Mathematical Proceedings of the Cambridge Philosophical Society

On the cohomology of Kobayashi's plus/minus norm groups and applications

BY MENG FAI LIM

School of Mathematics and Statistics & Hubei Key Laboratory of Mathematical Sciences, Central China Normal University, Hubei, Wuhan No. 152 *Luoyu Road,* 430079, *P.R.China.*
e-mail: limmf@mail.ccnu.edu.cn

Abstract

The plus and minus norm groups are constructed by Kobayashi as subgroups of the formal group of an elliptic curve with supersingular reduction, and they play an important role in Kobayashi's definition of the signed Selmer groups. In this paper, we study the cohomology of these plus and minus norm groups. In particular, we show that these plus and minus norm groups are cohomologically trivial. As an application of our analysis, we establish certain (quasi-)projectivity properties of the non-primitive mixed signed Selmer groups of an elliptic curve with good reduction at all primes above p. We then build on these projectivity results to derive a Kida formula for the signed Selmer groups under a slight weakening of the usual $\mu = 0$ assumption, and study the integrality property of the characteristic element attached to the signed Selmer groups.

2020 Mathematics Subject Classification: 11R23 (Primary); 11G05, 11S25 (Secondary)

---

1. *Introduction*

Let p be an odd prime. For now, let E denote an elliptic curve over $\mathbb{Q}_p$ with good supersingular reduction and $a_p = 1 + p - |\tilde{E}(\mathbb{F}_p)| = 0$, where $\tilde{E}_v$ is the reduced curve of E. Let $\mathcal{K}$ be a finite unramified extension of $\mathbb{Q}_p$, and let $\mathcal{K}_\infty$ denote the cyclotomic $\mathbb{Z}_p$-extension of $\mathcal{K}$. Kobayashi [21] defined the plus/minus norm groups $\widehat{E}^\pm(\mathcal{K}_\infty)$, which

are subgroups of the formal group of the said elliptic curve. These plus/minus norm groups are integral components in the definition of the signed Selmer groups. In particular, they come up in the local conditions at the supersingular primes in the definition of the Selmer groups, which were originally defined by Kobayashi [21], and later studied by other authors (for instances, see [2, 17–20, 22–25]). In this paper, we will study the cohomology of the plus/minus norm groups, and our results are as follow.

PROPOSITION (Proposition 3·8). *For every subgroup H of* $\mathrm{Gal}(\mathcal{K}/\mathbb{Q}_p)$, *we have*

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

The Λ-structure of the $\widehat{E}^{\pm}(\mathcal{K}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ has been well-studied (for instances, see [17, 19–21]). When 4 divides $|\mathcal{K} : \mathbb{Q}_p|$, it has been observed by Kitajima–Otsuki [20] that $E^+(\mathcal{K}_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p$ is not even cofree over Λ, much less $\Lambda[\mathrm{Gal}(\mathcal{K}/\mathbb{Q}_p)]$. Therefore, Proposition 3·8 may seems rather surprising in view of these prior results. After this work is completed, Takenori Kataoka has pointed out to the author that the cohomological triviality of the plus/minus groups can be established by a slight refinement of the approach of Kitajima–Otsuki which applies also to the case when 4 divides $|\mathcal{K} : \mathbb{Q}_p|$, and this was done in his thesis. (We thank him for making us aware of this.) We shall briefly say a bit on our proof which differs from the above approaches, and may be of independent interest. The proof requires a preliminary analysis of the formal group of E, where we have utilised a classical result of Noether [29] on the Galois module structure of the ring of integers of unramified extensions and a deep result of Coates–Greenberg [5] on the formal groups of E over infinitely ramified pro-p extensions. Curiously, no prior knowledge of the explicit structural description of the plus/minus groups, as mentioned above, is required in the eventual proof.

We move to global consideration, which is the main motivation behind our study on the plus/minus norm groups. From now on, E will denote an elliptic curve which is defined over a number field F'. Let F be a finite extension of F' and K a finite Galois extension of F. The following assumptions will be in full force for our datum $(E, F/F', K)$ throughout.

(S1) The elliptic curve E has good reduction at all primes of F' above p.

(S2) There exists at least one prime of F' above p at which the elliptic curve E has good supersingular reduction.

(S3) For each prime u of F' above p at which E has supersingular reduction, we have
   (a) $F_u' = \mathbb{Q}_p$ with u being unramified in K/F' (and hence in F/F').
   (b) $a_u = 1 + p - |\tilde{E}_u(\mathbb{F}_p)| = 0$, where $\tilde{E}_u$ is the reduction of E at u.

Let Σ be a finite set of primes of F which contains all the primes above p, all the ramified primes of F/F' and K/F, the bad reduction primes of E and the archimedean primes. Denote by Σ_p (resp., Σ_1) the set of primes of F above p (resp. the set of primes of F not dividing p). Write Σ_p^{ord} (resp., Σ_p^{ss}) for the set of primes in Σ_p at which E has good ordinary reduction (resp., good supersingular reduction).

For each $v \in \Sigma_p^{ss}$, we can choose one of the two plus and minus norm subgroups. Fix such a collection of choices $\overrightarrow{s} = (s_v)_{v \in \Sigma_p^{ss}} \in \{\pm\}^{\Sigma_p^{ss}}$. By choosing the signs of each supersingular prime of E over K in a consistent manner with respect to $\overrightarrow{s}$ (see Subsection 4·1), we attach a signed Selmer group $\mathrm{Sel}^{\overrightarrow{s}}(E/K_\infty)$ over the cyclotomic $\mathbb{Z}_p$-extension K_∞ of K. If Σ_0 is a subset of Σ_1, one can also define a non-primitive signed Selmer group $\mathrm{Sel}_{\Sigma_0}^{\overrightarrow{s}}(E/K_\infty)$

(see Subsection 4·2 for the precise definition). Every of these signed Selmer groups has a natural $\Lambda[G]$-action, where $\Lambda = \mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]]$ and $G = \mathrm{Gal}(K/F)$. We shall write $X^{\vec{s}}(E/K_\infty)$ and $X^{\vec{s}}_{\Sigma_0}(E/K_\infty)$ for the Pontryagin dual of $\mathrm{Sel}^{\vec{s}}(E/K_\infty)$ and the Pontryagin dual of $\mathrm{Sel}^{\vec{s}}_{\Sigma_0}(E/K_\infty)$ respectively.

Following Greenberg [**9**], we set

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

Our results on the non-primitive signed Selmer groups are as follow.

THEOREM (Theorem 4·7). *Suppose that* $(S1) - (S3)$ *are satisfied and that* Σ_0 *contains* $\Phi_{K/F}$. *Assume that* $X^{\vec{s}}(E/K_\infty)$ *is torsion over* $\mathbb{Z}_p[[\Gamma]]$ *and that* $\theta(X^{\vec{s}}(E/K_\infty)) \leqslant 1$. *Then* $X^{\vec{s}}_{\Sigma_0}(E/K_\infty)/X^{\vec{s}}_{\Sigma_0}(E/K_\infty)[p]$ *is quasi-projective as a* $\mathbb{Z}_p[G]$-*module. Furthermore, if* $X^{\vec{s}}(E/K_\infty)$ *is finitely generated over* $\mathbb{Z}_p$, *then* $X^{\vec{s}}_{\Sigma_0}(E/K_\infty)$ *is quasi-projective as a* $\mathbb{Z}_p[G]$-*module.*

Here $\theta(M)$ is the largest exponent of p occurring in the structural decomposition of the $\mathbb{Z}_p[[\Gamma]]$-module M.

THEOREM (Theorem 4·8). *Suppose that* $(S1) - (S3)$ *are satisfied and that* Σ_0 *contains* $\Phi_{K/F}$. *Assume that* $\mathrm{Sel}^{\vec{s}}(E/K_\infty)$ *is cotorsion over* $\mathbb{Z}_p[[\Gamma]]$, *and that for each* $v \in \Sigma_p^{ord}$, *either* v *is non-anomalous for* E/K *or* v *is tamely ramified in* K/F. *Then* $X^{\vec{s}}_{\Sigma_0}(E/K_\infty)$ *has a free resolution of length 1 as a* $\Lambda[G]$-*module. Moreover, if one assumes further that* $X^{\vec{s}}(E/K_\infty)$ *is finitely generated over* $\mathbb{Z}_p$, *then* $X^{\vec{s}}_{\Sigma_0}(E/K_\infty)$ *is projective as a* $\mathbb{Z}_p[G]$-*module.*

When the elliptic curve E has good ordinary reduction at all primes above p, the above results were proved by Greenberg for the p-primary Selmer group in his monograph [**9**]. The proof of our theorem follows his strategy, where the essential difference lies in that we rely on our Proposition 3·8 to handle the local analysis at supersingular primes above p. Readers would have observe that we require the extension K/F to be unramified at the supersingular primes (which is not required in the situation when E has good ordinary reduction at all primes above p). This latter assumption is imposed on us by necessity due to that we do not have a nice enough decent theory for the plus/minus norm groups in ramified extension outside cyclotomic $\mathbb{Z}_p$-extension (see [**25**]).

The remainder of the paper is concerned with applications of the above theorems. As a start, we establish a Kida formula for the signed Selmer groups under a slight weakening of the usual $\mu = 0$ assumption (see Proposition 5·2), which is inspired by an analogous result of Hachimori–Sharifi [**11**] for the classical λ-invariants in cyclotomic $\mathbb{Z}_p$-extensions of CM fields. When the elliptic curve E has good ordinary reduction at all primes above p, the Kida formula was first derived by Hachimori–Matsuno [**10**] building on an idea of Iwasawa [**13**] (also see [**9**]). When the elliptic curve E has good supersingular reduction at all primes above p, a Kida formula is also established for the signed Selmer groups in [**12**] and [**30**] by an argument via congruence of Galois representations. Our approach differs from these and has the advantage of obtaining a Kida's formula under a weakening of the usual $\mu = 0$ assumption, thus generalising these results slightly. We should also mention that pertaining to this sort of theme, Alexandra Nichifor had worked out the connection between Kida's formula and projectivity for the classical Iwasawa modules in her thesis

which unfortunately is unpublished. (The author thanks Bharathwaj Palvannan for pointing this out.) Finally, we study certain integrality property of the characteristic elements of the non-primitive signed Selmer groups (see Proposition 5·4). These characteristic elements are important objects of study and play a crucial role in the formulation of the main conjecture (see [**4**, **22**]). We should mention that for classical Iwasawa modules over totally real fields, the integrality property was recently studied by Nichifor–Palvannan in [**28**]. Our result can therefore be viewed as analogue of theirs.

2. *Projectivity properties*

In this section, we collect several results on the projectivity properties of modules, most of which can be found in the monograph [**9**]. For the convenience of the readers, we shall supply details to certain assertions that are essentially in [**9**] but perhaps not stated explicitly. In Subsection 2·3, we also recall the notion of characteristic elements of Iwasawa modules following [**4**], and a certain maximal order following [**28**], where the characteristic elements are expected to come from. Throughout this section, G will always denote a fixed finite group.

2·1. $\mathbb{Z}_p[G]$-*modules*

As a start, we record the following criterion for a module to be projective over $\mathbb{Z}_p[G]$.

