defined over F' with no additive reduction at all primes above p (multiplicative reduction is allowed). We shall introduce certain hypotheses, labeled (S1)–(S5), in the main body of the article. Our goal is to compute the Akashi series of mixed signed Selmer groups over F_∞ under hypotheses (S1)–(S4). Here, F_∞/F is a $\mathbb{Z}_p^d$-extension and F/F' is a finite extension, with $G = \mathrm{Gal}(F_\infty/F)$ as above. As a by-product, we compute the G-Euler characteristics of these Selmer groups under the additional hypothesis (S5). Our main results are:

Theorem 1.1 (Theorem 5.1)**.** *Suppose that* (S1)–(S4) *are satisfied. Assume that the Pontryagin dual of a signed Selmer group of E over F^{cyc}, denoted by $X^{\vec{s}}(E/F^{\mathrm{cyc}})$, is torsion over $\mathbb{Z}_p[\![\Gamma]\!]$. Then the Pontryagin dual of a signed Selmer group of E over F_∞, denoted by $X^{\vec{s}}(E/F_\infty)$, is torsion over $\mathbb{Z}_p[\![G]\!]$, whose Akashi series is well-defined and is given by, up to a unit in $\mathbb{Z}_p[\![\Gamma]\!]$,*

$$T^r \cdot \mathrm{char}_\Gamma(X^{\vec{s}}(E/F^{\mathrm{cyc}})),$$

where r is the number of primes of F^{cyc} above p with nontrivial decomposition group in $F_\infty/F^{\mathrm{cyc}}$ and at which E has split multiplicative reduction, $T = \gamma - 1$ with γ being a topological generator of Γ and $\mathrm{char}_\Gamma(X^{\vec{s}}(E/F^{\mathrm{cyc}}))$ denotes a characteristic power series of the $\mathbb{Z}_p[\![\Gamma]\!]$-module $X^{\vec{s}}(E/F^{\mathrm{cyc}})$.

Theorem 1.2 (Theorem 5.3)**.** *Suppose that* (S1)–(S5) *are satisfied. If the p-primary Selmer group of E over F is finite, then the G-Euler characteristic of $X^{\vec{s}}(E/F_\infty)$ is well-defined and is given by*

$$|Ш(E/F)[p^\infty]| \times \prod_{v\in\Sigma'} c_v^{(p)} \times \prod_{v\in\Sigma_{\mathrm{o}}} (d_v^{(p)})^2.$$

Here, Σ' denotes the set of primes of F where E has bad reduction, $c_v^{(p)}$ is the highest power of p dividing $|E(F_v) : E_0(F_v)|$, where $E_0(F_v)$ is the subgroup of $E(F_v)$ consisting of points with nonsingular reduction modulo v, Σ_{o} denotes the set of primes of F lying above p where E has good ordinary reduction and $d_v^{(p)}$ is the highest power of p dividing $|\widetilde{E}_v(f_v)|$, where f_v is the residue field of F_v.

The structure of our article is as follows. In Section 2, we gather preliminary algebraic results which will be used in subsequent sections of the article. In particular, we review the definition and some basic properties of Akashi series in Section 2.1 and prove some basic results on the structure of certain Iwasawa modules in Section 2.2. In Section 3, we study the local cohomology of elliptic curves. We consider the ordinary and supersingular cases separately. In the supersingular case, we build on results of Kitajima and Otsuki for the cyclotomic $\mathbb{Z}_p$-extension to study the structure of the local quotient $\frac{H^1(K_\infty, E[p^\infty])}{\widehat{E}^{\pm}(K_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p}$, where K_∞ is a $\mathbb{Z}_p^2$-extension of a finite unramified extension of $\mathbb{Q}_p$. This quotient is crucially used to define the signed

Selmer groups. We show that its Pontryagin dual is free over a two-variable Iwasawa algebra (see Corollary 3.9). This result is one of the key ingredients in the proof of Theorem 1.1 and may be of independent interest. In Section 4, we give the definition of mixed signed Selmer groups over the cyclotomic $\mathbb{Z}_p$-extension, as well as a $\mathbb{Z}_p^d$-extension. We show how these Selmer groups can be related via Galois descent (see Lemma 4.9), which also plays an important role in the proof of Theorem 1.1. Furthermore, we study the cotorsionness of these Selmer groups as well as a natural extension of the $\mathfrak{M}_H(G)$-conjecture of Coates et al. Finally, we put everything together to prove Theorems 1.1 and 1.2 in Section 5. At the end of the article, we show that we may use these theorems to study the vanishing of $X^{\vec{s}}(E/F_\infty)$ (see Corollaries 5.4 and 5.5).

2. Preliminary algebraic results

2.1. Review of Akashi series. In this subsection, G denotes a fixed compact pro-p p-adic Lie group without p-torsion (we will mostly work with G which is isomorphic to $\mathbb{Z}_p^d$ for some integer d). Furthermore, we suppose that there exists a closed normal subgroup H of G such that $\Gamma := G/H \cong \mathbb{Z}_p$.

Definition 2.1. If M is a finitely generated $\mathbb{Z}_p[\![\Gamma]\!]$-module, $\mathrm{char}_\Gamma(M)$ denotes a characteristic power series of M.

Note that $\mathrm{char}_\Gamma(M)$ is well-defined up to a unit in $\mathbb{Z}_p[\![\Gamma]\!]$. If $\mathrm{char}_\Gamma(M)$ is a unit, we shall write $\mathrm{char}_\Gamma(M) = 1$. Following [4, 7, 41], we have the following definition.

Definition 2.2. Let M be $\mathbb{Z}_p[\![G]\!]$-module. We say that the Akashi series of M is well-defined if $H_i(H, M)$ is $\mathbb{Z}_p[\![\Gamma]\!]$-torsion for every $i \geq 0$. In this case, we define $\mathrm{Ak}_H(M)$ to be the (H-)Akashi series of M, which is given by

$$\mathrm{Ak}_H(M) := \prod_{i\geq 0} \mathrm{char}_\Gamma H_i(H, M)^{(-1)^i}.$$

Note that the Akashi series is only well-defined up to a unit in $\mathbb{Z}_p[\![\Gamma]\!]$. If the Akashi series of M is a unit in $\mathbb{Z}_p[\![\Gamma]\!]$, we shall write $\mathrm{Ak}_H(M) = 1$. Note that since G (and hence H) has no p-torsion, H has finite p-cohomological dimension, and therefore, the alternating product is a finite product.

Lemma 2.3. *Suppose that we are given a short exact sequence of $\mathbb{Z}_p[\![G]\!]$-modules*

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0.$$

If any two of the modules have well-defined Akashi series, so does the third. In this case, we have

$$\mathrm{Ak}_H(M) = \mathrm{Ak}_H(M')\,\mathrm{Ak}_H(M'').$$

Proof. See [7, Lemma 4.1] or [41, Proposition 2.2]. □

Since the group G we will work with is isomorphic $\mathbb{Z}_p^d$, the following lemma will be useful in our subsequent discussion.

Lemma 2.4. *Suppose that $G \cong H \times \Gamma$ with $\dim H \geq 1$. For every $\mathbb{Z}_p[\![G]\!]$-module M that is finitely generated over $\mathbb{Z}_p$, we have*

$$\mathrm{Ak}_H(M) = 1.$$

Proof. See [7, Lemma 4.5] or [41, Proposition 2.3]. □

We end this section by recalling a link between Akashi series and Euler characteristics.

Definition 2.5. The G-Euler characteristics of a $\mathbb{Z}_p[\![G]\!]$-module M is said to be well-defined if $H_i(G, M)$ is finite for each $i \geq 0$. In this case, the G-Euler characteristics is given by

$$\chi(G, M) = \prod_{i \geq 0} |H_i(G, M)|^{(-1)^i}.$$

Again, since G has no p-torsion, the product in the definition of $\chi(G, M)$ is finite.

Proposition 2.6. *Let G be a compact p-adic group without p-torsion, and let H be a closed normal subgroup of G with $G/H \cong \mathbb{Z}_p$. Let M be a finitely generated $\mathbb{Z}_p[\![G]\!]$-module whose G-Euler characteristics is well-defined. Then the Akashi series of M is well-defined and we have*

$$\chi(G, M) = |\varphi(\mathrm{Ak}_H(M))|_p^{-1},$$

where $|\cdot|_p$ is the p-adic norm with $|p|_p = p^{-1}$, and φ is the augmentation map from $\mathbb{Z}_p[\![\Gamma]\!]$ to $\mathbb{Z}_p$.

Proof. See [4, Theorem 3.6] or [7, Lemma 4.2]. □

2.2. Modules over two-variable Iwasawa algebras. In this subsection, we will study modules over $\mathbb{Z}_p[\![G]\!]$, where G is a p-adic group isomorphic to $\mathbb{Z}_p^2$. We begin by recalling the following result on $\mathbb{Z}_p[\![\Gamma]\!]$-modules, where $\Gamma \cong \mathbb{Z}_p$ and we write $\Gamma_n = \Gamma^{p^n}$.

Proposition 2.7. *Let M be a finitely generated $\mathbb{Z}_p[\![\Gamma]\!]$-module and r a non-negative integer such that M_{Γ_n} is a free $\mathbb{Z}_p$-module of rank rp^n for every $n \geq 0$. Then M is a free $\mathbb{Z}_p[\![\Gamma]\!]$-module of rank r.*

Proof. See [35, p. 207, General Lemma]. □

Now, fix two subgroups H and Γ of G so that $G \cong H \times \Gamma$ and $H \cong \Gamma \cong \mathbb{Z}_p$. For an integer $n \geq 0$, we write $H_n = H^{p^n}$ and $G_n = H_n \times \Gamma$ (not to be confused with $H^{p^n} \times \Gamma^{p^n}$!). Let M be a finitely generated $\mathbb{Z}_p[\![G]\!]$-module.

