C.-H. Kim and M. Kurihara (2019) “On the Refined Conjectures on Fitting Ideals of Selmer Groups of Elliptic Curves with Supersingular Reduction,”
International Mathematics Research Notices, Vol. 00, No. 0, pp. 1–41
doi:10.1093/imrn/rnz129

# On the Refined Conjectures on Fitting Ideals of Selmer Groups of Elliptic Curves with Supersingular Reduction

**Chan-Ho Kim[1,*] and Masato Kurihara[2]**

[1]School of Mathematics, Korea Institute for Advanced Study (KIAS), 85 Hoegiro, Dongdaemun-gu, Seoul 02455, Republic of Korea and [2]Department of Mathematics, Faculty of Science and Technology, Keio University, 3-14-1 Hiyoshi, Kohoku-ku, Yokohama, 223-8522, Japan

[*]*Correspondence to be sent to: e-mail: chanho.math@gmail.com*

In this paper, we study the Fitting ideals of Selmer groups over finite subextensions in the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ of an elliptic curve over $\mathbb{Q}$. Especially, we present a proof of the “weak main conjecture” à la Mazur and Tate for elliptic curves with good (supersingular) reduction at an odd prime $p$. We also prove the “strong main conjecture” suggested by the second named author under the validity of the $\pm$-main conjecture and the vanishing of a certain error term. The key idea is the explicit comparison among “finite layer objects”, “$\pm$-objects”, and “fine objects” in Iwasawa theory. The case of good ordinary reduction is also treated.

## 1 Introduction

### 1.1 Overview

The main aim of this paper is to understand Selmer groups of an elliptic curve with supersingular reduction at $p$ over finite subextensions in the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ by using $\pm$-Iwasawa theory à la Kobayashi–Pollack. Let $E$ be an elliptic curve over $\mathbb{Q}$ with good reduction at an odd prime $p$. We assume that $a_p(E) \not\equiv 1 \pmod{p}$ throughout this article.

Received April 5, 2018; Revised December 13, 2018; Accepted March 21, 2019

The ±-Iwasawa theory is developed to understand Iwasawa theory for elliptic curves at supersingular primes (with assumption $a_p(E) = 0$). In the supersingular setting, the usual Selmer groups over $\mathbb{Z}_p$-extensions and $p$-adic $L$-functions do not behave well as in the classical framework of Iwasawa theory. Introducing ±-Selmer groups and ±-$p$-adic $L$-functions, Kobayashi [12] and Pollack [25] could apply the standard techniques of Iwasawa theory of elliptic curves with ordinary reduction to the supersingular setting.

On the other hand, Mazur–Tate conjectures [20] and the refined Iwasawa theory à la the second named author ([13], [14], and [15]) focus on understanding Iwasawa theory over finite abelian extensions over $\mathbb{Q}$.

In general, the refined Iwasawa theory (at finite layers) is regarded as a more delicate subject than the usual Iwasawa theory (at the infinite layer) since neither we can directly apply the theory of Iwasawa modules to finite layer objects nor we can ignore "finite errors". It is well known that the structure of group rings at finite layers is much more complicated than that of the Iwasawa algebra.

In this article, we consider the subextensions in the cyclotomic $\mathbb{Z}_p$-extension whose Galois group is cyclic of $p$-power order and only one prime ramifies. Thus, this case can be regarded as the simplest one, but the full understanding of the following conjectures is still deep. Their precise formulations are given in Section 1.2.

**Conjecture 1.1** (Mazur–Tate's weak main conjecture, Conjecture 1.4). Assume that $E$ has no rational $p$-torsion. Then the Mazur–Tate element of $E$ at a finite layer is contained in the Fitting ideal of the dual Selmer group of $E$ over the finite extension.

**Conjecture 1.2** (The strong main conjecture, Conjecture 1.6). Assume that $E$ has no rational $p$-torsion and $p$ does not divide the Tamagawa number of $E$. Then the Mazur–Tate element of $E$ at a finite layer and the traces of the Mazur–Tate elements of $E$ at all the lower layers generate the Fitting ideal of the dual Selmer group of $E$ over the finite extension.

In the case of good ordinary reduction with non-anomalous prime $p$ (i.e., $a_p(E) \not\equiv 1 \pmod{p}$), both conjectures follow from several standard ingredients in Iwasawa theory, including the Iwasawa main conjecture, the non-existence of proper $\Lambda$-submodules of finite index in the Selmer groups over the Iwasawa algebra $\Lambda$, and the control theorem. Although this case is more or less well known to experts, the argument is not explicitly written in the literature. Thus, we give a proof for the case of good ordinary reduction in Section 2. We note that in this case the Fitting ideal of the Selmer group is principal.

In the case of good supersingular reduction, the situation becomes much more complicated. Actually, the Fitting ideal of the Selmer group is never principal in this case. Very fortunately, we are able to strengthen the argument of the good ordinary reduction case by making an explicit comparison between Selmer groups and ±-Selmer groups in finite layers. This approach allows us to obtain the weak main conjecture. The proof is given in Section 4. We obtain Theorem 1.14 in this way.

Concerning the strong main conjecture, we prove it in Theorem 1.20 under certain assumptions including the validity of the ±-main conjecture. We also provide many examples that satisfy these assumptions in Example 1.21, so we have many examples for which the strong main conjecture holds. Especially, if the fine Selmer group over the $\mathbb{Z}_p$-extension is "all Mordell-Weil" described in Example 1.21, then we can prove the strong main conjecture. More generally, even without the assumptions imposed in Theorem 1.20, we are able to prove a slightly weaker version of the strong main conjecture in Theorem 1.18. In the weaker version, the statement involves an error term.