PROPOSITION 2·1. *Let X be a $\mathbb{Z}_p[G]$-module which is a free $\mathbb{Z}_p$-module of finite rank. Write $S = Hom(X, \mathbb{Q}_p/\mathbb{Z}_p)$. Suppose that $H^i(H, S) = 0$ for $i = 1, 2$ and for every subgroup H of G. Then X is projective as a $\mathbb{Z}_p[G]$-module.*

Proof. See [**9**, proposition 2·1·1].

As noted in [**9**], for arithmetic applications, it is usually useful to work with the following weaker projectivity properties which we now recall.

Definition 2·2. A finitely generated $\mathbb{Z}_p[G]$-module X is said to be strictly quasi-projective if there exists a projective $\mathbb{Z}_p[G]$-module Y and a $\mathbb{Z}_p[G]$-homomorphism $X \to Y$ with finite kernel and cokernel.

The finitely generated $\mathbb{Z}_p[G]$-module X is said to be quasi-projective if there is a short exact sequence

$$0 \longrightarrow X_1 \longrightarrow X_2 \longrightarrow X \longrightarrow 0$$

of finitely generated $\mathbb{Z}_p[G]$-modules with X_1 and X_2 being strictly quasi-projective as $\mathbb{Z}_p[G]$-modules.

For alternative (and equivalent) definitions of strictly quasi-projective modules and quasi-projective modules, we refer readers to [**9**, section 2].

For our purpose, it is useful to have a criterion for quasi-projectivity. To do this, we need to introduce certain notation and notions. Fix an integer $m \geqslant 1$ which is divisible by the order of all elements of G. Let $\mathcal{F}$ denote a finite extension of $\mathbb{Q}_p$ which contains all mth roots of unity, whose ring of integers is in turn denoted by $\mathcal{O}$. For a cyclic subgroup C of G, we write $C = PQ$, where P is a p-group and Q is a group with order prime to p. Set $S = \mathrm{Hom}(X, \mathbb{Q}_p/\mathbb{Z}_p)$. For a 1-dimensional character ε of Q, we denote by e_ε the idempotent for ε in $\mathcal{O}[Q]$. We shall then write $S^\varepsilon = e_\varepsilon(S \otimes_{\mathbb{Z}_p} \mathcal{O})$. In the subsequent discussion, we abbreviate $h_P(-)$ for the Herbrand quotient $|H^2(P, -)|/|H^1(P, -)|$.

PROPOSITION 2·3. *Let X be a finitely generated $\mathbb{Z}_p[G]$-module. Write $S = $ Hom$(X, \mathbb{Q}_p/\mathbb{Z}_p)$. Then X is quasi-projective as a $\mathbb{Z}_p[G]$-module if and only if for every cyclic subgroup $C = PQ$ of G and every 1-dimensional character character ε of Q, we have $h_P(S^\varepsilon) = 1$.*

Proof. See [**9**, proposition 2·1·3].

The properties of a quasi-projectivity $\mathbb{Z}_p[G]$-module are well-documented in [**9**]. For our purposes, we are mainly concerned with the following situation when G is a finite p-group.

PROPOSITION 2·4. *Suppose that G is a finite p-group and that X is a finitely generated quasi-projective $\mathbb{Z}_p[G]$-module. Then we have*

$$\operatorname{rank}_{\mathbb{Z}_p}(X) = |G|\operatorname{rank}_{\mathbb{Z}_p}(X_G).$$

This is essentially established in [**9**, sections 1 and 2] but not explicitly stated there. For the convenience of the reader, we give a proof here. To begin with, we have the following preparatory lemma.

LEMMA 2·5. *Suppose that X is a finitely generated quasi-projective $\mathbb{Z}_p[G]$-module. Then for every cyclic normal subgroup N of G, X_N is quasi-projective as a $\mathbb{Z}_p[G/N]$-module.*

Proof. If X is a projective $\mathbb{Z}_p[G]$-module, then X_N is clearly projective as a $\mathbb{Z}_p[G/N]$-module. Now suppose that X is strictly quasi-projective as a $\mathbb{Z}_p[G]$-module. Hence we have a $\mathbb{Z}_p[G]$-homomorphism $X \to Y$ with finite kernel and cokernel, and where Y is some projective $\mathbb{Z}_p[G]$-module. It is easy to see that the $\mathbb{Z}_p[G]$-homomorphism $X \to Y$ induces a $\mathbb{Z}_p[G/N]$-homomorphism $X_N \to Y_N$ with finite kernel and cokernel. But as noted at the beginning of the paragraph, Y_N is projective as a $\mathbb{Z}_p[G/N]$-module. Therefore, it follows that X_N is strictly quasi-projective as a $\mathbb{Z}_p[G/N]$-module.

Now suppose that X is a finitely generated quasi-projective $\mathbb{Z}_p[G]$-module. In other words, one has a short exact sequence

$$0 \longrightarrow X_1 \longrightarrow X_2 \longrightarrow X \longrightarrow 0$$

for some strictly quasi-projective $\mathbb{Z}_p[G]$-modules X_1 and X_2. Taking N-invariant, we have the following exact sequence

$$H_1(N, X) \longrightarrow (X_1)_N \stackrel{f}{\longrightarrow} (X_2)_N \longrightarrow X_N \longrightarrow 0.$$

Since N is cyclic, we have that $H_1(N, X)$ is finite by Proposition 2·3. Combining this observation with that $(X_1)_N$ is a strictly quasi-projective $\mathbb{Z}_p[G/N]$-module, it follows that im f is also strictly quasi-projective over $\mathbb{Z}_p[G/N]$. Hence X_N is a quasi-projective $\mathbb{Z}_p[G/N]$-module.

We can now give the proof of Proposition 2·4.

Proof of Proposition 2·4. We shall first prove the proposition for a projective $\mathbb{Z}_p[G]$-module. Since the ring $\mathbb{Z}_p[G]$ is local, a projective $\mathbb{Z}_p[G]$-module is necessarily free over $\mathbb{Z}_p[G]$, and one clearly has the equality of the proposition in this situation.

Now, suppose that X is strictly quasi-projective as a $\mathbb{Z}_p[G]$-module. By definition, there exists some projective $\mathbb{Z}_p[G]$-module Y and a $\mathbb{Z}_p[G]$-homomorphism $X \to Y$ with finite kernel and cokernel. The latter induces a $\mathbb{Z}_p$-homomorphism $X_G \to Y_G$ with finite kernel and cokernel. It then follows that

$$\operatorname{rank}_{\mathbb{Z}_p}(X) = \operatorname{rank}_{\mathbb{Z}_p}(Y) = |G|\operatorname{rank}_{\mathbb{Z}_p}(Y_G) = |G|\operatorname{rank}_{\mathbb{Z}_p}(X_G),$$

where the middle equality follows from the discussion in the previous paragraph.

It remains to consider the situation that X is a finitely generated quasi-projective $\mathbb{Z}_p[G]$-module. For now, we assume that the group G is cyclic of order p. Then one has a short exact sequence

$$0 \longrightarrow X_1 \longrightarrow X_2 \longrightarrow X \longrightarrow 0$$

for some strictly quasi-projective $\mathbb{Z}_p[G]$-modules X_1 and X_2. From this short exact sequence, we have

$$H_1(G, X) \longrightarrow (X_1)_G \longrightarrow (X_2)_G \longrightarrow X_G \longrightarrow 0.$$

By the quasi-projective hypothesis and our assumption on G being a cyclic group, we may apply Proposition 2·3 to conclude that $H_1(G, X)$ is finite. Combining this observation with the above exact sequence, we obtain

$$\operatorname{rank}_{\mathbb{Z}_p}(X) = \operatorname{rank}_{\mathbb{Z}_p}(X_2) - \operatorname{rank}_{\mathbb{Z}_p}(X_1) = p\left(\operatorname{rank}_{\mathbb{Z}_p}(X_2)_G - \operatorname{rank}_{\mathbb{Z}_p}(X_1)_G\right) = p\operatorname{rank}_{\mathbb{Z}_p}(X_G).$$

This proves the proposition for a quasi-projective $\mathbb{Z}_p[G]$-module when G is a cyclic group of order p.

For a general finite p-group G, let N be a normal subgroup of G which is cyclic of order p. Then by the previous paragraph, we have

$$\operatorname{rank}_{\mathbb{Z}_p}(X) = p\operatorname{rank}_{\mathbb{Z}_p}(X_N).$$

By Lemma 2·5, X_N is quasi-projective over $\mathbb{Z}_p[G/N]$. Since $|G/N| < |G|$, it follows by induction that

$$\operatorname{rank}_{\mathbb{Z}_p}(X_N) = |G/N|\operatorname{rank}_{\mathbb{Z}_p}(X_G).$$

Combining the two equalities, we obtain the conclusion of the proposition.

2·2. λ-invariants

We consider a slight refinement of Proposition 2·3, again following [9]. Let Λ denote the classical Iwasawa algebra $\mathbb{Z}_p[[T]]$. For a torsion Λ-module M, there exist irreducible Weierstrass polynomials f_j, numbers α_i, β_j and a homomorphism

$$M \longrightarrow \Lambda^r \oplus \left(\bigoplus_{i=1}^{s} \Lambda/p^{\alpha_i}\right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/f_j^{\beta_j}\right)$$

with finite kernel and cokernel, where the numbers α_i β_j and the Weierstrass polynomials f_j are determined by M (cf. [27, (5·3·8)]). The μ-invariant $\mu(M)$ (resp., λ-invariant $\lambda(M)$)

of M is defined to be $\sum_{i=1}^{s} \alpha_i$ (resp., $\sum_{j=1}^{t} \beta_j \deg(f_j)$). We also set

$$\theta(M) := \max\{\alpha_i \mid i = 1, .., s\}.$$

We now record two easy lemmas which can be deduced easily from the structural theorem and are left to the readers.

LEMMA 2·6. *For a torsion Λ-module, we have $\theta(M) \leqslant 1$ if and only if $M/M[p]$ is finitely generated over $\mathbb{Z}_p$. Furthermore, in the event of such, we have*

$$\lambda(M) = \operatorname{rank}_{\mathbb{Z}_p}(M/M[p]).$$

LEMMA 2·7. *Let $\phi : M \to M'$ be a homomorphism of finitely generated torsion Λ-modules, whose kernel and cokernel are finitely generated over $\mathbb{Z}_p$. Then $\theta(M) = \theta(M')$.*

The next result is a slightly refined criterion for quasi-projectivity.

PROPOSITION 2·8. *Let X be a finitely generated $\Lambda[G]$-module which is torsion as a Λ-module and satisfies $\theta(X) \leqslant 1$. Denote by S the Pontryagin dual of X. Suppose that $H^1(N, S)$ and $H^2(N, S)$ are finite for every cyclic p-subgroup N of G. Then $X/X[p]$ is quasi-projective as a $\mathbb{Z}_p[G]$-module if and only if for every cyclic subgroup $C = PQ$ of G and every 1-dimensional character character ε of Q, we have $h_P(S^\varepsilon) = 1$.*

Proof. See [**9**, proposition 2·2·1] or [**11**, section 2].