Since G_n is a subgroup of G of finite index, M is also finitely generated over $\mathbb{Z}_p[\![G_n]\!]$. It then follows from [27, Lemma 4.5] that M_{H_n} and $H_1(H_n, M)$ are finitely generated $\mathbb{Z}_p[\![\Gamma]\!]$-modules. Since $H_n \cong \mathbb{Z}_p$, we can identify M^{H_n} with $H_1(H_n, M)$, and in particular, M^{H_n} is finitely generated over $\mathbb{Z}_p[\![\Gamma]\!]$. We now come to the goal of this subsection, which is to prove the following analogue of Proposition 2.7.

Proposition 2.8. *Let M be a finitely generated $\mathbb{Z}_p[\![G]\!]$-module and $r \geq 0$ an integer such that M_{H_n} is a free $\mathbb{Z}_p[\![\Gamma]\!]$-module of rank rp^n for every $n \geq 0$. Then M is a free $\mathbb{Z}_p[\![G]\!]$-module of rank r.*

In preparation for the proof of Proposition 2.8, we prove the following two lemmas.

Lemma 2.9. *Let M be a finitely generated $\mathbb{Z}_p[\![G]\!]$-module. There exists an integer n_0 such that $M^{H_n} = M^{H_{n_0}}$ for all $n \geq n_0$.*

Proof. Since G is commutative, each M^{H_n} is also a $\mathbb{Z}_p[\![G]\!]$-submodule of M. Furthermore, they form an ascending chain and hence must stabilize by the Noetherian property of M. □

Lemma 2.10. *Let M be a finitely generated $\mathbb{Z}_p[\![G]\!]$-module. Then we have*

$$\operatorname{rank}_{\mathbb{Z}_p[\![\Gamma]\!]}\left(M_{H_n}\right) = p^n \operatorname{rank}_{\mathbb{Z}_p[\![G]\!]}(M) + c$$

for $n \gg 0$, where c is some constant independent of n.

Proof. It follows from [27, Lemma 4.5] that

$$\operatorname{rank}_{\mathbb{Z}_p[\![\Gamma]\!]}\left(M_{H_n}\right) = \operatorname{rank}_{\mathbb{Z}_p[\![G_n]\!]}(M) + \operatorname{rank}_{\mathbb{Z}_p[\![\Gamma]\!]}\left(M^{H_n}\right).$$

By Lemma 2.9, the quantity $\operatorname{rank}_{\mathbb{Z}_p[\![\Gamma]\!]}\left(M^{H_n}\right)$ stabilizes for large enough n. On the other hand, we have $\operatorname{rank}_{\mathbb{Z}_p[\![G_n]\!]}(M) = |G : G_n| \operatorname{rank}_{\mathbb{Z}_p[\![G]\!]}(M) = p^n \operatorname{rank}_{\mathbb{Z}_p[\![G]\!]}(M)$. Putting these equations together, the proposition follows. □

We can now prove Proposition 2.8:

Proof of Proposition 2.8. Since M_H is a free $\mathbb{Z}_p[\![\Gamma]\!]$-module of rank r, M is generated by r elements over $\mathbb{Z}_p[\![G]\!]$ by Nakayama's Lemma. In other words, we have a short exact sequence

$$0 \longrightarrow K \longrightarrow \mathbb{Z}_p[\![G]\!]^r \longrightarrow M \longrightarrow 0$$

of $\mathbb{Z}_p[\![G]\!]$-modules. Furthermore, it follows from the hypothesis of the proposition and Lemma 2.10 that $\operatorname{rank}_{\mathbb{Z}_p[\![G]\!]}(M) = r$. Thus, K must be torsion over $\mathbb{Z}_p[\![G]\!]$. But $\mathbb{Z}_p[\![G]\!]^r$ has no nontrivial torsion submodule, it follows that $K = 0$, and consequently, $M \cong \mathbb{Z}_p[\![G]\!]^r$. □

3. Elliptic curves over local fields

In this section, we record certain results on elliptic curves over a p-adic local field. We consider the ordinary and supersingular cases separately.

3.1. The ordinary case. Let K be a finite extension of $\mathbb{Q}_p$ and E an elliptic curve defined over K. In this subsection, our elliptic curve E is always assumed to have either good ordinary reduction or multiplicative reduction. Then from [5, p. 150], we have the following short exact sequence of $\mathrm{Gal}(\overline{K}/K)$-modules

$$0 \longrightarrow C \longrightarrow E[p^\infty] \longrightarrow D \longrightarrow 0,$$

where C and D are cofree $\mathbb{Z}_p$-modules of corank one. Furthermore, C and D are characterized by the fact that C is divisible and that D is the maximal quotient of $E[p^\infty]$ by a divisible subgroup on which $\mathrm{Gal}(\overline{K}/K^{ur})$ acts via a finite quotient. Here, K^{ur} is the maximal unramified extension of K. In fact, as a $\mathrm{Gal}(\overline{K}/K)$-module, D can be explicitly described as follows (see [5]):

$$D = \begin{cases} \widetilde{E}, & \text{if } E \text{ has good ordinary reduction,} \\ \mathbb{Q}_p/\mathbb{Z}_p, & \text{if } E \text{ has split multiplicative reduction,} \\ \mathbb{Q}_p/\mathbb{Z}_p \otimes \phi, & \text{if } E \text{ has nonsplit multiplicative reduction,} \end{cases} \tag{3.1}$$

where $\widetilde{E}$ is the reduction of E and ϕ is a nontrivial unramified character of $\mathrm{Gal}(\overline{K}/K)$.

Lemma 3.1. *Let E be an elliptic curve defined over a finite extension K of $\mathbb{Q}_p$. Let K_∞ be a $\mathbb{Z}_p^r$-extension of K which contains the cyclotomic $\mathbb{Z}_p$-extension K^{cyc}. Write $H = \mathrm{Gal}(K_\infty/K^{\mathrm{cyc}})$. Then the following statements hold.*

(a) *We have*
$$\frac{H^1(\mathcal{K}, E[p^\infty])}{E(\mathcal{K}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \cong H^1(\mathcal{K}, D)$$
for $\mathcal{K} = K^{\mathrm{cyc}}$ or K_∞.

(b) *$H^0(K^{\mathrm{cyc}}, D)$ is finite if E has either good ordinary or non-split multiplicative reduction. If E has split multiplicative reduction, then $H^0(K^{\mathrm{cyc}}, D) \cong \mathbb{Q}_p/\mathbb{Z}_p$.*

(c) *If $r \geq 2$, then $\mathrm{Ak}_H(D(K_\infty)^\vee) = 1$.*

Proof. Assertion (a) follows from a well-known result of Coates–Greenberg [5, Proposition 4.3]. Assertion (b) follows from the explicit description of D given in (3.1) above. Finally, assertion (c) is a consequence of Lemma 2.4 since $\mathrm{Gal}(K_\infty/K) \cong H \times \mathrm{Gal}(K^{\mathrm{cyc}}/K)$. □

3.2. The supersingular case. Let E be an elliptic curve defined over $\mathbb{Q}_p$ with good supersingular reduction and $a_p = 1 + p - |\widetilde{E}(\mathbb{F}_p)| = 0$, where $\widetilde{E}$ is the reduction of E. Let K be a finite unramified extension of $\mathbb{Q}_p$. Denote by $\widehat{E}$ the formal group of E. For convenience, if L is an extension of $\mathbb{Q}_p$, we write $\widehat{E}(L)$ for $\widehat{E}(\mathfrak{m}_L)$, where $\mathfrak{m}_L$ is the maximal ideal of the ring of integers of L. Denote by K^{cyc} (resp. K^{nr}) the cyclotomic (resp, the unramified) $\mathbb{Z}_p$-extension of K. If $n \geq 0$ is an integer, we write K_n (resp. $K^{(n)}$) for the unique subextension of K^{cyc}/K (resp. K^{nr}/K) whose degree over K is equal to p^n.

Lemma 3.2. *The formal groups $\widehat{E}(K^{(m)}K_n)$ has no p-torsion for all integers $m, n \geq 0$. In particular, $E(K^{(m)}K_n)$ has no p-torsion for every m, n.*

Proof. The first assertion is [19, Proposition 3.1] or [20, Proposition 8.7]. For the second assertion, consider the following short exact sequence

$$0 \longrightarrow \widehat{E}(K^{(m)}K_n) \longrightarrow E(K^{(m)}K_n) \longrightarrow \widetilde{E}(k_{m,n}) \longrightarrow 0,$$

where $k_{m,n}$ is the residue field of $K^{(m)}K_n$. Since $\widetilde{E}(k_{m,n})$ has no p-torsion by our assumption that E has good supersingular reduction, the second assertion follows from the first assertion. □

Following [15, 16, 17, 19, 20, 24, 31], we define the following plus and minus norm groups.

Definition 3.3. We define $\widehat{E}^+(K^{(m)}K_n)$ and $\widehat{E}^-(K^{(m)}K_n)$ to be

$$\left\{P \in \widehat{E}(K^{(m)}K_n) \ : \ \mathrm{tr}_{n/l+1}(P) \in E(K^{(m)}K_l), 2 \mid l, 0 \leq l \leq n-1\right\}$$

and

$$\left\{P \in \widehat{E}(K^{(m)}K_n) \ : \ \mathrm{tr}_{n/l+1}(P) \in E(K^{(m)}K_l), 2 \nmid l, 0 \leq l \leq n-1\right\}$$

respectively, where $\mathrm{tr}_{n/l+1} : \widehat{E}(K^{(m)}K_n) \longrightarrow \widehat{E}(K^{(m)}K_{l+1})$ denotes the trace map with respect to the formal group law of $\widehat{E}$.