In the proof of Theorem 1.18, we make an explicit comparison between Selmer groups and fine Selmer groups in finite layers. This comparison is related to the finite layer version of the construction of algebraic $p$-adic $L$-functions à la Perrin-Riou. See [27, 2.4.3 Proposition] and [28, §3.1] for example. The error term in Theorem 1.18 occurs in this finite layer comparison. Indeed, the assumptions in Theorem 1.20 are strong enough to force the error term to vanish. As a result, we deduce a "lower bound" of Selmer groups over finite extensions from the Iwasawa main conjecture and some Fitting ideal techniques described in Appendix A. The proof of Theorem 1.18 is given in Section 5, and the proof of Theorem 1.20 is given in Section 6.

It seems that our approach does not work directly if $p \mid a_p(E)$ but $a_p(E) \neq 0$ since the $\sharp/\flat$-Iwasawa theory à la Sprung [33] does not behave well in finite layers. See [33, Open Problem 7.22] for details.

In the rest of this section, we introduce various conjectures we are interested in and state our main results and their applications. In Section 2, we review the case for elliptic curves with good ordinary reduction and give a proof of the weak and strong main conjectures for this case in Theorem 1.14. In Section 3, we review relevant ±-Iwasawa theory for elliptic curves. In Section 4, we prove the weak main conjecture for elliptic curves with supersingular reduction in Theorem 1.14. In Section 5, we prove the slightly weaker version of the strong main conjecture for elliptic curves in Theorem 1.18. In Section 6, we prove the strong main conjecture for elliptic curves under certain assumptions in Theorem 1.20. In Appendix A, we study refined techniques on Fitting ideals.

## 1.2 Conjectures

We recall various conjectures on the arithmetic of elliptic curves.

### 1.2.1 *Birch and Swinnerton-Dyer conjecture*

One of the leading problems of modern number theory is the following conjecture.

**Conjecture 1.3** (Birch and Swinnerton-Dyer). Let $E$ be an elliptic curve over $\mathbb{Q}$. Then

$$\mathrm{rk}_{\mathbb{Z}} E(\mathbb{Q}) = \mathrm{ord}_{s=1} L(E,s).$$

We recall the formulation of the refinements and variants of Conjecture 1.3.

### 1.2.2 *Setting the stage*

Let $p$ be an odd prime. Fix embeddings $\iota_p : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ and $\iota_\infty : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. Let $E$ be an elliptic curve over $\mathbb{Q}$ of conductor $N$ with $(N,p) = 1$. Let

$$\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_{\mathbb{F}_p}(E[p]) \simeq \mathrm{GL}_2(\mathbb{F}_p)$$

be the mod $p$ representation arising from the $p$-torsion points on $E$. For a prime $\ell$ dividing $N$, let $E_0(\mathbb{Q}_\ell)$ be the preimage of the nonsingular locus of $\widetilde{E}(\mathbb{F}_\ell)$. Then the **Tamagawa number of** $E$ is defined by $\mathrm{Tam}(E) := \prod_{\ell \mid N} c_\ell$, where $c_\ell = [E(\mathbb{Q}_\ell) : E_0(\mathbb{Q}_\ell)]$.

Let $n \geq 1$ be an integer and $\mathbb{Q}_n$ the subextension of $\mathbb{Q}$ in $\mathbb{Q}(\mu_{p^{n+1}})$ with $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \simeq \mathbb{Z}/p^n\mathbb{Z}$. Let $\mathbb{Q}_\infty = \bigcup_{n \geq 1} \mathbb{Q}_n$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. Let $\Gamma_n := \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}_n)$ and $\Gamma := \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$. Let $\Lambda_n := \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})] = \mathbb{Z}_p[\Gamma/\Gamma_n]$ and $\Lambda := \varprojlim_n \Lambda_n = \mathbb{Z}_p[\![\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]\!] = \mathbb{Z}_p[\![\Gamma]\!]$. Let $\omega_n = \omega_n(X) := (1+X)^{p^n} - 1$. Fix a generator $\gamma$ of $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ and take a generator $\gamma_n$ of $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ as the image of $\gamma$. Then we have isomorphisms

$$\Lambda_n \simeq \mathbb{Z}_p[X]/\left(\omega_n(X)\right), \qquad \Lambda \simeq \mathbb{Z}_p[\![X]\!]$$

by sending the generators to $1+X$. Via the latter isomorphism, we also regard $\omega_n \in \Lambda$.