We end this subsection with the following refinement of Proposition 2·4.

COROLLARY 2·9. *Let G be a finite p-group. Suppose that X is a $\Lambda[G]$-module which is torsion as a Λ-module with $\theta(X) \leqslant 1$, and that $X/X[p]$ is quasi-projective as a $\mathbb{Z}_p[G]$-module. Then we have*

$$\lambda(X) = |G|\lambda(X_G).$$

Proof. By Lemma 2·6, the module $X/X[p]$ is finitely generated over $\mathbb{Z}_p$. Consequently, we have

$$\lambda(X) = \operatorname{rank}_{\mathbb{Z}_p}(X/X[p]) = |G|\operatorname{rank}_{\mathbb{Z}_p}\left((X/X[p])_G\right),$$

where the first equality follows from Lemma 2·6 and the second equality from Proposition 2·4. On the other hand, we have an exact sequence

$$X[p]_G \longrightarrow X_G \longrightarrow (X/X[p])_G \longrightarrow 0,$$

where $X[p]_G$ is p-torsion. Thus, it follows that

$$\lambda(X_G) = \operatorname{rank}_{\mathbb{Z}_p}\left((X/X[p])_G\right),$$

which yields the required conclusion of the corollary.

2·3. *Characteristic elements of $\Lambda[G]$-modules*

As before, G is a finite group, and Λ is the classical Iwasawa algebra $\mathbb{Z}_p[[T]]$. Following [**4**, **14**, **15**], we describe how to attach a characteristic element to a $\Lambda[G]$-module which is torsion over Λ.

Define the set

$$S = \{s \in \Lambda[G] \mid \Lambda[G]/\Lambda[G]s \text{ is finitely generated over } \mathbb{Z}_p\}.$$

It follows from [**4**, theorem 2·4] that S is a left and right Ore set consisting of nonzero divisors in $\Lambda[G]$. Set $S^* = \cup_n p^n S$. By [**4**, proposition 2·3], a finitely generated $\Lambda[G]$-module M is annihilated by S^* if and only if $M/M[p^\infty]$ is finitely generated over $\mathbb{Z}_p$. Since our group G is finite, the latter is equivalent to saying that M is torsion over Λ. In particular, the Grothendieck group of the category of finitely generated $\Lambda[G]$-modules that are torsion over Λ identifies with the relative K_0 group $K_0(\Lambda[G], \Lambda[G]_{S^*})$. Henceforth, if M is a finitely generated $\Lambda[G]$-module which is torsion over Λ, we may write $[M]$ for its class in $K_0(\Lambda[G], \Lambda[G]_{S^*})$. On the other hand, by the proof of [**14**, lemma 2·1], we have

$$\Lambda[G]_{S^*} \cong Q_\Lambda[G],$$

where Q_Λ is the fraction field of Λ. Under this identification, the localization sequence in K-theory yields the following exact sequence

$$K_1(\Lambda[G]) \longrightarrow K_1(Q_\Lambda[G]) \xrightarrow{\partial} K_0(\Lambda[G], Q_\Lambda[G]).$$

LEMMA 2·10. *The map ∂ in the above exact sequence is surjective.*

Proof. When G has no p-torsion, the surjectivity was established by Coates *et al* [**4**, proposition 3·4]. When G has p-torsion, the surjectivity was established by Kakde in [**14**, lemma 1·5] for the Ore set S rather than S^*. But it is not difficult to see that his proof goes through for S^* with G having p-torsion. Alternatively, one can also obtain the conclusion of lemma, appealing to the K-theory of Waldhausen categories as done by Witte [**32**, corollary 3·8].

In view of the preceding lemma, it makes sense to make the following definition.

Definition 2·11 (Coates *et al* [**4**]). For a finitely generated $\Lambda[G]$-module M which is torsion over Λ, a characteristic element for M is an element $\xi_M \in K_1(Q_\Lambda[G])$ such that $\partial(\xi_M) = [M]$.

Remark 2·12. We emphasis that since our group G is finite, we can attach characteristic element to Λ-torsion $\Lambda[G]$-module as above. In the case that G is an infinite p-adic Lie group, one needs to impose a stronger hypothesis (the so-called $\mathfrak{M}_H(G)$-conjecture) on the module M to be able to define its characteristic element. We shall not need this in our paper but we do refer the interested readers to [**4**, **14**, **15**, **25**] for discussion on this.

To facilitate further discussion, we introduce a maximal Λ-order in $Q_\Lambda[G]$, following Nichifor–Palvannan [**28**]. By the Artin–Wedderburn theorem, there is an isomorphism

$$\mathbb{Q}_p[G] \cong \prod_i M_{m_i}(D_i)$$

of $\mathbb{Q}_p$-algebras, where $M_{m_i}(D_i)$ is the ring of $m_i \times m_i$-matrices over D_i and D_i is a finite dimensional division algebra over $\mathbb{Q}_p$. Denote by $\mathcal{O}_{D_i}$ the maximal $\mathbb{Z}_p$-order in D_i. One then has the following commutative diagram

$$
\begin{array}{ccc}
\mathbb{Z}_p[G] & \longrightarrow & \mathbb{Q}_p[G] \\
\downarrow & & \downarrow \cong \\
\prod_i M_{m_i}(\mathcal{O}_{D_i}) & \longrightarrow & \prod_i M_{m_i}(D_i),
\end{array}
$$

where the horizontal maps and leftmost vertical map are injective. This in turn induces the commutative diagram

$$
\begin{array}{ccc}
\Lambda[G] & \longrightarrow & Q_\Lambda[G] \\
\downarrow & & \downarrow \cong \\
\prod_i M_{m_i}(\mathcal{O}_{D_i} \otimes_{\mathbb{Z}_p} \Lambda) & \longrightarrow & \prod_i M_{m_i}(D_i \otimes_{\mathbb{Q}_p} Q_\Lambda),
\end{array}
$$

where the horizontal maps and leftmost vertical map are also injective. We shall set

$$
M_{\Lambda[G]} := \prod_i M_{m_i}(\mathcal{O}_{D_i} \otimes_{\mathbb{Z}_p} \Lambda),
$$

which we view as a subring of $Q_\Lambda[G]$ containing $\Lambda[G]$. In fact, it follows from a combination of [**28**, proposition 2·11] and [**31**, theorem 10·5] that $M_{\Lambda[G]}$ is a maximal Λ-order of $Q_\Lambda[G]$ which contains $\Lambda[G]$. We can now state the following result.

PROPOSITION 2·13. *Let X be a finitely generated $\Lambda[G]$-module which is Λ-torsion. Suppose that X has a free resolution of length one as a $\Lambda[G]$-module. Then ξ_X belongs to the image of the following natural map*

$$
M_{\Lambda[G]} \cap Q_\Lambda[G]^\times \longrightarrow K_1(Q_\Lambda[G]).
$$

Proof. This was proved in [**28**, theorem 1] for a certain class of arithmetic Iwasawa modules. There they have an extra assumption on the validity of certain main conjecture [**28**, conjecture 3·2]. Going through the proof, one sees that the validity of the main conjecture is only used in attaching characteristic elements to their Iwasawa modules. However, for any module X satisfying the hypothesis in our proposition, we have seen from Lemma 2·10 and Definition 2·11 that one can always attach characteristic element to it. The remainder of the proof of [**28**, theorem 1] is purely algebraic relying on the free resolution hypothesis and an algebraic result [**28**, proposition 2·13], and requires no additional input of the main conjecture. Going though the proof, one can see that this part of the argument carries over to prove the proposition.

As the preceding proposition requires a $\Lambda[G]$-module to have a free resolution of length one, it will be useful to have the following criterion.

PROPOSITION 2·14. *Let X be a finitely generated $\Lambda[G]$-module, where $\Lambda = \mathbb{Z}_p[[T]]$. Suppose that X is torsion as a Λ-module and has no nonzero finite Λ-submodule. Let $S = \mathrm{Hom}_{\mathrm{cts}}(X, \mathbb{Q}_p/\mathbb{Z}_p)$. Then X has a free resolution of length one as a $\Lambda[G]$-module if and only if $H^i(H, S) = 0$ for $i = 1, 2$ and for every subgroup H of G.*

Proof. See [9, proposition 2·4·1] or [28, proposition 4·1 and Remark 4·2].

3. *Elliptic curve over $\mathbb{Q}_p$ with supersingular reduction*

In this section, E will denote an elliptic curve defined over $\mathbb{Q}_p$ with supersingular reduction and $a_p = 0$. We write $\widehat{E}$ for its formal group. Throughout, for an extension L 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. Let $\mathcal{K}$ be a finite unramified extension of $\mathbb{Q}_p$. Denote by $\mathbb{Q}_{p,\infty}$ (resp., $\mathcal{K}_\infty$) the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}_p$ (resp., $\mathcal{K}$). Since $\mathcal{K}/\mathbb{Q}_p$ is unramified and $\mathbb{Q}_{p,\infty}/\mathbb{Q}_p$ is totally ramified, we have $\mathbb{Q}_{p,\infty} \cap \mathcal{K} = \mathbb{Q}_p$ and $\mathcal{K}_\infty = \mathcal{K}\mathbb{Q}_{p,\infty}$. Consequently, we have an isomorphism $\mathrm{Gal}(\mathcal{K}_\infty/\mathbb{Q}_p) \cong \mathrm{Gal}(\mathcal{K}/\mathbb{Q}_p) \times \mathrm{Gal}(\mathcal{K}_\infty/\mathcal{K})$ of abelian groups. Denote by $\mathcal{K}_n$ the intermediate subextension of $\mathcal{K}_\infty/\mathcal{K}$ with $|\mathcal{K}_n : \mathcal{K}| = p^n$. The residue field of $\mathcal{K}_n$ is in turn denoted by k_n.

LEMMA 3·1. *The formal group $\widehat{E}(\mathcal{K}_n)$ has no p-torsion for every n. In particular, $E(\mathcal{K}_n)$ has no p-torsion for every n.*

Proof. The first assertion follows from [20, proposition 3·1] or [21, proposition 8·7]. The second assertion follows from the first, the following short exact sequence

$$0 \longrightarrow \widehat{E}(\mathcal{K}_n) \longrightarrow E(\mathcal{K}_n) \longrightarrow \widetilde{E}(k_n) \longrightarrow 0$$

and that $\widetilde{E}(k_n)$ has no p-torsion by the supersingular assumption.

For subsequent discussion in this section, we shall write $G = \mathrm{Gal}(\mathcal{K}/\mathbb{Q}_p)$ which is also identified with $\mathrm{Gal}(\mathcal{K}_\infty/\mathbb{Q}_{p,\infty})$. For a subgroup H of G, we write $\mathcal{L} := \mathcal{L}(H)$ for the fixed field of $\mathcal{K}$ by H. Via the above identification, we may regard H as a subgroup of $\mathrm{Gal}(\mathcal{K}_\infty/\mathbb{Q}_{p,\infty})$. Under this setup, one can verify easily that the fixed field of $\mathcal{K}_\infty$ by H is precisely given by $\mathcal{L}_\infty$, the cyclotomic $\mathbb{Z}_p$-extension of $\mathcal{L}$.