By [20, Lemma 8.17], the groups $\widehat{E}^{\pm}(K^{(m)}K^{\mathrm{cyc}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ inject into $H^1(K^{(m)}K^{\mathrm{cyc}}, E[p^\infty])$ via the Kummer map.

In the rest of this subsection, we write $K_\infty = \bigcup_{m,n\geq 0} K^{(m)}K_n$. Note that $\mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p^2$. Denote by Γ the Galois group $\mathrm{Gal}(K^{\mathrm{cyc}}/K)$ which is also identified with $\mathrm{Gal}(K^{\mathrm{cyc}}K^{(m)}/K^{(m)})$ for $m \geq 0$. We shall also write $H = \mathrm{Gal}(K_\infty/K^{\mathrm{cyc}})$ which is identified with $\mathrm{Gal}(K^{nr}/K)$. For $m \geq 0$, set $H_m = \mathrm{Gal}(K_\infty/K^{\mathrm{cyc}}K^{(m)})$, which is identified with $\mathrm{Gal}(K^{nr}/K^{(m)})$.

Lemma 3.4. *We have* $(\widehat{E}(K^{nr}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{H_m} = \widehat{E}(K^{(m)}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ *for* $m \geq 0$. *Furthermore,* $\widehat{E}(K^{nr}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ *is a cofree* $\mathbb{Z}_p[\![H]\!]$*-module of corank* $|K : \mathbb{Q}_p|$. *In particular,*

$$H^1\Big(H_m, \widehat{E}(K^{nr}) \otimes \mathbb{Q}_p/\mathbb{Z}_p\Big) = 0$$

for $m \geq 0$.

Proof. The first assertion is [17, Proposition 2.10]. Since $\widehat{E}(K^{(m)}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ is cofree over $\mathbb{Z}_p$ for each m, $(\widehat{E}(K^{nr}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{H_m}$, is a cofree $\mathbb{Z}_p$-module with $\mathbb{Z}_p$-corank $|K : \mathbb{Q}_p|p^m$ by Mattuck's theorem [28]. Proposition 2.7 then implies that $\widehat{E}(K^{nr}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ is a cofree $\mathbb{Z}_p[\![H]\!]$-module of corank $|K : \mathbb{Q}_p|$. □

We require an analog of the above lemma over K_∞. As a start, we record the following.

Lemma 3.5. *We have* $H^1(H_m, \widehat{E}(K_\infty)) = 0$.

Proof. Replacing K by $K^{(m)}$, it suffices to prove the case for K (or H). By a well-known result of Coates–Greenberg [5, Corollary 3.2], we have $H^i(K^{\mathrm{cyc}}, \widehat{E}(\overline{K})) = 0 = H^i(K_\infty, \widehat{E}(\overline{K}))$ for $i \geq 1$. Hence the spectral sequence

$$H^i(H, H^j(K_\infty, \widehat{E}(\overline{K})) \Longrightarrow H^{i+j}(K^{\mathrm{cyc}}, \widehat{E}(\overline{K}))$$

degenerates yielding the required isomorphism. □

We can now establish the following analog of Lemma 3.4.

Proposition 3.6. *We have*

$$H^i\Big(H_m, \widehat{E}(K_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p\Big) = \begin{cases} \widehat{E}(K^{\mathrm{cyc}}K^{(m)}) \otimes \mathbb{Q}_p/\mathbb{Z}_p, & \text{if } i = 0, \\ 0, & \text{if } i \geq 1. \end{cases}$$

Proof. As before, it suffices to prove the proposition for H. Since $H \cong \mathbb{Z}_p$, the vanishing is clear for $i \geq 2$. By Lemma 3.2, we have the following short exact sequence

$$0 \longrightarrow \widehat{E}(K_\infty) \longrightarrow \widehat{E}(K_\infty) \otimes \mathbb{Q}_p \longrightarrow \widehat{E}(K_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 0.$$

In view of Lemma 3.5, upon taking H-invariant, we have

$$0 \longrightarrow \widehat{E}(K^{\mathrm{cyc}}) \longrightarrow \widehat{E}(K^{\mathrm{cyc}}) \otimes \mathbb{Q}_p \longrightarrow (\widehat{E}(K_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^H \longrightarrow 0$$

and

$$H^1\Big(H, \widehat{E}(K_\infty) \otimes \mathbb{Q}_p\Big) \cong H^1\Big(H, \widehat{E}(K_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p\Big)$$

The isomorphism for $i = 0$ follows from the short exact sequence. Also, note that in the isomorphism above, the left-hand side is a $\mathbb{Q}_p$-vector space, while the right-hand side is p-power torsion. Hence we must have $H^1(H, \widehat{E}(K_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p) = 0$. □

Corollary 3.7. *We have*

$$H^i\Big(H_m, \widehat{E}^{\pm}(K_\infty)\otimes \mathbb{Q}_p/\mathbb{Z}_p\Big) = \begin{cases} \widehat{E}^{\pm}(K^{\mathrm{cyc}}K^{(m)})\otimes \mathbb{Q}_p/\mathbb{Z}_p, & \text{if } i=0,\\ 0, & \text{if } i\geq 1. \end{cases}$$

Proof. Again, it suffices to prove the proposition for H. Since $H\cong \mathbb{Z}_p$, the vanishing is clear for $i\geq 2$. By [17, Proposition 2.6], we have

$$0\longrightarrow \widehat{E}(K)\longrightarrow \widehat{E}^+(K^{\mathrm{cyc}})\oplus \widehat{E}^-(K^{\mathrm{cyc}})\longrightarrow \widehat{E}(K^{\mathrm{cyc}})\longrightarrow 0$$

and

$$0\longrightarrow \widehat{E}(K^{nr})\longrightarrow \widehat{E}^+(K_\infty)\oplus \widehat{E}^-(K_\infty)\longrightarrow \widehat{E}(K_\infty)\longrightarrow 0.$$

For simplicity, we shall write $A=\mathbb{Q}_p/\mathbb{Z}_p$, $\widehat{E}_L=\widehat{E}(L)$ and $\widehat{E}^{\pm}_L=\widehat{E}^{\pm}(L)$ for $L\in\{K, K^{\mathrm{cyc}}, K^{nr}, K_\infty\}$. In view of Lemma 3.2, the exact sequences above induce the following short exact sequences

$$0\longrightarrow \widehat{E}_K\otimes A\longrightarrow (\widehat{E}^+_{K^{\mathrm{cyc}}}\otimes A)\oplus (\widehat{E}^-_{K^{\mathrm{cyc}}}\otimes A)\longrightarrow \widehat{E}_{K^{\mathrm{cyc}}}\otimes A\longrightarrow 0,$$
$$0\longrightarrow \widehat{E}_{K^{nr}}\otimes A\longrightarrow (\widehat{E}^+_{K_\infty}\otimes A)\oplus (\widehat{E}^-_{K_\infty}\otimes A)\longrightarrow \widehat{E}_{K_\infty}\otimes A\longrightarrow 0,$$

which in turn fit into the following diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \widehat{E}_K\otimes A & \longrightarrow & (\widehat{E}^+_{K^{\mathrm{cyc}}}\otimes A)\oplus (\widehat{E}^-_{K^{\mathrm{cyc}}}\otimes A) & \longrightarrow & \widehat{E}_{K^{\mathrm{cyc}}}\otimes A & \longrightarrow & 0\\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & (\widehat{E}_{K^{nr}}\otimes A)^H & \to & (\widehat{E}^+_{K_\infty}\otimes A)^H\oplus (\widehat{E}^-_{K_\infty}\otimes A)^H & \to & (\widehat{E}_{K_\infty}\otimes A)^H. & & \end{array}$$

Since the leftmost and rightmost vertical maps are isomorphisms by Lemma 3.4 and Proposition 3.6, so is the middle map. This implies the isomorphism of the corollary for $i=0$. Finally, the bottom sequence of the diagram continues in the form

$$H^1(H, \widehat{E}(K^{nr})\otimes A)\longrightarrow H^1(H, \widehat{E}^+(K_\infty)\otimes A)\oplus H^1(H, \widehat{E}^-(K_\infty)\otimes A)$$
$$\longrightarrow H^1(H, \widehat{E}(K_\infty)\otimes A).$$

Again, taking Lemma 3.4 and Proposition 3.6 into account, we obtain the desired vanishing for $i=1$. □

We end this subsection with a discussion on the structure of the $\mathbb{Z}_p[\![G]\!]$-module $\frac{H^1(K_\infty, E[p^\infty])}{\widehat{E}^{\pm}(K_\infty)\otimes \mathbb{Q}_p/\mathbb{Z}_p}$.