Let $\Phi_n(1+X) = \omega_n/\omega_{n-1}$, where $\Phi_n$ is the $p^n$-th cyclotomic polynomial. Let $\omega_0^{\pm}(X) := X$, $\widetilde{\omega}_0^{\pm}(X) := 1$, and

$$\omega_n^+ = \omega_n^+(X) := X \cdot \prod_{2 \le m \le n, m\text{: even}} \Phi_m(1+X), \qquad \omega_n^- = \omega_n^-(X) := X \cdot \prod_{1 \le m \le n, m\text{: odd}} \Phi_m(1+X),$$
$$\widetilde{\omega}_n^+ = \widetilde{\omega}_n^+(X) := \prod_{2 \le m \le n, m\text{: even}} \Phi_m(1+X), \qquad \widetilde{\omega}_n^- = \widetilde{\omega}_n^-(X) := \prod_{1 \le m \le n, m\text{: odd}} \Phi_m(1+X).$$

Then we have $\omega_n(X) = \omega_n^{\pm}(X) \cdot \widetilde{\omega}_n^{\mp}(X)$, respectively. We also regard $\omega_n^{\pm}$, $\widetilde{\omega}_n^{\pm}$ as elements in $\Lambda_n$ or $\Lambda$ via fixed isomorphisms. Also, we identify $\Lambda_n = \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})] \simeq \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}_{n,p}/\mathbb{Q}_p)]$ if necessary. Here, $\mathbb{Q}_{n,p}$ is the completion of $\mathbb{Q}_n$ at the prime above $p$.

Let $f \in S_2(\Gamma_0(N))$ be the newform attached to $E$ by [2, Theorem A]. Let $G'_{n+1} := \mathrm{Gal}(\mathbb{Q}(\mu_{p^{n+1}})/\mathbb{Q})/\{\pm 1\} \simeq \left(\mathbb{Z}/p^{n+1}\mathbb{Z}\right)^{\times}/\{\pm 1\}$ and denote by $\sigma_a$ the element corresponding to $a \in \left(\mathbb{Z}/p^{n+1}\mathbb{Z}\right)^{\times}/\{\pm 1\}$. We define

$$\theta'_{n+1}(f) := \sum_{a \in (\mathbb{Z}/p^{n+1}\mathbb{Z})^{\times}/\{\pm 1\}} \left[\frac{a}{p^{n+1}}\right]^+ \cdot \sigma_a \in \mathbb{Z}_p\left[G'_{n+1}\right].$$

Here, $\left[\frac{a}{b}\right]^+$ is defined by

$$2\pi \int_0^{\infty} f\left(\frac{a}{b} + iy\right) \mathrm{d}y = \left[\frac{a}{b}\right]^+ \cdot \Omega_E^+ + \left[\frac{a}{b}\right]^- \cdot \Omega_E^-,$$

where $\Omega_E^{\pm}$ are the Néron periods of $E$. We write $\Omega_E = \Omega_E^+$. The **Mazur–Tate element $\theta_n(f)$ of $f$ at $\mathbb{Q}_n$** is defined by the image of $\theta'_{n+1}(f)$ in $\Lambda_n$. For simplicity, we assume that $\overline{\rho}$ is irreducible, and then we do not have to care about the integrality of Mazur–Tate elements and the Manin constant issue. See [13, page 200–201].

We also define

$$\widetilde{\delta}_n := \sum_{a \in (\mathbb{Z}/n\mathbb{Z})^{\times}} \left( \overline{\left[\frac{a}{n}\right]^+} \cdot \prod_{\ell \mid n} \overline{\log_{\mathbb{F}_\ell}(a)} \right) \in \mathbb{F}_p,$$

where $n$ is the square-free product of Kolyvagin primes, $\overline{\left[\frac{a}{n}\right]^+}$ is the mod $p$ reduction of $\left[\frac{a}{n}\right]^+$, and $\overline{\log_{\mathbb{F}_\ell}(a)}$ is the mod $p$ reduction of the discrete logarithm of $a$ modulo $\ell$ (with a fixed primitive root modulo $\ell$, indeed). Here, a prime $\ell$ is a Kolyvagin prime if $(\ell, Np) = 1$, $\ell \equiv 1 \pmod{p}$, and $a_\ell(E) \equiv \ell + 1 \pmod{p}$. These $\widetilde{\delta}_n$'s were used to study the structure of Selmer groups in [16]. In addition, the non-vanishing of $\widetilde{\delta}_n$ for some $n$

implies the Iwasawa main conjecture for elliptic curves with any type of good reduction ([10, Theorem 1.1]).

Let $\Sigma$ be a finite set of places of $\mathbb{Q}$ including $p$, $\infty$, and the bad reduction primes of $E$, and $\mathbb{Q}_\Sigma$ be the maximal extension of $\mathbb{Q}$ unramified outside $\Sigma$. We define the **Selmer group of $E$ over $\mathbb{Q}_n$** by

$$\mathrm{Sel}(\mathbb{Q}_n, E[p^\infty]) := \ker\left(\mathrm{H}^1\left(\mathbb{Q}_\Sigma/\mathbb{Q}_n, E[p^\infty]\right) \to \prod_v \frac{\mathrm{H}^1\left(\mathbb{Q}_{n,v}, E[p^\infty]\right)}{E(\mathbb{Q}_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}\right),$$

where $\mathrm{H}^1(\mathbb{Q}_\Sigma/\mathbb{Q}_n, E[p^\infty]) := \mathrm{H}^1(\mathrm{Gal}(\mathbb{Q}_\Sigma/\mathbb{Q}_n), E[p^\infty])$ is the Galois cohomology group, $v$ runs over all the (finite) places of $\mathbb{Q}_n$ dividing the places in $\Sigma$, and $\mathbb{Q}_{n,v}$ is the completion of $\mathbb{Q}_n$ at $v$. We also define the **Selmer group of $E$ over $\mathbb{Q}_\infty$** by

$$\mathrm{Sel}\left(\mathbb{Q}_\infty, E[p^\infty]\right) := \varinjlim_n \mathrm{Sel}\left(\mathbb{Q}_n, E[p^\infty]\right).$$

It is well known that these Selmer groups are independent of the choice of $\Sigma$ ([22, Corollary I.6.6]).