3·1. *Cohomology of formal groups*

In this subsection, we will study the cohomology of the formal group. We begin with the following observation which builds on a classical result of Noether [29].

LEMMA 3·2. $\widehat{E}(\mathcal{K})$ *is a free $\mathbb{Z}_p[G]$-module of rank* 1. *In particular, we have*

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

for every subgroup H of G and $i \geqslant 1$.

Proof. Since $\mathcal{K}$ is unramified over $\mathbb{Q}_p$, and taking Lemma 3·1 into account, the formal group logarithm gives an isomorphism $\widehat{E}(\mathcal{K}) \cong p\mathcal{O}_\mathcal{K} \cong \mathcal{O}_\mathcal{K}$. Again, as $\mathcal{K}$ is unramified over $\mathbb{Q}_p$, we may apply a classical result of Noether [29] to conclude that the latter is a free $\mathbb{Z}_p[G]$-module of rank 1. This proves the lemma.

Remark 3·3. The cohomological triviality of $\widehat{E}(\mathcal{K})$ is a classical result (for instance, see [5, proposition 3·9] or [6, propositions 3·10 and 4·2]). In fact, this suffices for the application in this paper. But we have thought it interesting to note down that one can actually establish the $\mathbb{Z}_p[G]$-freeness of $\widehat{E}(\mathcal{K})$ by appealing to Noether's result.

PROPOSITION 3·4. *For every subgroup H of G, we have*

$$H^i\left(H, \widehat{E}(\mathcal{K}) \otimes \mathbb{Q}_p/\mathbb{Z}_p\right) = \begin{cases} \widehat{E}(\mathcal{L}) \otimes \mathbb{Q}_p/\mathbb{Z}_p, & \text{if } i = 0, \\ 0, & \text{if } i \geqslant 1, \end{cases}$$

where $\mathcal{L} = \mathcal{K}^H$.

Proof. By Lemma 3·1, we have $\operatorname{Tor}_1^{\mathbb{Z}_p}(\widehat{E}(\mathcal{K}), \mathbb{Q}_p/\mathbb{Z}_p) = 0$ which in turn yields the following short exact sequence

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

In view of Lemma 3·2, upon taking H-invariant, we obtain

$$0 \longrightarrow \widehat{E}(\mathcal{L}) \longrightarrow \widehat{E}(\mathcal{L}) \otimes \mathbb{Q}_p \longrightarrow \left(\widehat{E}(\mathcal{K}) \otimes \mathbb{Q}_p/\mathbb{Z}_p\right)^H \longrightarrow 0$$

and

$$H^l\left(H, \widehat{E}(\mathcal{K}) \otimes \mathbb{Q}_p\right) \cong H^l\left(H, \widehat{E}(\mathcal{K}) \otimes \mathbb{Q}_p/\mathbb{Z}_p\right)$$

for $l \geqslant 1$. The isomorphism in the proposition for $i = 0$ follows from the short exact sequence. On the other hand, since H is finite and $\widehat{E}(\mathcal{K}) \otimes \mathbb{Q}_p$ is torsionfree, we have $H^l(H, \widehat{E}(\mathcal{K}) \otimes \mathbb{Q}_p) = 0$, or equivalently, $H^l(H, \widehat{E}(\mathcal{K}) \otimes \mathbb{Q}_p/\mathbb{Z}_p) = 0$.

We now record the following result on the structure of $\widehat{E}(\mathcal{K}_\infty)$ which is a partial analog of Lemma 3·2.

LEMMA 3·5. *We have $H^i\left(H, \widehat{E}(\mathcal{K}_\infty)\right) = 0$ for every subgroup H of G and $i \geqslant 1$.*

Proof. Recall that we write $\mathcal{L}$ for the fixed field of H. Then as seen in the discussion before Subsection 3·1, the cyclotomic $\mathbb{Z}_p$-extension $\mathcal{L}_\infty$ of $\mathcal{L}$ is the fixed field of $\mathcal{K}_\infty$ by H. By a well-known result of Coates–Greenberg [**5**, corollary 3·2], we have $H^i(\mathcal{K}_\infty, \widehat{E}(\bar{\mathcal{K}})) = 0 = H^i(\mathcal{L}_\infty, \widehat{E}(\bar{\mathcal{K}}))$ for $i \geqslant 1$. Hence the spectral sequence

$$H^i(H, H^j(\mathcal{K}_\infty, \widehat{E}(\bar{\mathcal{K}}))) \Longrightarrow H^{i+j}(\mathcal{L}_\infty, \widehat{E}(\bar{\mathcal{K}}))$$

degenerates yielding the required conclusion of the lemma.

PROPOSITION 3·6. *For every subgroup H of G, we have*

$$H^i\left(H, \widehat{E}(\mathcal{K}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p\right) = \begin{cases} \widehat{E}(\mathcal{L}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p, & \text{if } i = 0, \\ 0, & \text{if } i \geqslant 1, \end{cases}$$

where $\mathcal{L}_\infty = \mathcal{K}_\infty^H$.

Proof. This has a similar proof to that in Proposition 3·4, where we make use of Lemma 3·5 in place of Lemma 3·2.

3·2. *Cohomology of plus/minus norm groups*

In this subsection, we study the cohomology of the plus/minus norm groups. Following [18–21], we define the plus and minus norm groups

$$\widehat{E}^+(\mathcal{K}_n) = \big\{ P \in \widehat{E}(\mathcal{K}_n) \,:\, \mathrm{tr}_{n/m+1}(P) \in \widehat{E}(\mathcal{K}_l),\, 2 \mid m,\, 0 \leqslant m \leqslant n-1 \big\},$$

$$\widehat{E}^-(\mathcal{K}_n) = \big\{ P \in \widehat{E}(\mathcal{K}_n) \,:\, \mathrm{tr}_{n/m+1}(P) \in \widehat{E}(\mathcal{K}_l),\, 2 \nmid m,\, 0 \leqslant m \leqslant n-1 \big\},$$

where $\mathrm{tr}_{n/m+1} : \widehat{E}(\mathcal{K}_n) \longrightarrow \widehat{E}(\mathcal{K}_{m+1})$ denotes the trace map. These groups are related to the formal groups in the following way.

LEMMA 3·7. *There is a short exact sequence*

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

Proof. See [19, proposition 2·6] or [21, proposition 8·12].

We can now prove the following proposition as stated in the introductory section.

PROPOSITION 3·8. *For every subgroup H of G, we have*

$$H^i \left(H, \widehat{E}^\pm(\mathcal{K}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \right) = \begin{cases} \widehat{E}^\pm(\mathcal{L}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p, & \text{if } i = 0, \\ 0, & \text{if } i \geqslant 1. \end{cases}$$

Proof. In view of Lemmas 3·1 and 3·7, we have the following short exact sequences

$$0 \longrightarrow \widehat{E}(\mathcal{L}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \big(\widehat{E}^+(\mathcal{L}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \big) \oplus \big(\widehat{E}^-(\mathcal{L}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \big)$$
$$\longrightarrow \widehat{E}(\mathcal{L}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 0,$$
$$0 \longrightarrow \widehat{E}(\mathcal{K}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \big(\widehat{E}^+(\mathcal{K}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \big) \oplus \big(\widehat{E}^-(\mathcal{K}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \big)$$
$$\longrightarrow \widehat{E}(\mathcal{K}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 0,$$

which in turn fit into the following diagram

$$0 \longrightarrow \widehat{E}(\mathcal{L}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \big(\widehat{E}^+(\mathcal{L}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \big) \oplus \big(\widehat{E}^-(\mathcal{L}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \big) \longrightarrow \widehat{E}(\mathcal{L}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 0$$
$$\downarrow \qquad\qquad\qquad\qquad \downarrow \qquad\qquad\qquad\qquad \downarrow$$
$$0 \to \big(\widehat{E}(\mathcal{K}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \big)^H \to \big(\widehat{E}^+(\mathcal{K}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \big)^H \oplus \big(\widehat{E}^-(\mathcal{K}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \big)^H \to \big(\widehat{E}(\mathcal{K}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \big)^H \to \cdots$$

Since the leftmost and rightmost vertical maps are isomorphisms by Propositions 3·4 and 3·6, so is the middle map by a snake lemma argument. This yields the isomorphism of the proposition for $i = 0$. Now the bottom sequence of the diagram continues in the form

$$H^i(H, \widehat{E}(\mathcal{K}) \otimes \mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow H^i(H, \widehat{E}^+(\mathcal{K}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p) \oplus H^i(H, \widehat{E}^-(\mathcal{K}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p)$$
$$\longrightarrow H^i(H, \widehat{E}(\mathcal{K}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p).$$

Again, by virtue of Propositions 3·4 and 3·6, we obtain the desired vanishing for $i \geqslant 1$.

Recall that $\widehat{E}^\pm(\mathcal{K}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ injects into $H^1(\mathcal{K}_n, E[p^\infty])$ via the Kummer map (cf. [21, lemma 8·17]). Thus, it makes sense to speak of $H^1(\mathcal{K}_\infty, E[p^\infty])/\widehat{E}^\pm(\mathcal{K}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p$. We may now state and prove the following.

PROPOSITION 3·9. *For every subgroup H of G, we have*

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

Proof. Consider the spectral sequence

$$H^i\big(H, H^j(\mathcal{K}_\infty, E[p^\infty])\big) \Longrightarrow H^{i+j}(\mathcal{L}_\infty, E[p^\infty]).$$

By [**27**, theorem 7·1·8(i)], $H^l(\mathcal{K}_\infty, E[p^\infty]) = 0 = H^l(\mathcal{L}_\infty, E[p^\infty])$ for $l \geqslant 2$. Also, recall that $E(\mathcal{K}_\infty)[p^\infty] = 0$ by Lemma 3·1. Hence the spectral sequence degenerates to yield

$$H^i\big(H, H^1(\mathcal{K}_\infty, E[p^\infty])\big) = \begin{cases} H^1(\mathcal{L}_\infty, E[p^\infty]), & \text{if } i = 0, \\ 0, & \text{if } i \geqslant 1. \end{cases}$$

The conclusion of the corollary now follows from combining this latter observation with an analysis of the H-cohomology exact sequence of

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

and taking Proposition 3·8 into account.

It follows immediately from Proposition 3·9 that we have the following.

COROLLARY 3·10. *For every cyclic subgroup $C = PQ$ of G and every 1-dimensional character ε of Q, we have*

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

Proof. Write $M = H^1(\mathcal{K}_\infty, E[p^\infty])/\widehat{E}^\pm(\mathcal{K}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p$. By Proposition 3·9, we have $H^i(P, M) = 0$ for $i \geqslant 1$. Let $\mathcal{F}$ denote the ring of integers of a finite extension of $\mathbb{Q}_p$ which contains all m-th roots of unity, where m is divisible by the order of all elements of G. We clearly still have $H^i(P, M \otimes \mathcal{O}) = 0$ for $i \geqslant 1$. On the other hand, since $M \otimes \mathcal{O} = \oplus_\varepsilon e_\varepsilon(M \otimes_{\mathbb{Z}_p} \mathcal{O})$, it follows that we have $H^i(P, e_\varepsilon(M \otimes_{\mathbb{Z}_p} \mathcal{O})) = 0$ for $i \geqslant 1$. The conclusion of the corollary is now immediate from this.