Proposition 3.8. *We have*

$$H^i\left(H_m, \frac{H^1(K_\infty, E[p^\infty])}{\widehat{E}^{\pm}(K_\infty)\otimes \mathbb{Q}_p/\mathbb{Z}_p}\right) = \begin{cases} \frac{H^1(K^{\mathrm{cyc}}K^{(m)}, E[p^\infty])}{\widehat{E}^{\pm}(K^{\mathrm{cyc}}K^{(m)})\otimes \mathbb{Q}_p/\mathbb{Z}_p}, & \text{if } i=0,\\ 0, & \text{if } i\geq 1. \end{cases}$$

Proof. Consider the spectral sequence

$$H^i(H_m, H^j(K_\infty, E[p^\infty])) \Longrightarrow H^{i+j}(K^{\mathrm{cyc}}K^{(m)}, E[p^\infty]).$$

By [30, Theorem 7.1.8(i)], $H^r(K_\infty, E[p^\infty]) = 0 = H^r(K^{\mathrm{cyc}}K^{(m)}, E[p^\infty])$ for $r \geq 2$. Also, we have $H^0(K_\infty, E[p^\infty]) = 0$ by Lemma 3.2. Hence the spectral sequence degenerates to yield

$$H^i\Big(H_m, H^1(K_\infty, E[p^\infty])\Big) = \begin{cases} H^1(K^{\mathrm{cyc}}K^{(m)}, E[p^\infty]), & \text{if } i = 0, \\ 0, & \text{if } i \geq 1. \end{cases}$$

The conclusion of the corollary now follows from combining the above observations with an analysis of the H_m-cohomology exact sequence of

$$0 \longrightarrow \widehat{E}^{\pm}(K_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow H^1(K_\infty, E[p^\infty]) \longrightarrow \frac{H^1(K_\infty, E[p^\infty])}{\widehat{E}^{\pm}(K_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \longrightarrow 0$$

and taking Corollary 3.7 into account. □

Corollary 3.9. *The module* $\frac{H^1(K_\infty, E[p^\infty])}{\widehat{E}^{\pm}(K_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p}$ *is* $\mathbb{Z}_p[\![G]\!]$*-cofree of corank* $|K : \mathbb{Q}_p|$.

Proof. It follows from the preceding proposition that

$$\left(\frac{H^1(K_\infty, E[p^\infty])}{\widehat{E}^{\pm}(K_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p}\right)^{H_m} \cong \frac{H^1(K^{\mathrm{cyc}}K^{(m)}, E[p^\infty])}{\widehat{E}^{\pm}(K^{\mathrm{cyc}}K^{(m)}) \otimes \mathbb{Q}_p/\mathbb{Z}_p},$$

where the latter is $\mathbb{Z}_p[\![\Gamma]\!]$-cofree of corank $|K : \mathbb{Q}_p|p^m$ by a calculation of Kitajima–Otsuki [19, Proposition 3.32]. The required conclusion now follows from Proposition 2.8. □

4. Multiply signed Selmer groups

Throughout this section, we fix E to be an elliptic curve defined over a number field F' and F a finite extension of F'. The following assumptions will be in force.

(S1) There exists at least one prime u of F' lying above p at which E has good supersingular reduction.

(S2) For each u of F' above p at which E has good supersingular reduction, we have
  (a) $F'_u \cong \mathbb{Q}_p$ and u is unramified in F/F';
  (b) $a_u = 1 + p - |\widetilde{E}_u(\mathbb{F}_p)| = 0$, where $\widetilde{E}_u$ is the reduction of E at u.

(S3) E does not have additive reduction at all primes of F lying above p.

Let F^{cyc} be the cyclotomic $\mathbb{Z}_p$-extension of F and F_n the intermediate subfield of F^{cyc}/F with $|F_n : F| = p^n$ for $n \geq 0$.

4.1. Selmer groups over cyclotomic $\mathbb{Z}_p$-extensions. From now on, Σ is a fixed finite set of primes of F which contains all the primes above p, all the ramified primes of F/F', the bad reduction primes of E and the archimedean primes. Let F_Σ denote the maximal algebraic extension of F unramified outside Σ. For any extension $\mathcal{F}$ of F which is contained in F_Σ, we write $G_\Sigma(\mathcal{F}) = \mathrm{Gal}(F_\Sigma/\mathcal{F})$.

Definition 4.1. We define

$$\begin{aligned}\Sigma_p &= \{\text{primes of } F \text{ above } p\},\\ \Sigma' &= \Sigma \setminus \Sigma_p,\\ \Sigma_{\mathrm{ss}} &= \{u \in \Sigma_p : E \text{ has good supersingular reduction at } u\},\\ \Sigma_{\mathrm{o}} &= \Sigma_p \setminus \Sigma_{\mathrm{ss}}.\end{aligned}$$

For any subset S of Σ and any extension $\mathcal{F}$ of F, we write $S(\mathcal{F})$ for the set of primes of $\mathcal{F}$ above S.

By (S2), every prime in Σ_{ss} is totally ramified in F^{cyc}/F. In particular, for each such prime v, there is a unique prime of F_n lying above the said prime. We then write $\widehat{E}_v$ for the formal group E over F_v.

Definition 4.2. Let $\vec{s} = (s_v)_{v\in\Sigma_{\mathrm{ss}}} \in \{+,-\}^{\Sigma_{\mathrm{ss}}}$. The signed Selmer group $\mathrm{Sel}^{\vec{s}}(E/F_n)$ is defined to be the kernel of

$$\begin{aligned}&H^1(G_\Sigma(F_n), E[p^\infty])\\ &\longrightarrow \bigoplus_{v\in\Sigma_{\mathrm{ss}}(F_n)} \frac{H^1(F_{n,v}, E[p^\infty])}{\widehat{E}^{s_v}(F_{n,v})\otimes\mathbb{Q}_p/\mathbb{Z}_p} \times \bigoplus_{v\in\Sigma(F_n)\setminus\Sigma_{\mathrm{ss}}(F_n)} \frac{H^1(F_{n,v}, E[p^\infty])}{E(F_{n,v})\otimes\mathbb{Q}_p/\mathbb{Z}_p}.\end{aligned}$$

We set $\mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}}) = \varinjlim_n \mathrm{Sel}^{\vec{s}}(E/F_n)$ and write $X^{\vec{s}}(E/F^{\mathrm{cyc}})$ for its Pontryagin dual.

For our purposes, we work with a different description of $\mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}})$. Note that for primes outside p, we have $E(F_{n,v})\otimes\mathbb{Q}_p/\mathbb{Z}_p = 0$. For primes in $\Sigma_{\mathrm{o}}(F^{\mathrm{cyc}})$, we have

$$\frac{H^1(F_v^{\mathrm{cyc}}, E[p^\infty])}{E(F_v^{\mathrm{cyc}})\otimes\mathbb{Q}_p/\mathbb{Z}_p} \cong H^1(F_v^{\mathrm{cyc}}, D_v)$$

by Lemma 3.1 (a), where D_v is defined as in Section 3.1.

Definition 4.3. Let $\vec{s} = (s_v)_{v\in\Sigma_{\mathrm{ss}}} \in \{+,-\}^{\Sigma_{\mathrm{ss}}}$. Given $v \in \Sigma(F^{\mathrm{cyc}})$, we define

$$J_v^{\vec{s}}(E/F^{\mathrm{cyc}}) := \begin{cases} \frac{H^1(F_v^{\mathrm{cyc}}, E[p^\infty])}{\widehat{E}^{s_v}(F_v^{\mathrm{cyc}})\otimes\mathbb{Q}_p/\mathbb{Z}_p} & v \in \Sigma_{\mathrm{ss}}(F^{\mathrm{cyc}}),\\ H^1(F_v^{\mathrm{cyc}}, D_v) & v \in \Sigma_{\mathrm{o}}(F^{\mathrm{cyc}}),\\ H^1(F_v^{\mathrm{cyc}}, E[p^\infty]) & v \in \Sigma'(F^{\mathrm{cyc}}).\end{cases}$$

Remark 4.4. The Selmer group $\mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}})$ sits inside the following exact sequence:

$$0 \longrightarrow \mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}}) \longrightarrow H^1(G_\Sigma(F^{\mathrm{cyc}}), E[p^\infty]) \longrightarrow \bigoplus_{v\in\Sigma(F^{\mathrm{cyc}})} J_v^{\vec{s}}(E/F^{\mathrm{cyc}}).$$

Conjecture 4.5. *For all choices of $\vec{s}$, the $\mathbb{Z}_p[\![\Gamma]\!]$-module $X^{\vec{s}}(E/F^{\mathrm{cyc}})$ is torsion.*

When E has good ordinary reduction at all primes above p, the above conjecture is precisely Mazur's conjecture in [29], which is known to hold in the case when E is defined over $\mathbb{Q}$ and F an abelian extension of $\mathbb{Q}$ (see [14]). For an elliptic curve over $\mathbb{Q}$ with good supersingular reduction at p, this conjecture has been proved to be true by Kobayashi in [20]; see also [3] for a generalization of this conjecture for abelian varieties and [2] for progress towards this conjecture for CM abelian varieties. We record certain consequences of Conjecture 4.5, which will be utilized in subsequent discussion of the article.

Proposition 4.6. *Suppose that* (S1)–(S3) *are valid, and that $X^{\vec{s}}(E/F^{\mathrm{cyc}})$ is a torsion $\mathbb{Z}_p[\![\Gamma]\!]$-module. Then the following assertions hold.*

(a) $H^2(G_\Sigma(F^{\mathrm{cyc}}), E[p^\infty]) = 0$.

(b) *There is a short exact sequence*

$$0 \longrightarrow \mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}}) \longrightarrow H^1(G_\Sigma(F^{\mathrm{cyc}}), E[p^\infty]) \longrightarrow \bigoplus_{v\in\Sigma(F^{\mathrm{cyc}})} J_v^{\vec{s}}(E/F^{\mathrm{cyc}}) \longrightarrow 0.$$

Proof. See [21, Proposition 2.7] or [23, Proposition 4.4]. □

4.2. Selmer groups over $\mathbb{Z}_p^d$-extensions. Throughout this subsection, let F_∞ be a $\mathbb{Z}_p^d$-extension of F which satisfies the following hypothesis.

(S4) $F^{\mathrm{cyc}} \subseteq F_\infty$, and every $v \in \Sigma_{\mathrm{ss}}(F^{\mathrm{cyc}})$ is unramified in $F_\infty/F^{\mathrm{cyc}}$.