We recall the notion of Fitting ideals for the convenience of readers. For a ring $R$ and a finitely presented $R$-module $M$, take a presentation

$$\begin{tikzcd} R^s \arrow[r, "h"] & R^r \arrow[r] & M \arrow[r] & 0 \end{tikzcd}$$

where $h \in \mathrm{M}_{r\times s}(R)$. Then the **Fitting ideal** $\mathrm{Fitt}_R(M)$ **of $M$ over $R$** is defined to be the ideal of $R$ generated by the determinants of the $r \times r$-minors of the matrix $h$. It is well known that the Fitting ideal is independent of the choice of a presentation of $M$.

For a $\mathbb{Z}_p$-module $M$, let $M^\vee := \mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p)$.

### 1.2.3 *Mazur–Tate's refined conjecture*

In [20], Mazur and Tate gave the following conjecture, which implies Conjecture 1.15. Conjecture 1.15 is a refinement of the Birch and Swinnerton-Dyer conjecture (Conjecture 1.3) in some sense. As we said in Section 1.1, $a_p(E) \not\equiv 1 \pmod{p}$ is always assumed.

**Conjecture 1.4** ([20, Conjecture 3, "weak main conjecture"]).

$$\theta_n(f) \in \mathrm{Fitt}_{\Lambda_n}\left(\mathrm{Sel}(\mathbb{Q}_n, E[p^\infty])^\vee\right).$$

**Remark 1.5.** Note that the original statement covers general abelian extensions of $\mathbb{Q}$ as we mentioned in Section 1.1. There are other approaches towards Conjecture 1.4 due to Bley–Macias Castillo [1, Theorem 2.12] assuming the $p$-part of the relevant equivariant Tamagawa number conjecture, Emerton–Pollack–Weston [3] using the $p$-adic local Langlands correspondence as well as Kato's zeta elements and Popescu using the theory of 1-motives. We are informed that T. Kataoka proved the weak main conjecture over more general abelian extensions under certain assumptions by developing equivariant ±-Iwasawa theory for elliptic curves and by adapting our strategy in his Ph.D. thesis.

### 1.2.4 *The (refined)$^2$ conjecture*

Comparing with Conjecture 1.4, the second named author proposed the following more refined conjecture, which we call the "strong main conjecture". (cf. [20, Remark after Conjecture 3].) This conjecture can be regarded as a refinement of the Iwasawa main conjecture. As we said in Section 1.1, $a_p(E) \not\equiv 1 \pmod{p}$ is always assumed.

**Conjecture 1.6** ([13, Conjecture 0.3, "strong main conjecture"]). Let $E$ be an elliptic curve over $\mathbb{Q}$ with good reduction at an odd prime $p$. If $E(\mathbb{Q})[p]$ is trivial and $p \nmid \mathrm{Tam}(E)$, then

$$\left(\theta_n(f), \nu_{n-1,n}\left(\theta_{n-1}(f)\right)\right) = \mathrm{Fitt}_{\Lambda_n}\left(\mathrm{Sel}(\mathbb{Q}_n, E[p^\infty])^\vee\right).$$

Here, $\nu_{n-1,n}$ is the trace map $\Lambda_{n-1} \to \Lambda_n$ defined by $\sigma \mapsto \sum_{\tau\mapsto\sigma} \tau$ for $\sigma \in \mathrm{Gal}(\mathbb{Q}_{n-1}/\mathbb{Q})$, where $\tau$ runs over all elements of $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ projecting to $\sigma$.

**Remark 1.7.** This conjecture explains the growth of $\mathrm{Sel}(\mathbb{Q}_n, E[p^\infty])$ as $n$ goes to infinity.

The second named author proved Conjecture 1.6 for the "most basic" case (cf. [6, §5]) using Kato's zeta elements.

**Theorem 1.8** ([13, Theorem 0.1.(4)]). If we further assume

(1) $E$ has good supersingular reduction at $p$,
(2) $p$ does not divide $\dfrac{L(E,1)}{\Omega_E}$, and
(3) $\overline{\rho}$ is surjective

as well as the assumptions of Conjecture 1.6, then Conjecture 1.6 is true.

**Remark 1.9.** Note that $a_p(E) = 0$ is not assumed in Theorem 1.8. In [26, Theorem 1.1.(3)], R. Pollack proved an algebraic analogue of Theorem 1.8 using a formal group argument assuming $a_p(E) = 0$. His work does not require the surjectivity of $\overline{\rho}$.

**Remark 1.10.** For the case of $p = 2$, Conjecture 1.6 may not hold. See [26, Remark 1.2] and [17] for details.

Pollack reformulates Conjecture 1.6 in terms of his signed $p$-adic $L$-functions under the assumption $a_p(E) = 0$. See Section 3.1 for the characterization of the $\pm$-$p$-adic $L$-functions $L_p^{\pm}(\mathbb{Q}_\infty, f)$. We recall a proposition of Pollack, which shows us the connection between Mazur–Tate elements and $\pm$-$p$-adic $L$-functions.

**Proposition 1.11** ([25, Proposition 6.18]).

$$\theta_n(f) \equiv \widetilde{\omega}_n^{\mp} \cdot L_p^{\mp}(\mathbb{Q}_\infty, f) \pmod{\omega_n}$$

in $\Lambda_n$ if $n$ is even/odd, respectively.