Remark 3·11. One can actually have relative versions of the results in this section in the following sense. Let $\mathcal{K}$ and $\mathcal{M}$ be two finite unramified extensions of $\mathbb{Q}_p$ with $\mathcal{K} \subseteq \mathcal{M}$. Then every subgroup H' of $\mathrm{Gal}(\mathcal{M}/\mathcal{K})$, the same argument in this section can prove the following version of Propositions 3·8 and 3·9:

$$H^i\left(H', \widehat{E}^\pm(\mathcal{M}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p\right) = \begin{cases} \widehat{E}^\pm(\mathcal{M}_\infty^{H'}) \otimes \mathbb{Q}_p/\mathbb{Z}_p, & \text{if } i = 0, \\ 0, & \text{if } i \geqslant 1, \end{cases}$$

and

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

Similarly, one can also state relative versions of Proposition 3·4, Proposition 3·6 and Corollary 3·10 which we leave to the readers to fill in.

4. *Generalities on signed Selmer groups*

We now turn to the global situation, where we begin by fixing some notation and standing assumptions that will be adhered throughout the section. Let E be an elliptic curve defined over a number field F' and F a finite extension of F'. Fix a finite Galois extension K of F. The following assumptions will be in full force for our data $(E, F/F', K)$ throughout.

(S1) The elliptic curve E has good reduction at all primes of F' above p.

(S2) There exists at least one prime of F' above p at which the elliptic curve E has good supersingular reduction.

(S3) For each u of F' above p at which E has supersingular reduction, we have
(a) $F'_u = \mathbb{Q}_p$ and u is unramified in K/F'.
(b) $a_u = 1 + p - |\tilde{E}_u(\mathbb{F}_p)| = 0$, where $\tilde{E}_u$ is the reduction of E at u.

Let Σ be a finite set of primes of F which contains all the primes above p, all the ramified primes of F/F' and K/F, the bad reduction primes of E and the archimedean primes. Denote by Σ_p the set of primes of K above p. Write Σ_p^{ord} (resp., Σ_p^{ss}) for the set of primes in Σ_p at which E has good ordinary reduction (resp., good supersingular reduction). We shall also write $\Sigma_1 = \Sigma - \Sigma_p$ for the set of primes of F which are not divisible by p. For any subset R of Σ and any extension $\mathcal{F}$ of F, we shall write $R(\mathcal{F})$ for the set of primes of $\mathcal{F}$ above R.

Denote by K_∞ the cyclotomic $\mathbb{Z}_p$-extension of K and K_n the intermediate subfield of K_∞/K with $|K_n : K| = p^n$. Let L be an intermediate subextension of K/F. By (S2)-(S3), $K \cap L_\infty = L$, where L_∞ is the cyclotomic $\mathbb{Z}_p$-extension of L. Furthermore, denoting by L_n the intermediate intermediate subfield of L_∞/L with $|L_n : L| = p^n$, we have $K_n \cap L_\infty = L_n$ and $K_n = L_n K$. Thus, we have $\mathrm{Gal}(K_\infty/L) \cong \mathrm{Gal}(L_\infty/L) \times \mathrm{Gal}(K/L)$. We write Γ for $\mathrm{Gal}(F_\infty/F)$ which is identified with $\mathrm{Gal}(L_\infty/L)$ and, in particular, $\mathrm{Gal}(K_\infty/K)$. We shall also write $H_L = \mathrm{Gal}(K/L)$ which is identified with $\mathrm{Gal}(K_\infty/L_\infty)$. Finally, set $G = H_F = \mathrm{Gal}(K/F)$.

4·1. *A consistent choice of signs*

We now define our signed Selmer group. As we need to compare signed Selmer groups over different extensions, our signs for the Selmer group have to be chosen in a consistent way which we now describe. We shall always fix $\vec{s} = (s_v)_{v \in \Sigma_p^{ss}} \in \{\pm\}^{\Sigma_p^{ss}}$. Let L be an intermediate subextension of F/K. By (S2)-(S3), for each prime u in $\Sigma_p^{ss}(L)$, there is a unique prime of L_n lying above the said prime which, by abuse of notation, is still denoted by u. For each $u \in \Sigma_p^{ss}(L_n)$, we set $s_u = s_v$, where v is a prime of F below u. The $\vec{s}$-signed Selmer groups $\mathrm{Sel}^{\vec{s}}(E/L_n)$ over L_n are then defined by

$$\ker\Bigg(H^1(G_\Sigma(L_n), E[p^\infty]) \longrightarrow \bigoplus_{u \in \Sigma_p^{ord}(L_n)} \frac{H^1(L_{n,u}, E[p^\infty])}{E(L_{n,u}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \times \bigoplus_{u \in \Sigma_p^{ss}(L_n)} \frac{H^1(L_{n,v}, E[p^\infty])}{E^{s_u}(L_{n,u}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}$$

$$\times \bigoplus_{v \in \Sigma_1(L_n)} H^1(L_{n,u}, E[p^\infty]) \Bigg).$$

We set $\mathrm{Sel}^{\vec{s}}(E/L_\infty) = \varinjlim \mathrm{Sel}^{\vec{s}}(E/L_n)$. In particular, we have

$$\mathrm{Sel}^{\vec{s}}(E/L_\infty) = \ker\left(H^1(G_\Sigma(L_\infty), E[p^\infty]) \longrightarrow \bigoplus_{u \in \Sigma_p^{ord}(L_\infty)} \frac{H^1(L_{\infty,u}, E[p^\infty])}{E(L_{\infty,u}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right.$$

$$\left. \times \bigoplus_{u \in \Sigma_p^{ss}(L_\infty)} \frac{H^1(L_{\infty,v}, E[p^\infty])}{E^{s_u}(L_{\infty,u}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \times \bigoplus_{v \in \Sigma_1(L_\infty)} H^1(L_{\infty,u}, E[p^\infty]) \right).$$

To simplify notation, for each $u \in \Sigma(L_\infty)$, we shall write $J_u(E/L_\infty)$ for $\frac{H^1(L_{\infty,u}, E[p^\infty])}{E(L_{\infty,u}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}$, $\frac{H^1(L_{\infty,u}, E[p^\infty])}{E^{s_v}(L_{\infty,u}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}$ or $H^1(L_{\infty,u}, E[p^\infty])$ accordingly to u belonging to $\Sigma_p^{ord}(L_\infty)$, $\Sigma_p^{ss}(L_\infty)$ or $\Sigma_1(L_\infty)$.

By the manner of the choice of signs, we then have a natural map

$$\mathrm{Sel}^{\vec{s}}(E/L_\infty) \longrightarrow \mathrm{Sel}^{\vec{s}}(E/K_\infty)^{H_L}$$

induced by the restriction map on cohomology.

LEMMA 4·1. *The map*

$$\mathrm{Sel}^{\vec{s}}(E/L_\infty) \longrightarrow \mathrm{Sel}^{\vec{s}}(E/K_\infty)^{H_L}$$

is injective with finite cokernel.

Proof. We have the following commutative diagram

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

with exact rows. For $w \in \Sigma_p^{ss}(K_\infty)$, we have $E(K_{\infty,w})[p^\infty] = 0$ by Lemma 3·1, which in turn implies that $E(F_\infty)[p^\infty] = 0$ noting (S2). Combining this observation with a Hochschild–Serre spectral sequence argument, we see that h_L is an isomorphism. For $u \in \Sigma_p^{ss}(L_\infty)$, it follows from Proposition 3·9 and Remark 3·11 that l_u is an isomorphism. Finally, it follows from the proof of [10, lemma 3·3] that $\ker l_u$ is finite for the remaining primes. The assertion of the lemma is now an immediate consequence of these observations.

CONJECTURE. *Write* $X^{\vec{s}}(E/K_\infty)$ *for the Pontryagin dual of* $\mathrm{Sel}^{\vec{s}}(E/K_\infty)$. *Then* $X^{\vec{s}}(E/K_\infty)$ *is a torsion* $\mathbb{Z}_p[[\Gamma]]$-*module, where* $\Gamma = \mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$.

When E has good ordinary reduction at all primes above p, the above conjecture is precisely Mazur's conjecture [26] which is known in the case when E is defined over $\mathbb{Q}$ and F an abelian extension of $\mathbb{Q}$ (see [16]). For an elliptic curve over $\mathbb{Q}$ with good supersingular reduction at p, this conjecture was established by Kobayashi (cf. [21]; also see [3] for some recent progress on this conjecture). We now record an equivalent characterisation of this property.

PROPOSITION 4·2. *The module* $X^{\vec{s}}(E/K_\infty)$ *is* $\mathbb{Z}_p[[\Gamma]]$*-torsion if and only if we have* $H^2(G_S(K_\infty), E[p^\infty]) = 0$ *and the following short exact sequence*

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

Proof. See [**2**, proposition 3·3·1] or [**23**, proposition 2·7].

Remark 4·3. If $\mathrm{Sel}^{\vec{s}}(E/K_\infty)$ is a cotorsion $\mathbb{Z}_p[[\Gamma]]$-module, then so is $\mathrm{Sel}^{\vec{s}}(E/L_\infty)$ for every intermediate subextension L of K/F by Lemma 4·1. Hence Proposition 4·2 also applies to $\mathrm{Sel}^{\vec{s}}(E/L_\infty)$.

We give two more consequences of $X^{\vec{s}}(E/K_\infty)$ being torsion $\mathbb{Z}_p[[\Gamma]]$-module.

PROPOSITION 4·4. *Suppose that* $\mathrm{Sel}^{\vec{s}}(E/K_\infty)$ *is a cotorsion* $\mathbb{Z}_p[[\Gamma]]$*-module. Then the cohomology group* $H^i(H, \mathrm{Sel}^{\vec{s}}(E/K_\infty))$ *is finite for every subgroup H of G and $i \geqslant 1$.*

Proof. As before, we write L for the fixed field of H. In view of Proposition 4·2, we have the following commutative diagram

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

with exact rows, and the bottom row continues as

$$H^1\left(H, \mathrm{Sel}^{\vec{s}}(E/K_\infty)\right) \longrightarrow H^1\left(H, H^1(G_\Sigma(K_\infty), E[p^\infty])\right)$$

$$\longrightarrow H^1\left(H, \bigoplus_{w \in \Sigma(K_\infty)} J_w(E/K_\infty)\right) \longrightarrow \cdots$$

Now consider the spectral sequence

$$H^i(H_L, H^j(G_\Sigma(K_\infty), E[p^\infty])) \Longrightarrow H^{i+j}(G_\Sigma(L_\infty), E[p^\infty]).$$

As seen in the proof of Lemma 4·1, $H^0(G_\Sigma(K_\infty), E[p^\infty]) = 0 = H^0(G_\Sigma(L_\infty), E[p^\infty])$. By Proposition 4·2 and Remark 4·3, we have $H^2(G_\Sigma(K_\infty), E[p^\infty]) = 0 = H^2(G_\Sigma(L_\infty), E[p^\infty])$. Hence the spectral sequence degenerates yielding

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

As seen in the proof of Lemma 4·1, h_L is an isomorphism. For $w \in \Sigma_p^{ss}(K_\infty)$, it follows from Proposition 3·9 and Remark 3·11 that $\mathrm{coker}\, l_u = 0$ and $H^i(H, J_w(E/K_\infty)) = 0$. For the remaining primes, it follows from the discussion in [**10**, section 4] that $\mathrm{coker}\, l_u$ and

$H^i(H, J_w(E/K_\infty))$ are finite. Putting all these observations into the long exact sequence of the bottom row, we obtain the conclusion of the corollary.