Write $G = \mathrm{Gal}(F_\infty/F)$, $H = \mathrm{Gal}(F_\infty/F^{\mathrm{cyc}})$ and $\Gamma = \mathrm{Gal}(F^{\mathrm{cyc}}/F)$. Let L_n be the unique subextension of F_∞/F such that $\mathrm{Gal}(L_n/F) \cong (\mathbb{Z}/p^n)^d$. Let $\vec{s} = (s_v)_{v\in\Sigma_{\mathrm{ss}}} \in \{+,-\}^{\Sigma_{\mathrm{ss}}}$. For $w \in \Sigma_{\mathrm{ss}}(L_n)$, we set $s_w = s_v$, where v is the prime of F below w. By (S4), $L_{n,w}$ is the compositum of a subextension of the cyclotomic $\mathbb{Z}_p$-extension of F_v and a subextension of the unramified $\mathbb{Z}_p$-extension of F_v. Hence we can define $\widehat{E}^{s_w}(L_{n,w})$ as in Definition 3.3.

Definition 4.7. For $\vec{s} = (s_v)_{v\in\Sigma_{\mathrm{ss}}} \in \{+,-\}^{\Sigma_{\mathrm{ss}}}$, the signed Selmer group $\mathrm{Sel}^{\vec{s}}(E/L_n)$ is then defined to be the kernel of

$$H^1(G_\Sigma(L_n), E[p^\infty]) \longrightarrow \bigoplus_{w\in\Sigma_{\mathrm{ss}}(L_n)} \frac{H^1(L_{n,w}, E[p^\infty])}{\widehat{E}^{s_w}(L_{n,w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \times \bigoplus_{w\in\Sigma(L_n)\setminus\Sigma_{\mathrm{ss}}(L_n)} \frac{H^1(L_{n,w}, E[p^\infty])}{E(L_{n,w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}.$$

We set $\mathrm{Sel}^{\vec{s}}(E/F_\infty) = \varinjlim_n \mathrm{Sel}^{\vec{s}}(E/L_n)$ and write $X^{\vec{s}}(E/F_\infty)$ for its Pontryagin dual.

Remark 4.8. Analogous to Definition 4.3 and Remark 4.4, we define for $w \in \Sigma(F_\infty)$

$$J_w^{\vec{s}}(E/F_\infty) := \begin{cases} \frac{H^1(F_{\infty,w}, E[p^\infty])}{\widehat{E}^{s_w}(F_{\infty,w})\otimes\mathbb{Q}_p/\mathbb{Z}_p} & w \in \Sigma_{\mathrm{ss}}(F_\infty), \\ H^1(F_{\infty,w}, D_w) & w \in \Sigma_{\mathrm{o}}(F_\infty), \\ H^1(F_{\infty,w}, E[p^\infty]) & w \in \Sigma'(F_\infty). \end{cases}$$

and we have the exact sequence

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

We may now relate the signed Selmer groups over F_∞ to those over F^{cyc} via the following lemma.

Lemma 4.9. *Suppose that* (S1)–(S4) *hold. There is an injection*

$$\mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}}) \longrightarrow \mathrm{Sel}^{\vec{s}}(E/F_\infty)^H$$

with cokernel being cofinitely generated over $\mathbb{Z}_p$.

Proof. Consider the following diagram

$$\begin{array}{ccccc} 0 \to \mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}}) & \to & H^1\big(G_\Sigma(F^{\mathrm{cyc}}), E[p^\infty]\big) & \longrightarrow & \bigoplus_{v\in\Sigma(F^{\mathrm{cyc}})} J_v^{\vec{s}}(E/F^{\mathrm{cyc}}) \\ \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma=\oplus\gamma_v} \\ 0 \to \mathrm{Sel}^{\vec{s}}(E/F_\infty)^H & \to & H^1\big(G_\Sigma(F_\infty), E[p^\infty]\big)^H & \to & \Big(\bigoplus_{w\in\Sigma(F_\infty)} J_w^{\vec{s}}(E/F_\infty)\Big)^H \end{array}$$

with exact rows. As seen in the proof of Proposition 3.8, for all $w \in \Sigma_{\mathrm{ss}}(F_\infty)$, we have $E(F_{\infty,w})[p^\infty] = 0$. Hence we also have $E(F_\infty)[p^\infty] = 0$. Combining this observation with a Hochschild–Serre spectral sequence argument, we see that β is an isomorphism. Thus, α is injective.

It remains to show that $\ker\gamma$ is cofinitely generated over $\mathbb{Z}_p$. By Proposition 3.8, γ_v is injective for $v \in \Sigma_{\mathrm{ss}}(F^{\mathrm{cyc}})$. For $v \in \Sigma(F^{\mathrm{cyc}}) \setminus \Sigma_{\mathrm{ss}}(F^{\mathrm{cyc}})$, the kernel of γ_v is given by $H^1(H_v, D_v(F_{\infty,w}))$ or $H^1(H_v, E[p^\infty](F_{\infty,w}))$ accordingly to v divides p or not, where H_v is the decomposition group of H with respect to a prime w of F_∞ above v. The conclusion now follows from the fact that the cohomology groups $H^1(H, W)$ are cofinitely generated over $\mathbb{Z}_p$ for any p-adic Lie group H and any $\mathbb{Z}_p$-cofinitely generated H-module W. (Note: In fact, since $\mathbb{Z}_p^d$-extension is unramified outside p (cf. [12, Theorem 1]), we have $H_v = 1$ for $v \in \Sigma'(F_\infty)$, and so one even has $\ker\gamma_v = 0$ for these primes. This latter observation will be used in the proof of Theorem 5.1.) □

Remark 4.10. The above lemma is certainly well-known when E has good ordinary reduction (see [6, 7, 10]). Unlike the ordinary case, where the argument is quite formal, the supersingular situation is less straightforward. This is because we do not have a nice enough descent theory for the formal group of an elliptic curve in ramified towers (see [25, Section 6]). In the setting considered in the present article, thanks to hypothesis (S4), we have applied results of Kim [17] and Kitajima–Otsuki [19] to obtain such a descent theory in Section 3.2.

We now state the following natural generalisation of Conjecture 4.5.

Conjecture 4.11. *For all choices of $\vec{s} \in \{+,-\}^{\Sigma_{\mathrm{ss}}}$, the Selmer group $X^{\vec{s}}(E/F_\infty)$ is torsion over $\mathbb{Z}_p[\![G]\!]$.*

When E has good ordinary reduction at all primes above p, the above conjecture is a natural extension of Mazur's conjecture (see [6, 7, 9, 10, 32]). When E has supersingular reduction with $F' = \mathbb{Q}$ and F an imaginary quadratic field where p splits, this was studied in [18, 22, 23].

Conjecture 4.11 has the following consequence, which is analogous to Proposition 4.6 as a consequence of Conjecture 4.5.

Proposition 4.12. *Suppose that* (S1)–(S4) *are valid, and that $X^{\vec{s}}(E/F_\infty)$ is a torsion $\mathbb{Z}_p[\![G]\!]$-module. Then we have the following assertions.*

(a) $H^2(G_\Sigma(F_\infty), E[p^\infty]) = 0$.

(b) *There is a short exact sequence*

$$0 \longrightarrow \mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}}) \longrightarrow H^1(G_\Sigma(F_\infty), E[p^\infty]) \longrightarrow \bigoplus_{w \in \Sigma(F_\infty)} J_w^{\vec{s}}(E/F_\infty) \longrightarrow 0.$$

Proof. The proof is similar to that of Proposition 4.6 with some extra technicality. By [34, Proposition A.3.2], we have an exact sequence

$$0 \longrightarrow \mathrm{Sel}^{\vec{s}}(E/F_\infty) \longrightarrow H^1(G_\Sigma(F_\infty), E[p^\infty]) \longrightarrow \bigoplus_{w \in \Sigma(F_\infty)} J_w^{\vec{s}}(E/F_\infty) \longrightarrow \mathfrak{S}^{\vec{s}}(E/F_\infty)^\vee \longrightarrow H^2(G_\Sigma(F_\infty), E[p^\infty]) \longrightarrow 0,$$

where $\mathfrak{S}^{\vec{s}}(E/F_\infty)$ is a $\mathbb{Z}_p[\![G]\!]$-submodule of

$$H^1_{\mathrm{Iw}}(F_\infty/F, T_pE) := \varprojlim_n H^1(G_\Sigma(L_n), T_pE).$$

(For the precise definition of $\mathfrak{S}^{\vec{s}}(E/F_\infty)$, we refer readers to loc. cit. For our purposes, the submodule theoretical information suffices.) The conclusion of the proposition will follow once we can show that $\mathfrak{S}^{\vec{s}}(E/F_\infty) = 0$.

A standard corank calculation (see [32, Theorem 3.2]) tells us that

$$\operatorname{corank}_{\mathbb{Z}_p[\![G]\!]}\left(H^1(G_\Sigma(F_\infty), E[p^\infty])\right) - \operatorname{corank}_{\mathbb{Z}_p[\![G]\!]}\left(H^2(G_\Sigma(F_\infty), E[p^\infty])\right) = |F:\mathbb{Q}|.$$

For the local summands, we also have

$$\operatorname{corank}_{\mathbb{Z}_p[\![G]\!]}\left(\bigoplus_{w\in\Sigma(F_\infty)} J_w^{\vec{s}}(E/F_\infty)\right) = [F:\mathbb{Q}],$$

where in the calculations, we made use of [32, Theorem 4.1] for primes in $\Sigma(F_\infty)\setminus\Sigma_{\mathrm{ss}}(F_\infty)$ and Corollary 3.9 for primes in $\Sigma_{\mathrm{ss}}(F_\infty)$. It follows from these formulas and the above exact sequence that if $\mathrm{Sel}^{\vec{s}}(E/F_\infty)$ is a cotorsion $\mathbb{Z}_p[\![G]\!]$-module, then $\mathfrak{S}^{\vec{s}}(E/F_\infty)$ is a torsion $\mathbb{Z}_p[\![G]\!]$-module.