Then, as ideals of $\Lambda$, the following equality holds:

$$\left(\omega_n, \theta_n(f), \nu_{n-1,n}\left(\theta_{n-1}(f)\right)\right) = \left(\omega_n, \widetilde{\omega}_n^{+} \cdot L_p^{+}(\mathbb{Q}_\infty, f), \widetilde{\omega}_n^{-} \cdot L_p^{-}(\mathbb{Q}_\infty, f)\right).$$

Thus, assuming $a_p(E) = 0$, Conjecture 1.6 is equivalent to the following conjecture.

**Conjecture 1.12** ([25, Conjecture 6.19]). We assume $a_p(E) = 0$ as well as the conditions in Conjecture 1.6. Then

$$\left(\widetilde{\omega}_n^{+} \cdot L_p^{+}(\mathbb{Q}_\infty, f) \pmod{\omega_n}, \widetilde{\omega}_n^{-} \cdot L_p^{-}(\mathbb{Q}_\infty, f) \pmod{\omega_n}\right) = \mathrm{Fitt}_{\Lambda_n}\left(\mathrm{Sel}(\mathbb{Q}_n, E[p^\infty])^\vee\right).$$

**Remark 1.13.** It is known that Kato's zeta elements exist integrally when $\overline{\rho}$ is surjective. In this case, Proposition 1.11 can be interpreted as a comparison between the $P_n$-pairing made by the second named author and the $\pm$-Coleman maps made by Kobayashi (modulo $\omega_n$) as in the following diagram. See also [18, §1].

$$\begin{tikzcd}
\text{Kato's zeta elements} \arrow[r, mapsto, "P_n\text{-pairing}", "{[13, \text{Lemma } 7.2]}"'] \arrow[d, mapsto, "{\pm\text{-Coleman maps } [12, \text{Theorem } 6.3]}"'] & \text{Mazur-Tate elements} \\
\pm\text{-}p\text{-adic } L\text{-functions} \arrow[ur, dashed, leftrightarrow, "\text{Propsition } 1.11"'] &
\end{tikzcd}$$

### 1.3 Main theorems

We state three main theorems (mainly for elliptic curves with good supersingular reduction).

**Theorem 1.14** (Main Theorem I). Let $E$ be an elliptic curve over $\mathbb{Q}$ with good reduction at an odd prime $p$. Assume that $\overline{\rho}$ is surjective if $E$ is non-CM. Assume one of the following:

(ord) If $p \nmid a_p(E)$, then $a_p(E) \not\equiv 1 \pmod{p}$, or

(ss) If $p \mid a_p(E)$, then $a_p(E) = 0$.

Then

$$\left(\theta_n(f), \nu_{n-1,n}\left(\theta_{n-1}(f)\right)\right) \subseteq \mathrm{Fitt}_{\Lambda_n}\left(\mathrm{Sel}(\mathbb{Q}_n, E[p^\infty])^\vee\right).$$

Thus, Mazur–Tate's weak main conjecture (Conjecture 1.4) for $E$ over $\mathbb{Q}_n$ follows.

In Case (ord), if we further assume $p \nmid \mathrm{Tam}(E)$ and the Iwasawa main conjecture (Conjecture 2.2) holds, then the inclusion becomes an equality, so the strong main conjecture (Conjecture 1.6) holds.

See Section 2 for proof of Case (ord) and Section 4 for proof of Case (ss). See Theorem 2.3 and Theorem 2.4 for the current status of the Iwasawa main conjecture.

Let $\chi : \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \to \overline{\mathbb{Q}}_p^\times$ be a character and $\mathbb{Z}_p[\chi]$ the ring generated by the image of $\chi$ over $\mathbb{Z}_p$. The map $\chi$ naturally extends to an algebra homomorphism $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})] \to \mathbb{Z}_p[\chi]$ defined by $\sigma \mapsto \chi(\sigma)$ where $\sigma \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ and also denote it by $\chi$. Then we also define the **augmentation ideal at** $\chi$ by

$$I_\chi := \ker\left(\chi : \Lambda_n \to \mathbb{Z}_p[\chi]\right).$$

Let $L \in \Lambda_n$. We say $L$ **vanishes to infinite order at** $\chi$ if $L$ is contained in all powers of $I_\chi$. We say $L$ **vanishes to order** $r$ **at** $\chi$ if $L \in I_\chi^r \setminus I_\chi^{r+1}$. See [20, (1.5)] for details.

**Conjecture 1.15** ([20, Conjecture 1, "weak vanishing conjecture"]). The order of vanishing of $\theta_n(f)$ at $\chi$ is greater than or equal to the dimension of the $\chi$-part of the Mordell–Weil group of $E(\mathbb{Q}_n)$.

**Corollary 1.16.** Under the same assumptions of Theorem 1.14, Conjecture 1.15 holds.

**Proof.** [20, Proposition 3]. ■

**Remark 1.17.**

(1) In both conditions (ord) and (ss) in Theorem 1.14, $a_p(E) \not\equiv 1 \pmod{p}$ or $a_p(E) = 0$ ensures that $E(\mathbb{Q})[p]$ is trivial.

(2) An anticyclotomic analogue of Theorem 1.14 is investigated in [9].

(3) See [24] for progress towards Conjecture 1.15.