PROPOSITION 4·5. *Suppose that* $X^{\vec{s}}(E/K_\infty)$ *is a torsion* $\mathbb{Z}_p[[\Gamma]]$-*module. Then* $X^{\vec{s}}(E/K_\infty)$ *has no nonzero finite* $\mathbb{Z}_p[[\Gamma]]$-*submodules.*

Proof. We follow the approach of [**8**, proposition 4·14] and [**18**, theorem 3·14]. Fix an isomorphism $\kappa : \Gamma \cong 1 + p\mathbb{Z}_p$. For each s, we write $\mathbb{Z}_p(s)$ for the abelian group $\mathbb{Z}_p$ with a Γ-action given by $\gamma \cdot x = \kappa(\gamma)x$. For every Γ-module M, write $M(s) = M \otimes \mathbb{Z}_p(s)$, where Γ acts diagonally. As in [**8**, proposition 4·14] or [**18**, theorem 3·14], one can choose an s such that the twisted Selmer group $\mathrm{Sel}(E/K)(s)$ is finite. Then we have the following commutative diagram

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Sel}(E/K)(s) & \longrightarrow & H^1(G_\Sigma(K), E[p^\infty](s)) & \longrightarrow & \displaystyle\bigoplus_{u \in \Sigma(K)} J_u(E/K)(s) & \longrightarrow & 0 \\
& & \downarrow & & \downarrow{\scriptstyle h'} & & \downarrow{\scriptstyle \oplus g_u} & & \\
0 & \to & \left(\mathrm{Sel}^{\vec{s}}(E/K_\infty)(s)\right)^\Gamma & \to & \left(H^1(G_\Sigma(K_\infty), E[p^\infty])(s)\right)^\Gamma & \to & \left(\displaystyle\bigoplus_{w \in \Sigma(K_\infty)} J_w(E/K_\infty)(s)\right)^\Gamma & \to & \cdots
\end{array}
$$

with exact rows. Here the surjectivity of the rightmost map in the top row follows from the finiteness of $\mathrm{Sel}(E/K)(s)$ by a similar argument to that in [**18**, proposition 3·8]. By a similar argument to that in Proposition 4·4, the map h' is bijective. For $u \in \Sigma_p^{ss}$, the map g_u is given by

$$
g_u : \frac{H^1(K_u, E[p^\infty])}{E(K_u) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \longrightarrow \left(\frac{H^1(K_{\infty,w}, E[p^\infty])}{E^\pm(K_{\infty,w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}\right)^\Gamma .
$$

It follows from [**20**, proposition 3·32] that the term $\left(\frac{H^1(K_{\infty,w}, E[p^\infty])}{E^\pm(K_{\infty,w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}\right)^\Gamma$ is a cofree $\mathbb{Z}_p$-module and hence coker g_u is cofree over $\mathbb{Z}_p$. (Note: the map g_u need not be surjective; see [**1**, section 3].) For each of the remaining primes, the map g_u is surjective, since Γ has p-cohomological dimension one (for instance, see [**8**, proposition 4·14]). Hence it follows that we have an exact sequence

$$
0 \longrightarrow \bigoplus_{u \in \Sigma_p^{ss}(K)} \mathrm{coker}\, g_u \longrightarrow H^1\left(\Gamma, \mathrm{Sel}^{\vec{s}}(E/K_\infty)(s)\right) \longrightarrow H^1\left(\Gamma, H^1(G_\Sigma(K_\infty), E[p^\infty])(s)\right).
$$

Via a similar argument to that in [**1**, lemma 2·5], we see that $H^1(\Gamma, H^1(G_\Sigma(K_\infty), E[p^\infty])(s)) = 0$ using the fact that $\mathrm{Sel}(E/K)(s)$ is finite. Now, it follows from the above exact sequence that $H^1(\Gamma, \mathrm{Sel}^{\vec{s}}(E/K_\infty)(s))$ is a cofree $\mathbb{Z}_p$-module. By [**27**, proposition 5·3·19(i)], this in turn implies that $(\mathrm{Sel}^{\vec{s}}(E/K_\infty)(s))^\vee$ has no nonzero finite Λ-submodule. It then follows from this that $X^{\vec{s}}(E/K_\infty)$ also has no nonzero finite Λ-submodule.

4·2. *Non-primitive signed Selmer groups*

For our purposes, it is useful to work with a non-primitive Selmer group (for instance, see [**9**]). Let Σ_0 be a subset of Σ_1. The non-primitive signed Selmer group (with respect to

Σ_0) is defined by

$$\operatorname{Sel}_{\Sigma_0}^{\vec{s}}(E/L_\infty) = \ker\left(H^1(G_\Sigma(L_\infty), E[p^\infty]) \longrightarrow \bigoplus_{w \in \Sigma(L_\infty) - \Sigma_0(L_\infty)} J_w(E/L_\infty)\right).$$

We shall write $X_{\Sigma_0}^{\vec{s}}(E/L_\infty)$ for the Pontryagin dual of $\operatorname{Sel}_{\Sigma_0}^{\vec{s}}(E/L_\infty)$.

The non-primitive signed Selmer group and the signed Selmer group fit into the following commutative diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & \operatorname{Sel}^{\vec{s}}(E/L_\infty) & \longrightarrow & H^1\big(G_\Sigma(L_\infty), E[p^\infty]\big) & \longrightarrow & \displaystyle\bigoplus_{u \in \Sigma(L_\infty)} J_u(E/L_\infty) \\
& & \downarrow & & \| & & \downarrow \\
0 & \longrightarrow & \operatorname{Sel}_{\Sigma_0}^{\vec{s}}(E/L_\infty) & \longrightarrow & H^1\big(G_\Sigma(L_\infty), E[p^\infty]\big) & \longrightarrow & \displaystyle\bigoplus_{u \in \Sigma(L_\infty) - \Sigma_0(L_\infty)} J_u(E/L_\infty)
\end{array}$$

with exact rows. It then follows from a diagram chasing argument that we have the following exact sequence

$$0 \longrightarrow \operatorname{Sel}^{\vec{s}}(E/L_\infty) \longrightarrow \operatorname{Sel}_{\Sigma_0}^{\vec{s}}(E/L_\infty) \longrightarrow \bigoplus_{u \in \Sigma_0(F_\infty)} H^1(L_{\infty,u}, E[p^\infty]).$$

We now record certain important properties of the non-primitive signed Selmer group.

PROPOSITION 4·6. *Suppose that* $\operatorname{Sel}^{\vec{s}}(E/K_\infty)$ *is a cotorsion* $\mathbb{Z}_p[[\Gamma]]$-*module. Then the following statements are valid.*

(*a*) *There are short exact sequences*

$$0 \longrightarrow \operatorname{Sel}^{\vec{s}}(E/K_\infty) \longrightarrow \operatorname{Sel}_{\Sigma_0}^{\vec{s}}(E/K_\infty) \longrightarrow \bigoplus_{w \in \Sigma_0(K_\infty)} H^1(K_{\infty,w}, E[p^\infty]) \longrightarrow 0$$

and

$$0 \longrightarrow \operatorname{Sel}_{\Sigma_0}^{\vec{s}}(E/K_\infty) \longrightarrow H^1(G_\Sigma(K_\infty), E[p^\infty]) \longrightarrow \bigoplus_{w \in \Sigma(K_\infty) - \Sigma_0(K_\infty)} J_w(E/K_\infty) \longrightarrow 0.$$

(*b*) $\theta(X^{\vec{s}}(E/K_\infty)) = \theta(X_{\Sigma_0}^{\vec{s}}(E/K_\infty))$.

(*c*) *The cohomology groups* $H^i(H, \operatorname{Sel}_{\Sigma_0}^{\vec{s}}(E/K_\infty))$ *are finite for every subgroup* H *of* G *and* $i \geqslant 1$.

(*d*) $X_{\Sigma_0}^{\vec{s}}(E/K_\infty)$ *has no non-trivial finite* Λ-*submodule.*

Proof. The first assertion is immediate from the above diagram and Proposition 4·2. The second follows from a combination of assertion *(a)* and Lemma 2·7, noting that $H^1(K_{\infty,u}, E[p^\infty])$ is cofinitely generated over $\mathbb{Z}_p$ by [**7**, proposition 2]. Assertion *(c)* can either be proven by a similar argument to that in Proposition 4·4, or by taking H-invariant of the first short exact sequence in assertion *(a)* and applying the conclusion of Proposition 4·4.

Finally, we prove Assertion *(d)*. From the first exact sequence in *(a)*, we have

$$H^1\big(\Gamma, \operatorname{Sel}^{\vec{s}}(E/K_\infty)\big) \longrightarrow H^1\big(\Gamma, \operatorname{Sel}_{\Sigma_0}^{\vec{s}}(E/K_\infty)\big) \longrightarrow 0,$$

where the zero on the right is a consequence of the well-known fact that

$$H^1\left(\Gamma, \bigoplus_{w \in \Sigma_0(K_\infty)} H^1(K_{\infty,w}, E[p^\infty])\right) = 0.$$

As seen in the proof of Proposition 4·5, $H^1\left(\Gamma, \mathrm{Sel}^{\vec{s}}(E/K_\infty)\right)$ is cofree over $\mathbb{Z}_p$. Hence so is $H^1\left(\Gamma, \mathrm{Sel}_{\Sigma_0}^{\vec{s}}(E/K_\infty)\right)$. It then follows from [**27**, proposition 5·3·19(i)] that $X_{\Sigma_0}^{\vec{s}}(E/K_\infty)$ has no non-trivial finite Λ-submodule.

4·3. *Projectivity results*

Retain the notation of the previous subsections. Let $v \in \Sigma_p^{ord}$, and w a prime of K lying above v. Write k_w for the residue field of the local field K_w. Following Mazur [**26**], the prime v is said to be anomalous for E/K if $|\widetilde{E}_v(k_w)|$ is divisible by p. Otherwise, we say that v is non-anomalous for E/K. Note that this definition is independent of the choice of w above v.

As in [**9**], we set

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

We can now state and prove our results on the projectivity properties of the signed Selmer groups.

THEOREM 4·7. *Suppose that* $(S1) - (S3)$ *are satisfied and that* Σ_0 *contains* $\Phi_{K/F}$. *Assume that* $X^{\vec{s}}(E/K_\infty)$ *is torsion over* $\mathbb{Z}_p[[\Gamma]]$ *and that* $\theta(X^{\vec{s}}(E/K_\infty)) \leqslant 1$.