Hence the required assertion $\mathfrak{S}^{\vec{s}}(E/F_\infty)=0$ will follow once we can show that $H^1_{\mathrm{Iw}}(F_\infty/F, T_pE)$ is a torsion-free $\mathbb{Z}_p[\![G]\!]$-module. To see this, we first recall the following spectral sequence of Jannsen ([13, Theorem 1])

$$\mathrm{Ext}^i_{\mathbb{Z}_p[\![G]\!]}\big(H^j(G_\Sigma(F_\infty), E[p^\infty])^\vee, \mathbb{Z}_p[\![G]\!]\big) \Longrightarrow H^{i+j}_{\mathrm{Iw}}(F_\infty/F, T_pE).$$

By considering the low degree terms, we have an exact sequence

$$0 \longrightarrow \mathrm{Ext}^1_{\mathbb{Z}_p[\![G]\!]}\big((E(F_\infty)[p^\infty])^\vee, \mathbb{Z}_p[\![G]\!]\big) \longrightarrow H^1_{\mathrm{Iw}}(F_\infty/F, T_pE) \longrightarrow \mathrm{Ext}^0_{\mathbb{Z}_p[\![G]\!]}\left(H^1(G_\Sigma(F_\infty), E[p^\infty])^\vee, \mathbb{Z}_p[\![G]\!]\right).$$

From the proof of Lemma 4.9, we have $E(F_\infty)[p^\infty]=0$. Hence the leftmost term vanishes, which in turn implies that $H^1_{\mathrm{Iw}}(F_\infty, T_pE)$ injects into an Ext^0-term. But since the latter is a reflexive $\mathbb{Z}_p[\![G]\!]$-module by [30, Corollary 5.1.3], $H^1_{\mathrm{Iw}}(F_\infty/F, T_pE)$ must be torsion-free over $\mathbb{Z}_p[\![G]\!]$. This completes the proof of the proposition. □

We now relate Conjectures 4.5 and 4.11.

Proposition 4.13. *Suppose that* (S1)–(S4) *are satisfied. Assume that* $X^{\vec{s}}(E/F^{\mathrm{cyc}})$ *is torsion over* $\mathbb{Z}_p[\![\Gamma]\!]$. *Then the* $\mathbb{Z}_p[\![G]\!]$*-module* $X^{\vec{s}}(E/F_\infty)$ *is torsion.*

Proof. It follows from Lemma 4.9 that $X^{\vec{s}}(E/F_\infty)_H$ is torsion over $\mathbb{Z}_p[\![\Gamma]\!]$. Since H is abelian (and hence solvable), we may apply [9, Lemma 2.6] to conclude that $X^{\vec{s}}(E/F_\infty)$ is torsion over $\mathbb{Z}_p[\![G]\!]$. □

In what follows, we discuss a natural extension of the $\mathfrak{M}_H(G)$-conjecture formulated by Coates et al. in [4] for the signed Selmer groups in our setting. Although we do not use it in subsequent calculations, it may be of independent interest. See also [11, 25] on this subject.

Conjecture 4.14 ($\mathfrak{M}_H(G)$-conjecture)**.** *For all choices of* $\vec{s}$*, the module* $X^{\vec{s}}(E/F_\infty)/X^{\vec{s}}(E/F_\infty)[p^\infty]$ *is finitely generated over* $\mathbb{Z}_p[\![H]\!]$.

We give a partial evidence towards this conjecture (compare with [4, Proposition 5.6] and [6, Theorem 6.4]). Again, we remind the reader that the result is available in this context thanks to hypothesis (S4) and descent results of Kim and Kitajima–Otsuki [17, 19].

Proposition 4.15. *Suppose that* (S1)–(S4) *are satisfied. Assume that* $X^{\vec{s}}(E/F^{\mathrm{cyc}})$ *is finitely generated over* $\mathbb{Z}_p$*. Then the dual Selmer group* $X^{\vec{s}}(E/F_\infty)$ *is finitely generated over* $\mathbb{Z}_p[\![H]\!]$*. In particular, the* $\mathfrak{M}_H(G)$*-conjecture is valid.*

Proof. It follows from Lemma 4.9 and the hypothesis of the proposition that $X^{\vec{s}}(E/F_\infty)_H$ is finitely generated over $\mathbb{Z}_p$. The conclusion thus follows from Nakayama's Lemma. □

5. Proofs of main results

This section is devoted to proving the main results of the article (Theorems 1.1 and 1.2 in the introduction). Throughout, we retain the setting and notation of Section 4. Furthermore, we fix a choice of $\vec{s} = (s_v)_{v\in\Sigma_{\mathrm{ss}}} \in \{+,-\}^{\Sigma_{\mathrm{ss}}}$.

For convenience, we identify $\mathbb{Z}_p[\![\Gamma]\!] \cong \mathbb{Z}_p[\![T]\!]$ under a choice of a topological generator of Γ. We first prove our result on Akashi series of signed Selmer groups (Theorem 1.1).

Theorem 5.1. *Suppose that* (S1)–(S4) *are satisfied. Assume that the* $\mathbb{Z}_p[\![\Gamma]\!]$*-module* $X^{\vec{s}}(E/F^{\mathrm{cyc}})$ *is torsion. Then* $X^{\vec{s}}(E/F_\infty)$ *is torsion over* $\mathbb{Z}_p[\![G]\!]$*, whose Akashi series is well-defined and is given by*

$$\mathrm{Ak}_H(X^{\vec{s}}(E/F_\infty)) = T^r \cdot \mathrm{char}_\Gamma(X^{\vec{s}}(E/F^{\mathrm{cyc}})),$$

where r *is the number of primes of* F^{cyc} *above* p *with nontrivial decomposition group in* $F_\infty/F^{\mathrm{cyc}}$ *and at which* E *has split multiplicative reduction.*

Proof. The first assertion is precisely Proposition 4.13. Hence it follows from Propositions 4.6 and 4.12 that $H^2(G_\Sigma(\mathcal{F}), E[p^\infty]) = 0$ for $\mathcal{F} = F^{\mathrm{cyc}}, F_\infty$. Also, we have $H^0(K_\infty, E[p^\infty]) = 0$ by the proof of Lemma 4.9. Hence the spectral sequence

$$H^i(H, H^j(G_\Sigma(F_\infty), E[p^\infty])) \Rightarrow H^{i+j}(G_\Sigma(F^{\mathrm{cyc}}), E[p^\infty])$$

degenerates to yield

$$H^i\left(H, H^1(G_\Sigma(F_\infty), E[p^\infty])\right) = \begin{cases} H^1(G_\Sigma(F^{\mathrm{cyc}}), E[p^\infty]), & \text{if } i = 0, \\ 0, & \text{if } i \geq 1. \end{cases} \tag{5.1}$$

On the other hand, it follows from Propositions 4.6 and 4.12 that we have a short exact sequence

$$0 \longrightarrow \mathrm{Sel}^{\vec{s}}(E/\mathcal{F}) \longrightarrow H^1(G_\Sigma(\mathcal{F}), E[p^\infty]) \longrightarrow \bigoplus_{u\in\Sigma(\mathcal{F})} J_u^{\vec{s}}(E/\mathcal{F}) \longrightarrow 0 \tag{5.2}$$

for $\mathcal{F} = F^{\mathrm{cyc}}$ and F_∞, and where as before, we write $J_u(E/\mathcal{F})$ for the local terms. The short exact sequence (5.2) for $\mathcal{F} = F^{\mathrm{cyc}}$ and the H-cohomology long exact sequence associated to (5.2) when $\mathcal{F} = F_\infty$ fit in the following commutative diagram

$$\begin{array}{ccccccc} 0 \to \mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}}) & \to & H^1\big(G_\Sigma(F^{\mathrm{cyc}}), E[p^\infty]\big) & \to & \bigoplus_{v\in\Sigma(F^{\mathrm{cyc}})} J_v^{\vec{s}}(E/F^{\mathrm{cyc}}) & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow{\scriptstyle g=\oplus g_v} & & \\ 0 \to \mathrm{Sel}^{\vec{s}}(E/F_\infty)^H & \to & H^1\big(G_\Sigma(F_\infty), E[p^\infty]\big)^H & \longrightarrow & \Big(\bigoplus_{w\in\Sigma(F_\infty)} J_w^{\vec{s}}(E/F_\infty)\Big)^H & & \end{array}$$

with exact rows.