In the case of elliptic curves with good supersingular reduction (under the surjectivity of $\overline{\rho}$), we can also obtain a lower bound of the Selmer groups as follows. Let $T = \varprojlim_n E[p^n]$ be the $p$-adic Tate module of $E$ and $\mathbb{H}^1_{\mathrm{glob}}(T)$ the global Iwasawa cohomology (defined in Section 5.1). We define the "error term" by

$$\mathrm{Err}_n := \mathrm{coker}\left( \frac{\mathrm{H}^1(\mathbb{Q}_\Sigma/\mathbb{Q}_n, T)}{\mathrm{im}\ \mathbb{H}^1_{\mathrm{glob}}(T)} \to \frac{\mathrm{H}^1(\mathbb{Q}_{n,p}, T)}{E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p + \mathrm{im}\ \mathbb{H}^1_{\mathrm{glob}}(T)} \right),$$

where $\mathrm{im}\ \mathbb{H}^1_{\mathrm{glob}}(T)$ is the image of $\mathbb{H}^1_{\mathrm{glob}}(T)$ in $A$ in the notation $\frac{A}{\mathrm{im}\ \mathbb{H}^1_{\mathrm{glob}}(T)}$. The error term $\mathrm{Err}_n$ also naturally appears as the cokernel of a certain map $g_n$ (Remark 5.4), which is explicitly defined in (5.1) (cf. [12, (10.36) and Proposition 10.6]).

**Theorem 1.18** (Main Theorem II). Let $E$ be an elliptic curve over $\mathbb{Q}$ with good supersingular reduction at an odd prime $p$. Assume that $a_p(E) = 0$, $\overline{\rho}$ is surjective and $p \nmid \mathrm{Tam}(E)$. If the ±-main conjectures (Conjecture 3.5) hold, then

$$\mathrm{Fitt}_{\Lambda_n}\left(\mathrm{Err}_n\right) \cdot \mathrm{Fitt}_{\Lambda_n}\left(\mathrm{Sel}(\mathbb{Q}_n, E[p^\infty])^\vee\right) \subseteq \left(\theta_n(f), \nu_{n-1,n}\left(\theta_{n-1}(f)\right)\right) \subseteq \mathrm{Fitt}_{\Lambda_n}\left(\mathrm{Sel}(\mathbb{Q}_n, E[p^\infty])^\vee\right).$$

See Section 5 for proof. Note that the surjectivity of $\overline{\rho}$ implies $E$ has no CM. Also, see Theorem 3.6 and Remark 3.7 for the current status of the ±-Iwasawa main conjecture. Although $\mathrm{Err}_n$ might not be zero in general, if it vanishes, then Conjecture 1.6 holds.

**Remark 1.19.** As a $\mathbb{Z}_p$-module, $\mathrm{Err}_n$ is finitely generated. Also, $\mathrm{Err}_n$ stabilizes as $n >> 0$. See [12, (Proof of) Proposition 10.6].

We define the **fine Selmer groups of $E$ over $\mathbb{Q}_n$** by

$$\mathrm{Sel}_0(\mathbb{Q}_n, E[p^\infty]) := \ker\left(\mathrm{Sel}(\mathbb{Q}_n, E[p^\infty]) \to \mathrm{H}^1(\mathbb{Q}_{n,p}, E[p^\infty])\right)$$

and $\mathrm{Sel}_0(\mathbb{Q}_\infty, E[p^\infty]) := \varinjlim_n \mathrm{Sel}_0(\mathbb{Q}_n, E[p^\infty])$ as in [13, Definition 4.1] and [18, §0.3].

**Theorem 1.20** (Main Theorem III). Under the assumptions of Theorem 1.18, we further assume (fineNF) $\mathrm{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^\vee$ has no nontrivial finite $\Lambda$-submodule, and

(III) if $\Phi_n(1+X)$ divides a generator of $\mathrm{char}_\Lambda\left(\mathrm{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^\vee\right)$, then $\mathrm{rk}_{\mathbb{Z}} E(\mathbb{Q}_n) > \mathrm{rk}_{\mathbb{Z}} E(\mathbb{Q}_{n-1})$ (if $n = 0$, then $\Phi_0(1+X) = X$, and this inequality means $\mathrm{rk}_{\mathbb{Z}} E(\mathbb{Q}) > 0$).

Then $\mathrm{Err}_n$ vanishes. Therefore, the strong main conjecture (Conjecture 1.6)

$$\left(\theta_n(f), \nu_{n-1,n}\left(\theta_{n-1}(f)\right)\right) = \mathrm{Fitt}_{\Lambda_n}\left(\mathrm{Sel}(\mathbb{Q}_n, E[p^\infty])^\vee\right)$$

holds.

See Section 6 for proof.

**Example 1.21.** There are many examples satisfying Assumptions (fineNF) and (III) in Theorem 1.20.

(1) We note that Assumption (III) is satisfied if at least one of the following conditions is satisfied:

(a) The characteristic ideal of $\mathrm{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^\vee$ is prime to $\omega_n$ for all $n$.

(b) If $\Phi_n(1+X)$ divides a generator of the characteristic ideal of $\mathrm{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^\vee$, then $\text{Ш}(E/\mathbb{Q}_n)[p^\infty]$ is finite for all $n$.

In fact, the implication of Assumption (III) from (a) is trivial and that from (b) can be proved by the control theorem for fine Selmer groups (cf. [13, Lemma 4.2, Remark 4.4]). By (b), we expect that Assumption (III) always holds. Therefore, the only essential condition in Theorem 1.20 is Assumption (fineNF).