Then $X_{\Sigma_0}^{\vec{s}}(E/K_\infty)/X_{\Sigma_0}^{\vec{s}}(E/K_\infty)[p]$ *is quasi-projective as a* $\mathbb{Z}_p[G]$-module. *Furthermore, if* $X^{\vec{s}}(E/K_\infty)$ *is finitely generated over* $\mathbb{Z}_p$, *then* $X_{\Sigma_0}^{\vec{s}}(E/K_\infty)$ *is quasi-projective as a* $\mathbb{Z}_p[G]$-module.

Proof. Let $C = PQ$ be a cyclic subgroup of G and ε a 1-dimensional character of Q. By Proposition 4·6(a), we have a short exact sequence

$$0 \longrightarrow \mathrm{Sel}_{\Sigma_0}^{\vec{s}}(E/K_\infty)^\varepsilon \longrightarrow H^1(G_\Sigma(K_\infty), E[p^\infty])^\varepsilon \longrightarrow \bigoplus_{w \in \Sigma(K_\infty) \setminus \Sigma_0(K_\infty)} J_w(E/K_\infty)^\varepsilon \longrightarrow 0.$$

As seen in the proof of [**9**, proposition 3·2·1], we have

$$h_p\left(H^1(G_\Sigma(K_\infty), E[p^\infty])^\varepsilon\right) = 1$$

and

$$h_p\left(J_w(E/K_\infty)^\varepsilon\right) = 1$$

for $w \in \Sigma^{ord}(K_\infty) \cup (\Sigma_1(K_\infty) \setminus \Sigma_0(K_\infty))$. By Corollary 3·10 (and noting Remark 3·11), the remaining local summands at the supersingular primes also have trivial P-Herbrand quotients. Hence we conclude that

$$h_p\left(\mathrm{Sel}_{\Sigma_0}^{\vec{s}}(E/K_\infty)^\varepsilon\right) = 1.$$

Now combining this with Proposition 4·4, we obtain the first assertion of the theorem. The second assertion of the theorem will follow from an application of Proposition 2·3.

THEOREM 4·8. *Suppose that* $(S1) - (S3)$ *are satisfied and that* Σ_0 *contains* $\Phi_{K/F}$. *Assume that* $\mathrm{Sel}^{\vec{s}}(E/K_\infty)$ *is cotorsion over* $\mathbb{Z}_p[[\Gamma]]$, *and that for each* $v \in \Sigma_p^{ord}$, *either* v *is non-anomalous for* E/K *or* v *is tamely ramified in* K/F. *Then* $X_{\Sigma_0}^{\vec{s}}(E/K_\infty)$ *has a free resolution of length* 1 *as a* $\Lambda[G]$-*module.*

Moreover, if one further assumes that $X^{\vec{s}}(E/K_\infty)$ *is finitely generated over* $\mathbb{Z}_p$, *then* $X_{\Sigma_0}^{\vec{s}}(E/K_\infty)$ *is projective as a* $\mathbb{Z}_p[G]$-*module.*

Proof. We first show that $H^i(H, \mathrm{Sel}_{\Sigma_0}^{\vec{s}}(E/K_\infty)) = 0$ for $i = 1, 2$ and every subgroup H of G. Let L be the fixed field of H. Then we have the following commutative diagram

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Sel}_{\Sigma_0}^{\vec{s}}(E/L_\infty) & \longrightarrow & H^1(G_\Sigma(L_\infty), E[p^\infty]) & \longrightarrow & \displaystyle\bigoplus_{v \in \Sigma(L_\infty) \backslash \Sigma_0(L_\infty)} J_v(E/L_\infty) & \longrightarrow & 0 \\
& & \downarrow & & \downarrow{\scriptstyle h} & & \downarrow{\scriptstyle g = \oplus g_v} & & \\
0 & \longrightarrow & \mathrm{Sel}_{\Sigma_0}^{\vec{s}}(E/K_\infty)^H & \longrightarrow & H^1(G_\Sigma(K_\infty), E[p^\infty])^H & \longrightarrow & \left(\displaystyle\bigoplus_{w \in \Sigma(K_\infty) \backslash \Sigma_0(K_\infty)} J_w(E/K_\infty) \right)^H & &
\end{array}
$$

with exact rows, where we note that the rightmost map on top sequence is surjective by Remark 4·3. As seen in the proof of Proposition 4·4, the map h is an isomorphism and $H^i(H, H^2(G_\Sigma(K_\infty), E[p^\infty])) = 0$ for $i \geq 1$. Hence one can conclude that

$$
H^i\left(H, \mathrm{Sel}_{\Sigma_0}^{\vec{s}}(E/K_\infty)\right) \cong \begin{cases} \mathrm{coker}\, g, & \text{if } i = 1, \\ H^1\left(H, \displaystyle\bigoplus_{w \in \Sigma(K_\infty) \backslash \Sigma_0(K_\infty)} J_w(E/K_\infty)\right), & \text{if } i = 2. \end{cases}
$$

Note that $g = \oplus_v g_v$, where

$$
g_v : J_v(E/L_\infty) \longrightarrow \left(\bigoplus_{w|v} J_w(E/K_\infty) \right)^H .
$$

For good ordinary primes above p and primes above $\Sigma_1 \setminus \Sigma_0$, it was seen in the proof of [**9**, proposition 3·1·1] that $\mathrm{coker}\, g_v = 0$ and

$$
H^1\left(H, \bigoplus_{w|v} J_w(E/K_\infty)\right) = 0.
$$

For the supersingular primes above p, the vanishing follows from Proposition 3·9 and Remark 3·11. In conclusion, one has $H^i(H, \mathrm{Sel}_{\Sigma_0}^{\vec{s}}(E/K_\infty)) = 0$ for $i = 1, 2$. Combining this observation with Propositions 2·14 and 4·6(d), we obtain the first assertion of the theorem.

Now supposing further that $X^{\vec{s}}(E/K_\infty)$ is finitely generated over $\mathbb{Z}_p$. Then, by Proposition 4·6(a) and (d), we have that $X_{\Sigma_0}^{\vec{s}}(E/K_\infty)$ is finitely generated and free over $\mathbb{Z}_p$. Combining this with the above established fact that $H^i(H, \mathrm{Sel}_{\Sigma_0}^{\vec{s}}(E/K_\infty)) = 0$ for $i = 1$ and $i = 2$, the second assertion then follows from Proposition 2·1.

5. *Applications of Theorems* 4·7 *and* 4·8

In this section, we discuss some applications of Theorems 4·7 and 4·8.

5·1. *Kida formula for signed Selmer groups*

As a start, we shall prove the Kida formula for our signed Selmer groups. Recall that

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

LEMMA 5·1. *Suppose that K/F is a finite Galois p-extension. For each $v \in \Phi_{K/F}$, we have $\mu_p \subseteq F_v$ and $\mu_p \subseteq K_w$ for every prime w of K above v.*

Proof. Let w be a prime of K above v, and u a prime of K_∞ above w (and hence above v). Write x for the prime of F_∞ below u. By the assumption $v \in \Phi$, it follows that K_w/F_v is ramified. As v does not divide p, the field $F_{\infty,x}$ is a unramified $\mathbb{Z}_p$-extension of F_v. Therefore, we have $K_w \nsubseteq F_{\infty,x}$. Recall that by [27, proposition 7·5·9], if a local field with residue characteristic $\neq p$ does not contain μ_p, then its the maximal pro-p extension is a $\mathbb{Z}_p$-extension. But from the above discussion, we have seen that $K_{\infty,u}$ is an extension of F_v with Galois group (slightly) bigger than $\mathbb{Z}_p$. Hence we must have $\mu_p \subseteq F_v$.

We can now prove the Kida's formula for the signed Selmer groups (compared with [9–12, 30]). Recall that we write $\lambda(M)$ for the λ-invariant of a torsion Λ-module M and that our conclusion is more in line with that in [11].

PROPOSITION 5·2. *Suppose that $p \geqslant 5$, that $(S1) - (S3)$ are satisfied and that K/F is a finite Galois p-extension. Furthermore, assume that $X^{\vec{s}}(E/K_\infty)$ is torsion over Λ with $\theta\left(X^{\vec{s}}(E/K_\infty)\right) \leqslant 1$. Then we have*

$$\lambda\left(\mathrm{Sel}^{\vec{s}}(E/K_\infty)\right) = |K : F| \cdot \lambda\left(\mathrm{Sel}^{\vec{s}}(E/F_\infty)\right) + \sum_{w \in P_1}(e_w - 1) + 2\sum_{w \in P_2}(e_w - 1),$$

where P_1 is the set of primes in $\Phi(K_\infty)$ at which E has split multiplicative reduction, P_2 is the set of primes in $\Phi(K_\infty)$ at which E has good reduction with $E(K_{\infty,v})[p] \neq 0$, and e_w is the ramification index of w in K_∞/F_∞.

Proof. Set $\Sigma_0 = \Phi_{K/F}$. By Theorem 4·7, the $\mathbb{Z}_p[G]$-module $X_{\Sigma_0}^{\vec{s}}(E/K_\infty)/X_{\Sigma_0}^{\vec{s}}(E/K_\infty)[p]$ is quasi-projective. It then follows from Corollary 2·9 that

$$\lambda\left(\mathrm{Sel}_{\Sigma_0}^{\vec{s}}(E/K_\infty)\right) = |K : F| \cdot \lambda\left(\mathrm{Sel}_{\Sigma_0}^{\vec{s}}(E/K_\infty)^G\right) = |K : F|\lambda\left(\mathrm{Sel}_{\Sigma_0}^{\vec{s}}(E/F_\infty)\right),$$

where the second equality follows from Lemma 4·1. Now, taking Proposition 4·6*(a)* into account, we have

$$\lambda\left(\mathrm{Sel}^{\vec{s}}(E/K_\infty)\right) = |K : F| \cdot \lambda\left(\mathrm{Sel}^{\vec{s}}(E/F_\infty)\right) + |K : F| \sum_{v \in \Phi_{K/F}(F_\infty)} \mathrm{corank}_{\mathbb{Z}_p}\left(H^1(F_{\infty,v}, E[p^\infty])\right)$$

$$- \sum_{w \in \Phi_{K/F}(K_\infty)} \mathrm{corank}_{\mathbb{Z}_p}\left(H^1(K_{\infty,w}, E[p^\infty])\right).$$

Denote by Q_1 the set of primes in $\Phi_{K/F}(F_\infty)$ at which E has split multiplicative reduction, and denote by Q_2 the set of primes in $\Phi_{K/F}(F_\infty)$ at which E has good reduction with

$E(F_{\infty,v})[p] \neq 0$. Taking our assumption that $p \geqslant 5$ into account, it is straightforward to verify that $Q_i(K_\infty) = P_i$ for $i = 1, 2$. Now, by a combination of [**7**, proposition 2] and [**10**, proposition 5·1], we see that

$$\mathrm{corank}_{\mathbb{Z}_p}\Big(H^1(F_{\infty,v}, E[p^\infty])\Big) = \begin{cases} 1, & \text{if } v \in Q_1, \\ 2, & \text{if } v \in Q_2, \\ 0, & \text{if } v \in \Sigma_0(F_\infty) - Q_1 \cup Q_2 \end{cases}$$

and

$$\mathrm{corank}_{\mathbb{Z}_p}\Big(H^1(K_{\infty,w}, E[p^\infty])\Big) = \begin{cases} 1, & \text{if } w \in P_1, \\ 2, & \text{if } w \in P_2, \\ 0, & \text{if } w \in \Sigma_0(K_\infty) - P_1 \cup P_2, \end{cases}$$

where we note that to apply the results of Hachimori–Matsuno [**10**, proposition 5·1], one requires the corresponding local fields to contain μ_p which is guaranteed by our Lemma 5·1. Therefore, we obtain

$$\lambda\Big(\mathrm{Sel}^{\vec{s}}(E/K_\infty)\Big) = |K:F| \cdot \lambda\Big(\mathrm{Sel}^{\vec{s}}(E/F_\infty)\Big) + |K:F| \sum_{v \in Q_1} 1 + |K:F| \sum_{v \in Q_2} 2$$
$$- \sum_{w \in P_1} 1 - \sum_{w \in P_2} 2.$$

Since the set of primes of K_∞ above Q_i is precisely P_i as noted above, we have

$$|K:F| \sum_{v \in Q_i} 1 = \sum_{v \in Q_i} \sum_{w|v} e_w = \sum_{w \in P_i} e_w$$

for $i = 1, 2$. Putting this back into the above equation, we obtain the equality of the theorem.