As already seen in the proof of Lemma 4.9, the middle vertical map is an isomorphism. By Proposition 3.8, g_v is an isomorphism for $v \in \Sigma_{\mathrm{ss}}(F^{\mathrm{cyc}})$. Since $\mathbb{Z}_p^d$-extension is unramified outside p (cf. [12, Theorem 1]), it follows that $H_v = 1$ for primes outside p, and so we also have that g_v is an isomorphism for such prime. In conclusion, we have the following short exact sequence

$$\begin{aligned} 0 \longrightarrow \mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}}) &\longrightarrow \mathrm{Sel}^{\vec{s}}(E/F_\infty)^H \\ &\longrightarrow \bigoplus_{\substack{v\in\Sigma_{\mathrm{o}}(F^{\mathrm{cyc}}) \\ \dim H_v\geq 1}} H^1(H_v, D_v(F_\infty)) \longrightarrow 0 \end{aligned}$$

by the snake lemma and the isomorphisms

$$H^i\left(H, \mathrm{Sel}^{\vec{s}}(E/F_\infty)\right) \cong \bigoplus_{\substack{v\in\Sigma_{\mathrm{o}}(F^{\mathrm{cyc}}) \\ \dim H_v\geq 1}} H^{i+1}(H_v, D_v(F_\infty))$$

for $i \geq 1$, coming from the H-cohomology long exact sequence associated to (5.2) when $\mathcal{F} = F_\infty$ (thanks to the vanishing of $H^i(H, H^1(G_\Sigma(F_\infty), E[p^\infty]))$ as given by (5.1)). Via the duality

$$H_i(H, M) \cong H^i(H, M^\vee)^\vee,$$

the above calculations can be translated to yield

$$\mathrm{Ak}_H(X^{\vec{s}}(E/F_\infty)) = \mathrm{char}_\Gamma(X^{\vec{s}}(E/F^{\mathrm{cyc}})) \cdot \prod_{\substack{v\in\Sigma_{\mathrm{o}}(F^{\mathrm{cyc}}) \\ \dim H_v\geq 1}} \frac{\mathrm{char}_\Gamma(D_v(F_v^{\mathrm{cyc}})^\vee)}{\mathrm{Ak}_{H_v}(D_v(F_{\infty,w})^\vee)}.$$

But by Lemma 3.1, $\mathrm{Ak}_{H_v}(D_v(F_{\infty,w})^\vee) = 1$. Also, if v is a prime of good ordinary reduction or non-split multiplicative reduction, then $D_v(F_v^{\mathrm{cyc}})$ is finite and so $\mathrm{char}_\Gamma(D_v(F_v^{\mathrm{cyc}})^\vee) = 1$. Finally, if v is a prime of split multiplicative reduction, we have $\mathrm{char}_\Gamma(D_v(F_v^{\mathrm{cyc}})^\vee) = \mathrm{char}_\Gamma(\mathbb{Z}_p) = T$. Thus, we have proven our theorem. □

Remark 5.2. In [7, 41], the Akashi series are computed under the validity of the $\mathfrak{M}_H(G)$-conjecture. However, as noted in [26, p. 284], one can perform these computations under the weaker hypothesis that the Pontryagin dual of the signed Selmer group over F_∞ is a torsion $\mathbb{Z}_p[\![G]\!]$-module.

We introduce one last hypothesis.

(S5) (a) The elliptic curve E has good reduction at all primes above p;
(b) For our fixed choice of $\vec{s}$, we have $4 \nmid |F_v : \mathbb{Q}_p|$ whenever $s_v = +$.

We can now prove Theorem 1.2.

Theorem 5.3. *Suppose that* (S1)–(S5) *are satisfied. If the p-primary Selmer group* $\mathrm{Sel}(E/F)$ *is finite, then* $\chi(G, X^{\vec{s}}(E/F_\infty))$ *is well-defined and is given by*

$$\chi(G, X^{\vec{s}}(E/F_\infty)) = |Ш(E/F)[p^\infty]| \times \prod_{v\in\Sigma'} c_v^{(p)} \times \prod_{v\in\Sigma_o} (d_v^{(p)})^2.$$

Here, $c_v^{(p)}$ is the highest power of p dividing $|E(F_v) : E_0(F_v)|$, where $E_0(F_v)$ is the subgroup of $E(F_v)$ consisting of points with nonsingular reduction modulo v, and $d_v^{(p)}$ is the highest power of p dividing $|\widetilde{E}_v(f_v)|$, where f_v is the residue field of F_v.

Proof. By [1, Theorem 2.3], we have that $\mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}})$ is cotorsion over $\mathbb{Z}_p[\![\Gamma]\!]$ and that

$$\chi(\Gamma, X^{\vec{s}}(E/F^{\mathrm{cyc}})) = |Ш(E/F)[p^\infty]| \times \prod_{v\in\Sigma'} c_v^{(p)} \times \prod_{v\in\Sigma_o} (d_v^{(p)})^2.$$

In view of Proposition 2.6 and Theorem 5.1, it remains to show that the G-Euler characteristics of $X^{\vec{s}}(E/F_\infty)$ is well-defined. Since $G \cong \mathbb{Z}_p^d$, it is sufficient to show that $\mathrm{Sel}^{\vec{s}}(E/F_\infty)^G$ is finite by [38, part (1) of the theorem on p. 3455]. Let $J_v(E/F)$ denote the quotient $\frac{H^1(F_v, E[p^\infty])}{E(F_v)\otimes\mathbb{Q}_p/\mathbb{Z}_p}$ for $v \in \Sigma$. Consider the following diagram

(5.3)

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Sel}(E/F) & \longrightarrow & H^1(G_\Sigma(F), E[p^\infty]) & \longrightarrow & \bigoplus_{v\in\Sigma} J_v(E/F) \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \oplus l_v} \\
0 & \to & \mathrm{Sel}^{\vec{s}}(E/F_\infty)^G & \to & H^1(G_\Sigma(F_\infty), E[p^\infty])^G & \to & \Big(\bigoplus_{w\in\Sigma(F_\infty)} J_w^{\vec{s}}(E/F_\infty)\Big)^G
\end{array}$$

with exact rows (the surjectivity of the first row follows from the finiteness of $\mathrm{Sel}(E/F)$; see [16, Proposition 3.8]). By a similar argument to that in the proof of Lemma 4.9, the middle vertical map is an isomorphism. Hence it remains to show that $\ker l_v$ is finite for every v. For $v \in \Sigma \setminus \Sigma_{\mathrm{ss}}$, this follows from [8, Propositions 4.1 and 4.5].

Now let $v \in \Sigma_{\mathrm{ss}}$ and $w \in \Sigma_{\mathrm{ss}}(F_\infty)$ a prime above v. Writing $G_v = \mathrm{Gal}(F_{\infty,w}/F_v)$ and $A = \mathbb{Q}_p/\mathbb{Z}_p$, we have the following diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & E(F_v)\otimes A & \longrightarrow & H^1(F_v, E[p^\infty]) & \longrightarrow & \frac{H^1(F_v,E[p^\infty])}{E(F_v)\otimes A} \longrightarrow 0 \\ & & \downarrow{\scriptstyle a_v} & & \downarrow{\scriptstyle b_v} & & \downarrow{\scriptstyle l_v} \\ 0 & \to & \big(E^{\pm}(F_{\infty,w})\otimes A\big)^{G_v} & \to & H^1(F_{\infty,w}, E[p^\infty])^{G_v} & \to & \left(\frac{H^1(F_{\infty,w},E[p^\infty])}{\widehat{E}^{\pm}(F_{\infty,w})\otimes A}\right)^{G_v} \end{array}$$

with exact rows and that b_v is an isomorphism. Consequently, a_v is injective and $\ker l_v \cong \operatorname{coker} a_v$. Under (S5)(b), [17, Proposition 2.18] tells us that a_v is an isomorphism, which in turn implies that l_v is injective. The proof of the theorem is now complete. □

We now prove the following vanishing criterion. When the elliptic curve has good ordinary reduction at all primes above p, this was established in [10, Proposition 4.12] and [26, Theorem 5.11]. Our result shows that the analogue assertion holds even allowing supersingular reduction.

Corollary 5.4. *Suppose that* (S1)–(S5) *are satisfied. Assume that the* $\mathbb{Z}_p[\![\Gamma]\!]$*-module* $X^{\vec{s}}(E/F^{\mathrm{cyc}})$ *is torsion. Then* $\mathrm{Ak}_H(X^{\vec{s}}(E/F_\infty)) = 1$ *if and only if* $\mathrm{Sel}^{\vec{s}}(E/F_\infty) = 0$.

Proof. We shall freely use the notation of Theorem 5.3 in the proof. The if direction is clear. Conversely, suppose that $\mathrm{Ak}_H(X^{\vec{s}}(E/F_\infty)) = 1$. By Theorem 5.1, we have $\mathrm{char}_\Gamma(X^{\vec{s}}(E/F^{\mathrm{cyc}})) = 1$, which in turn implies that $\mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}})$ is finite. Following the proof of Theorem 5.3, we may show that the restriction map

$$\mathrm{Sel}(E/F) \to \mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}})^\Gamma$$

is injective with finite cokernel. Thus, $\mathrm{Sel}(E/F)$ is also finite and Theorem 5.3 says that $\chi(G, X^{\vec{s}}(E/F_\infty))$ is well-defined.

Since $\mathrm{Ak}_H(X^{\vec{s}}(E/F_\infty)) = 1$, Proposition 2.6 gives $Ш(E/F)[p^\infty] = 0$, $c_v^{(p)} = 1$ for every $v \in \Sigma'$ and $|\widetilde{E}_v(f_v)| = 1$ for every $v \in \Sigma_{\mathrm{o}}$. As seen in the proof of Theorem 5.3, one has $\ker l_v = 0$ for $v \in \Sigma_{\mathrm{ss}}$ in the diagram (5.3). By [8, Proposition 4.1] and that $c_v^{(p)} = 1$, it follows that $\ker l_v = 0$ for $v \in \Sigma'$. For $v \in \Sigma_{\mathrm{o}}$, the equality $|\widetilde{E}_v(f_v)| = 1$ implies that $D_v(F_v) = 0$. Since $F_{\infty,w}$ is a pro-p extension of F_v for w above v, we have $D_v(F_{\infty,w}) = 0$ and hence $\ker l_v = 0$ for $v \in \Sigma_{\mathrm{o}}$. Therefore, $\ker l_v = 0$ for every $v \in \Sigma$. Thus, the diagram (5.3) gives the isomorphism

$$\mathrm{Sel}(E/F) \to \mathrm{Sel}^{\vec{s}}(E/F_\infty)^G.$$

Recall that $\mathrm{Sel}(E/F)$ is finite and $Ш(E/F)[p^\infty] = 0$. This implies that $\mathrm{Sel}(E/F) = 0$. Consequently, $\mathrm{Sel}^{\vec{s}}(E/F_\infty)^G = 0$. Since G is pro-p, this in turn yields that $\mathrm{Sel}^{\vec{s}}(E/F_\infty) = 0$ as required. □

Finally, we end our article with the following observation, which is a generalization of [1, Corollary 2.8].