(2) If one of the following conditions occurs, then both Assumptions (fineNF) and (III) follow:

- $\mathrm{Sel}_0(\mathbb{Q}, E[p^\infty])$ is trivial. (See [13, Lemma 4.3] and [26].)
- $\mathrm{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])_{\Gamma_n}$ is trivial. (It is a weaker condition than the one above.)
- $\mathrm{Sel}_0(\mathbb{Q}_\infty, E[p^\infty]) = \ker\left(E(\mathbb{Q}_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to E(\mathbb{Q}_{\infty,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p\right)$.

Note that the first two cases never occur if $\mathrm{rk}_{\mathbb{Z}} E(\mathbb{Q}) > 1$. The fine Selmer group is said to be **all Mordell–Weil** if the last case holds. In the all Mordell–Weil case, $\mathrm{Sel}_0(\mathbb{Q}_n, E[p^\infty])^\vee$ is free over $\mathbb{Z}_p$, so Assumptions (fineNF) and (III) follow.

(3) It is conjectured by Greenberg that the roots of a generator of $\mathrm{char}_\Lambda(\mathrm{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^\vee)$ are all of the form $\zeta - 1$ where $\zeta$ is a $p$-power root of unity. See [18, Problem 0.7] for details.

## 2 Review of the Case for Elliptic Curves with Good Ordinary Reduction

In this section, we prove Theorem 1.14 for elliptic curves with good ordinary reduction.

### 2.1 Tools from Iwasawa theory

Let $E$ be an elliptic curve over $\mathbb{Q}$ with good ordinary reduction at $p$. We first recall the $\Lambda$-cotorsion property of Selmer groups. See [30, Theorem 4.4], [4, Theorem 1.5], and [7, Theorem 17.4.(1)] for details.

**Theorem 2.1.** The Selmer group $\mathrm{Sel}(\mathbb{Q}_\infty, E[p^\infty])$ is $\Lambda$-cotorsion.

The following statement is the Iwasawa main conjecture for elliptic curves with ordinary reduction. See [19, §1.(c)], [4, Conjecture 1.13], and [7, Conjecture 17.6] for details.

**Conjecture 2.2** (Iwasawa main conjecture). Let $p$ be an odd prime and $E$ an elliptic curve over $\mathbb{Q}$ with $p \nmid a_p(E)$. Then

$$\left(L_p(\mathbb{Q}_\infty, f_\alpha)\right) = \mathrm{char}_\Lambda \left(\mathrm{Sel}(\mathbb{Q}_\infty, E[p^\infty])^\vee\right),$$

where $L_p(\mathbb{Q}_\infty, f_\alpha)$ is the $p$-adic $L$-function of the $p$-stabilized form $f_\alpha$ with the unit root $\alpha$.

The following theorem is due to Rubin [31, Theorem 12.3] for the CM case and Kato [7, Theorem 17.4.(3)] for the non-CM case.

**Theorem 2.3.** Let $p$ be an odd prime and $E$ be an elliptic curve over $\mathbb{Q}$ with $p \nmid a_p(E)$.

(1) If $E$ has CM, then Conjecture 2.2 holds.

(2) If $E$ has no CM, then we assume $\overline{\rho}$ is surjective. Then

$$\left(L_p(\mathbb{Q}_\infty, f_\alpha)\right) \subseteq \mathrm{char}_\Lambda \left(\mathrm{Sel}(\mathbb{Q}_\infty, E[p^\infty])^\vee\right).$$

For the non-CM case, we have the following theorem is due to Skinner–Urban [32, Theorem 3.29], X. Wan [35, Theorem 4], and Kim–Kim–Sun [10, Theorem 1.1].

**Theorem 2.4.** Keep all the assumptions in Theorem 2.3.

[33] If there exists a prime $q\|N$ such that $\overline{\rho}$ is ramified at $q$, then Conjecture 2.2 holds.

[35] If there exists a real quadratic field $F/\mathbb{Q}$ such that

- $p$ is unramified in $F$,
- any prime $q$ dividing $N$ such that $q \equiv -1 \pmod{p}$ is inert in $F/\mathbb{Q}$, and any other prime dividing $N$ splits in $F/\mathbb{Q}$,
- the canonical period of $f$ over $F$ is the square of its canonical period over $\mathbb{Q}$ up to a $p$-adic unit,

then Conjecture 2.2 holds.

[10] If $\widetilde{\delta}_n \neq 0$ for some $n$ and $p \nmid \mathrm{Tam}(E) \cdot \prod_{q|N_{\mathrm{sp}}}(q-1) \cdot \prod_{q'|N_{\mathrm{ns}}}(q'+1)$, where $N_{\mathrm{sp}}$ is the product of split multiplicative reduction primes of $E$ and $N_{\mathrm{ns}}$ is the product of non-split multiplicative reduction primes of $E$, then Conjecture 2.2 holds.

The following theorem is due to Greenberg [4, Proposition 4.14] and Hachimori–Matsuno [5, Corollary].

**Theorem 2.5.** The Selmer group $\mathrm{Sel}(\mathbb{Q}_\infty, E[p^\infty])$ has no proper $\Lambda$-submodule of finite index.

We recall the control theorem for $E$ over the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$.

**Theorem 2.6.** The restriction map

$$\mathrm{Sel}\big(\mathbb{Q}_n, E[p^\infty]\big) \to \mathrm{Sel}\big(\mathbb{Q}_\infty, E[p^\infty]\big)[\omega_n]$$

is injective with the finite cokernel whose size is bounded independently of $n$. If we further assume that $a_p(E) \not\equiv 1 \pmod{p}$ and $p \nmid \mathrm{Tam}(E)$, then the restriction map is an isomorphism.