Remark 5·3. Retaining the hypothesis of Theorem 5·2 and assuming further that $\mathrm{Sel}^{\vec{s}}(E/F_\infty)$ is cofinitely generated over $\mathbb{Z}_p$, it then follows from Lemma 4·1 that $\mathrm{Sel}^{\vec{s}}(E/K_\infty)^G$ is cofinitely generated over $\mathbb{Z}_p$. Since G is a finite p-group, Nakayama lemma tells us that $\mathrm{Sel}^{\vec{s}}(E/K_\infty)$ is cofinitely generated over $\mathbb{Z}_p[G]$, and hence over $\mathbb{Z}_p$. In this context, Theorem 4·7 yields

$$\mathrm{corank}_{\mathbb{Z}_p}\Big(\mathrm{Sel}^{\vec{s}}(E/K_\infty)\Big) = |K:F|\mathrm{corank}_{\mathbb{Z}_p}\Big(\mathrm{Sel}^{\vec{s}}(E/F_\infty)\Big) + \sum_{w \in P_1}(e_w - 1) + 2\sum_{w \in P_2}(e_w - 1),$$

which is the usual Kida's formula under the $\mu = 0$ setting (see [**9**, **10**, **12**, **30**]).

5·2. *Characteristic elements of non-primitive signed Selmer groups*

We retain notation from Subsection 2·3 and Section 4. Now if $\mathrm{Sel}^{\vec{s}}(E/K_\infty)$ is cotorsion over $\mathbb{Z}_p[[\Gamma]]$, we can then attach characteristic elements to $X^{\vec{s}}(E/K_\infty)$ and $X_{\Sigma_0}^{\vec{s}}(E/K_\infty)$. We shall write ξ_E (resp., ξ_{E,Σ_0}) for a characteristic element of $X^{\vec{s}}(E/K_\infty)$ (resp., $X_{\Sigma_0}^{\vec{s}}(E/K_\infty)$). Recall that these characteristic elements live in the relative K-group $K_0(\Lambda[G], Q_\Lambda[G])$. It has been conjectured that these elements are related to a (conjectural) p-adic L-function in a precise manner (see [**4**, **22**, **28**]). These p-adic L-functions are believed to satisfy certain integrality properties. Therefore, in view of these

conjectures, one would expect that the characteristic elements satisfy certain integrality properties in an appropriate sense. Motivated by this, our result is as follows (compare with [**28**, theorem 1]).

PROPOSITION 5·4. *Suppose that* $(S1) - (S3)$ *are satisfied and that* Σ_0 *contains* Φ. *Assume that* $\mathrm{Sel}^{\overrightarrow{s}}(E/K_\infty)$ *is cotorsion over* $\mathbb{Z}_p[[\Gamma]]$ *and that for each* $v \in \Sigma_p^{ord}$, *the prime* v *is either non-anomalous for* E/K *or tamely ramified in* K/F. *Then* ξ_{E,Σ_0} *belongs to the image of the following natural map*

$$M_{\Lambda[G]} \cap Q_\Lambda[G]^\times \longrightarrow K_1(Q_\Lambda[G]).$$

Proof. This follows from a combination of Proposition 2·13 and Theorem 4·8.

It is natural to ask whether we can obtain a similar conclusion for ξ_E. Of course, if G is a group of order coprime to p, then we clearly have the conclusion. Therefore, we shall only concern ourselves with the situation when p divides $|G|$. Unfortunately, at this point of writing, we do not have a complete answer to this. But we shall describe a situation, where one can prove such an integrality property. Recall from Theorem 5·2, P_1 is the set of primes in $\Phi_{K/F}(K_\infty)$ at which E has split multiplicative reduction, and P_2 is the set of primes w in $\Phi_{K/F}(K_\infty)$ at which E has good reduction with $E(K_{\infty,w})[p] \neq 0$.

PROPOSITION 5·5. *Retain the settings of Theorem* 5·4. *Suppose further that the sets* P_1 *and* P_2 *are empty. Then* ξ_E *belongs to the image of the following natural map*

$$M_{\Lambda[G]} \cap Q_\Lambda[G]^\times \longrightarrow K_1(Q_\Lambda[G]).$$

Proof. Set $\Sigma_0 = \Phi_{K/F}$. By Proposition 4·6(b), we have the following short exact sequence

$$0 \longrightarrow \mathrm{Sel}^{\overrightarrow{s}}(E/K_\infty) \longrightarrow \mathrm{Sel}_{\Sigma_0}^{\overrightarrow{s}}(E/K_\infty) \longrightarrow \bigoplus_{w \in \Sigma_0(K_\infty)} H^1(K_{\infty,w}, E[p^\infty]) \longrightarrow 0.$$

Since the sets P_1 and P_2 are empty, it follows from the proof of Theorem 5·2 that $H^1(K_{\infty,w}, E[p^\infty])$ are finite for $w \in \Sigma_0(K_\infty)$. Thus, the classes of $X^{\overrightarrow{s}}(E/K_\infty)$ and $X_{\Sigma_0}^{\overrightarrow{s}}(E/K_\infty)$ agree in $K_0(\Lambda[G], Q_\Lambda[G])$, and so they share the same characteristic elements. The conclusion of the proposition now follows from Theorem 5·4.

REFERENCES

[1] S. AHMED and M. F. LIM. On the Euler characteristics of signed Selmer groups. *Bull. Aust. Math. Soc.* **101** (2020), no. 2, 238–246.

[2] S. AHMED and M. F. LIM. On the signed Selmer groups of congruent elliptic curves with semistable reduction at all primes above *p*. *Acta Arithmetica* **197** (2021), no. 4, 353–377.

[3] K. BÜYÜKBODUK and A. LEI. Integral Iwasawa theory of Galois representations for non-ordinary primes. *Math. Z.* **286** (2017), no. 1–2, 361–398.

[4] J. COATES, T. FUKAYA, K. KATO, R. SUJATHA and O. VENJAKOB. The GL_2 main conjecture for elliptic curves without complex multiplication. *Publ. Math. Inst. Hautes Études Sci*. No. 101, (2005), 163-208.

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

[6] N. ELLERBROCK and A. NICKEL. On formal groups and Tate cohomology in local fields. *Acta Arith.* **182** (2018), no. 3, 285–299.

[7] R. GREENBERG. Iwasawa theory for p-adic representations, in: Algebraic number theory, 97–137. *Adv. Stud. Pure Math.,* **17** (Academic Press, Boston, MA, 1989).

[8] R. GREENBERG. Iwasawa theory for elliptic curves, in: Arithmetic theory of elliptic curves (Cetraro, 1997), 51–144, Lecture Notes in Math., 1716 (Springer, Berlin, 1999).

[9] R. GREENBERG. Iwasawa theory, projective modules and modular representations. *Mem. Amer. Math. Soc.* **211** (2011), no. 992, vi+185 pp.

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

[11] Y. HACHIMORI and R. SHARIFI. On the failure of pseudo-nullity of Iwasawa modules. *J. Algebraic Geom.* **14** (2005), no. 3, 567–591.

[12] J. HATLEY and A. LEI. Arithmetic properties of signed Selmer groups at non-ordinary primes. *Ann. Inst. Fourier (Grenoble)* **69** (2019), no. 3, 1259–1294.

[13] K. IWASAWA. Riemann–Hurwitz formula and p-adic Galois representations for number fields. *Tohoku Math. J.* (2) **33** (1981), no. 2, 263–288.

[14] M. KAKDE. Proof of the main conjecture of noncommutative Iwasawa theory for totally real number fields in certain cases. *J. Algebraic Geom.* **20** (2011), no. 4, 631–683.

[15] M. KAKDE. The main conjecture of Iwasawa theory for totally real fields. *Invent. Math.* **193** (2013), no. 3, 539–626.

[16] K. KATO. p-adic Hodge theory and values of zeta functions of modular forms, in: Cohomologies p-adiques et applications arithmétiques. III. *Astérisque* **295** (2004), ix, pp. 117–290.

[17] B. D. KIM. The parity conjecture for elliptic curves at supersingular reduction primes. *Compos. Math.* **143** (2007), no. 1, 47–72.

[18] B. D. KIM. The plus/minus Selmer groups for supersingular primes. *J. Aust. Math. Soc.* **95** (2) (2013) 189–200.

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

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

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

[22] A. LEI. Non-commutative p-adic L-functions for supersingular primes. *Int. J. Number Theory* **8** (2012), no. 8, 1813–1830

[23] A. LEI and M. F. LIM. Mordell–Weil ranks and Tate–Shafarevich groups of elliptic curves with mixed-reduction type over cyclotomic extensions, arXiv:1911.10643 [math.NT].

[24] A. LEI and M. F. LIM. Akashi series and Euler characteristics of signed Selmer groups of elliptic curves with semistable reduction at primes above p, accepted for publication in *J. Theor. Nombres Bordeaux*.

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

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

[27] J. NEUKIRCH A. SCHMIDT and K. WINGBERG. *Cohomology of Number Fields,* 2nd edn., Grundlehren Math. Wiss. 323 (Springer-Verlag, Berlin, 2008).

[28] A. NICHIFOR and B. PALVANNAN. On free resolutions of Iwasawa modules. *Doc. Math.* **24** (2019), 609–662.

[29] E. NOETHER. Normalbasis bei Körpern ohne höhere Verzweigung. *J. Reine Angew. Math.* **167** (1932), 147–152.

[30] R. POLLACK and T. WESTON. Kida's formula and congruences. *Doc. Math.* (2006), Extra Vol., 615–630.

[31] I. REINER. Maximal orders. Corrected reprint of the 1975 original. With a foreword by M. J. Taylor. London Math. Soc. Monog. New Series, 28 (The Clarendon Press, Oxford University Press, Oxford, 2003), xiv+395 pp.

[32] M. WITTE. On a localisation sequence for the K-theory of skew power series rings. *J. K-Theory* **11** (2013), no. 1, 125–154.