Corollary 5.5. *Assume that* (S1)–(S5) *are valid. Suppose that* $\vec{s}$ *is such that* $\mathrm{Sel}^{\vec{s}}(E/F_\infty) = 0$. *Then* $\mathrm{Sel}^{\vec{t}}(E/F_\infty) = 0$ *for every* $\vec{t} \in \{+,-\}^{\Sigma_{\mathrm{ss}}}$ *that verifies* (S5)(b).

Proof. Following from the proof of Theorem 5.3, the restriction map

$$\mathrm{Sel}(E/F) \to \mathrm{Sel}^{\vec{s}}(E/F_\infty)^G$$

is injective with finite cokernel. In particular, our hypothesis implies that $\mathrm{Sel}(E/F) = 0$ and hence is finite. By the fact that $\chi(G, X^{\vec{s}}(E/F_\infty)) = 1$ and Theorem 5.3, we have $Ш(E/F)[p^\infty] = 0$, $c_v^{(p)} = 1$ for every $v \in \Sigma'$ and $|\widetilde{E}_v(f_v)| = 1$ for every $v \in \Sigma_{\mathrm{o}}$. One may now proceed as in the proof of Corollary 5.4 to show that $\mathrm{Sel}^{\vec{t}}(E/F_\infty) = 0$. □

References

[1] S. Ahmed & M. F. Lim, "On the Euler characteristics of signed Selmer groups", *Bull. Aust. Math. Soc.* **101** (2020), no. 2, p. 238-246.

[2] K. Büyükboduk & A. Lei, "Coleman-adapted Rubin–Stark Kolyvagin systems and supersingular Iwasawa theory of CM abelian varieties", *Proc. Lond. Math. Soc.* **111** (2015), no. 6, p. 1338-1378.

[3] ———, "Integral Iwasawa theory of Galois representations for non-ordinary primes", *Math. Z.* (2017), p. 361-398.

[4] J. Coates, T. Fukaya, K. Kato, R. Sujatha & O. Venjakob, "The GL_2 main conjecture for elliptic curves without complex multiplication", *Publ. Math., Inst. Hautes Étud. Sci.* **101** (2005), p. 163-208.

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

[6] J. Coates & S. Howson, "Euler characteristics and elliptic curves II", *J. Math. Soc. Japan* **53** (2001), no. 1, p. 175-235.

[7] J. Coates, P. Schneider & R. Sujatha, "Links between cyclotomic and GL_2 Iwasawa theory", *Doc. Math.* **8** (2003), p. 187-215, Extra Volume: Kazuya Kato's fiftieth birthday.

[8] R. Greenberg, "Galois theory for the Selmer group of an abelian variety", *Compos. Math.* **136** (2003), no. 3, p. 255-297.

[9] Y. Hachimori & T. Ochiai, "Notes on non-commutative Iwasawa theory", *Asian J. Math.* **14** (2010), no. 1, p. 11-17.

[10] Y. Hachimori & O. Venjakob, "Completely faithful Selmer groups over Kummer extensions", *Doc. Math.* **8** (2003), p. 443-478, Extra Volume: Kazuya Kato's fiftieth birthday.

[11] P.-C. Hung & M. F. Lim, "On the growth of Mordell–Weil ranks in p-adic Lie extensions", *Asian J. Math.* **24** (2020), no. 4, p. 549-570.

[12] K. Iwasawa, "On $\mathbb{Z}_l$-extensions of algebraic number fields", *Ann. Math.* **98** (1973), no. 2, p. 246-326.

[13] U. Jannsen, "A spectral sequence for Iwasawa adjoints", *Münster J. Math.* **7** (2014), no. 1, p. 135-148.

[14] K. Kato, "p-adic Hodge theory and values of zeta functions of modular forms", in *Cohomologies p-adiques et applications arithmétiques. III*, Astérisque, vol. 295, Société Mathématique de France, 2004, p. 117-290.
[15] B. D. Kim, "The parity conjecture for elliptic curves at supersingular reduction primes", *Compos. Math.* **143** (2007), no. 1, p. 47-72.
[16] ———, "The plus/minus Selmer groups for supersingular primes", *J. Aust. Math. Soc.* **95** (2013), no. 2, p. 189-200.
[17] ———, "Signed–Selmer groups over the $\mathbb{Z}_p^2$-extension of an imaginary quadratic field", *Can. J. Math.* **66** (2014), no. 4, p. 826-843.
[18] B. D. Kim & J. Park, "The main conjecture of Iwasawa theory for elliptic curves with complex multiplication over abelian extensions at supersingular primes", *Acta Arith.* **181** (2017), no. 3, p. 209-238.
[19] T. Kitajima & R. Otsuki, "On the plus and the minus Selmer groups for elliptic curves at supersingular primes", *Tokyo J. Math.* **41** (2018), no. 1, p. 273-303.
[20] S.-i. Kobayashi, "Iwasawa theory for elliptic curves at supersingular primes", *Invent. Math.* **152** (2003), no. 1, p. 1-36.
[21] A. Lei & M. F. Lim, "Mordell–Weil ranks and Tate–Shafarevich groups of elliptic curves with mixed-reduction type over cyclotomic extensions", *Int. J. Number Theory* (2021), to appear, `https://doi.org/10.1142/S1793042122500208`.
[22] A. Lei & B. Palvannan, "Codimension two cycles in Iwasawa theory and elliptic curves with supersingular reduction", *Forum Math.* **7** (2019), article no. e25 (81 pages).
[23] A. Lei & F. Sprung, "Ranks of elliptic curves over $\mathbb{Z}_p^2$-extensions", *Isr. J. Math.* **236** (2020), no. 1, p. 183-206.
[24] A. Lei & R. Sujatha, "On Selmer groups in the supersingular reduction case", *Tokyo J. Math.* **43** (2020), no. 2, p. 455-479.
[25] A. Lei & S. L. Zerbes, "Signed Selmer groups over p-adic Lie extensions", *J. Théor. Nombres Bordeaux* **24** (2012), no. 2, p. 377-403.
[26] M. F. Lim, "A remark on the $\mathfrak{M}_H(G)$-conjecture and Akashi series", *Int. J. Number Theory* **11** (2015), no. 1, p. 269-297.
[27] ———, "Notes on the fine Selmer groups", *Asian J. Math.* **21** (2017), no. 2, p. 337-362.
[28] A. Mattuck, "Abelian varieties over p-adic ground field", *Ann. Math.* **62** (1955), no. 1, p. 92-119.
[29] B. Mazur, "Rational points of abelian varieties with values in towers of number fields", *Invent. Math.* **18** (1972), p. 183-266.
[30] J. Neukirch, A. Schmidt & K. Wingberg, *Cohomology of Number Fields*, 2nd ed., Grundlehren der Mathematischen Wissenschaften, vol. 323, Springer, 2008.
[31] F. A. E. Nuccio & R. Sujatha, "Residual supersingular Iwasawa theory and signed Iwasawa invariants", `https://arxiv.org/abs/1911.10649`, to appear in *Rend. Semin. Mat. Univ. Padova*, 2021.
[32] Y. Ochi & O. Venjakob, "On the ranks of Iwasawa modules over p-adic Lie extensions", *Math. Proc. Camb. Philos. Soc.* **135** (2003), no. 1, p. 25-43.
[33] B. Perrin-Riou, *Arithmétique des courbes elliptiques et theórie d'Iwasawa*, Mémoires de la Société Mathématique de France, vol. 17, Société Mathématique de France, 1984, 130 pages.
[34] ———, *p-adic L-functions and p-adic representations*, SMF/AMS Texts and Monographs, vol. 3, Société Mathématique de France; American Mathematical Society, 2000, xx+150 pages.
[35] A. Saikia, "Selmer groups of elliptic curves with complex multiplication", *Can. J. Math.* **56** (2004), no. 1, p. 194-208.
[36] P. Schneider, "Iwasawa L-functions of varieties over algebraic number fields, A first approach", *Invent. Math.* **71** (1983), p. 251-293.
[37] ———, "p-adic height pairings II", *Invent. Math.* **79** (1985), p. 329-374.
[38] S. Wadsley, "Euler characteristics, Akashi series and compact p-adic Lie groups", *Proc. Am. Math. Soc.* **138** (2010), no. 10, p. 3455-3465.
[39] S. L. Zerbes, "Selmer groups over p-adic Lie extensions I", *J. Lond. Math. Soc.* **70** (2004), no. 3, p. 586-608.

[40] ———, "Generalised Euler characteristics of Selmer groups", *Proc. Lond. Math. Soc.* **98** (2009), no. 3, p. 775-796.
[41] ———, "Akashi series of Selmer groups", *Math. Proc. Camb. Philos. Soc.* **151** (2011), no. 2, p. 229-243.

Antonio Lei
Département de Mathématiques et de Statistique
Université Laval
Pavillion Alexandre-Vachon
1045 Avenue de la Médecine
Québec, QC
Canada G1V 0A6
E-mail: antonio.lei@mat.ulaval.ca

Meng Fai Lim
School of Mathematics and Statistics & Hubei Key Laboratory of Mathematical Sciences
Central China Normal University
Wuhan, 430079
P.R.China
E-mail: limmf@mail.ccnu.edu.cn