**Proof.** See [4, Proposition 3.7, Proposition 3.8, and Proposition 3.9]. ■

### 2.2 Proof of Theorem 1.14 for the case of good ordinary reduction

This is basically obtained in [14, Corollary 10.3]. From Theorem 2.3, we have

$$\big(L_p(\mathbb{Q}_\infty, f_\alpha)\big) \subseteq \mathrm{char}_\Lambda \left(\mathrm{Sel}(\mathbb{Q}_\infty, E[p^\infty])^\vee\right).$$

By Theorem 2.1 and Theorem 2.5, characteristic ideals are equal to Fitting ideals via Lemma A.7; thus, we have

$$\left(L_p(\mathbb{Q}_\infty, f_\alpha)\right) \subseteq \mathrm{Fitt}_\Lambda \left(\mathrm{Sel}(\mathbb{Q}_\infty, E[p^\infty])^\vee\right).$$

Taking the quotient by $\omega_n$, we have

$$\left(\vartheta_n(f_\alpha)\right) \subseteq \mathrm{Fitt}_{\Lambda_n} \left(\left(\mathrm{Sel}(\mathbb{Q}_\infty, E[p^\infty])[\omega_n]\right)^\vee\right),$$

where

$$\vartheta_n(f_\alpha) = \frac{1}{\alpha^n} \cdot \left(\theta_n(f) - \frac{1}{\alpha} \cdot \nu_{n-1,n}\left(\theta_{n-1}(f)\right)\right)$$

is the $p$-stabilized Mazur–Tate element with the unit root $\alpha$. Using Theorem 2.6 and Lemma A.1, we have

$$\left(\vartheta_n(f_\alpha)\right) \subseteq \mathrm{Fitt}_{\Lambda_n} \left(\mathrm{Sel}(\mathbb{Q}_n, E[p^\infty])^\vee\right).$$

Since $a_p(E) \not\equiv 1 \pmod{p}$, it is not difficult to observe

$$\vartheta_n(f_\alpha) = u \cdot \theta_n(f)$$

for some $u \in \Lambda_n^\times$. It shows that

$$\left(\theta_n(f), \nu_{n-1,n}\left(\theta_{n-1}(f)\right)\right) \subseteq \mathrm{Fitt}_{\Lambda_n} \left(\mathrm{Sel}(\mathbb{Q}_n, E[p^\infty])^\vee\right).$$

We also note that $\nu_{n-1,n}(\theta_{n-1}(f))$ is a multiple of $\vartheta_n(f)$, so the ideal $(\theta_n(f), \nu_{n-1,n}(\theta_{n-1}(f))$ is the principal ideal generated by $\vartheta_n(f)$, equivalently by $\theta_n(f)$.

If we further assume $p \nmid \mathrm{Tam}(E)$ and the Iwasawa main conjecture (Conjecture 2.2, Theorem 2.3, and Theorem 2.4), then all the inclusions in the proof become equalities, so we have

$$\left(\theta_n(f)\right) = \mathrm{Fitt}_{\Lambda_n} \left(\mathrm{Sel}(\mathbb{Q}_n, E[p^\infty])^\vee\right).$$

## 3 Tools from ±-Iwasawa Theory

### 3.1 Basic objects of ±-Iwasawa theory

We quickly recall the basic objects of ±-Iwasawa theory. For a more detailed description, we refer to [12] for the algebraic side and to [25] for the analytic side.

**Remark 3.1** (Sign convention). We fix the sign convention of ±-Iwasawa theory as follows:

(1) Selmer groups: [12]

(2) $p$-adic $L$-functions: [25] = −[12]

(3) Coleman maps: [18] = −[12]

### 3.1.1 *Local conditions at p*

Let $E$ be an elliptic curve over $\mathbb{Q}$ with $a_p(E) = 0$. Then we define

$$E^+(\mathbb{Q}_{n,p}) := \left\{P \in E(\mathbb{Q}_{n,p}) : \mathrm{Tr}_{n/m+1}(P) \in E(\mathbb{Q}_{m,p}) \text{ for even } m\ (0 \le m < n)\right\}$$
$$E^-(\mathbb{Q}_{n,p}) := \left\{P \in E(\mathbb{Q}_{n,p}) : \mathrm{Tr}_{n/m+1}(P) \in E(\mathbb{Q}_{m,p}) \text{ for odd } m\ (0 \le m < n)\right\},$$

where $\mathbb{Q}_{n,p}$ is the completion of $\mathbb{Q}_n$ at $p$ and $\mathrm{Tr}_{n/m+1} : E(\mathbb{Q}_{n,p}) \to E(\mathbb{Q}_{m+1,p})$ is the trace map.

### 3.1.2 *The norm subgroups*

Let $\widehat{E}$ be the formal group associated to $E$ and $\mathfrak{m}_n$ be the maximal ideal of $\mathbb{Q}_{n,p}$. We define

$$\widehat{E}^+(\mathfrak{m}_n) := \left\{P \in \widehat{E}(\mathfrak{m}_n) : \mathrm{Tr}_{n/m+1}(P) \in \widehat{E}(\mathfrak{m}_m) \text{ for even } m\ (0 \le m < n)\right\}$$
$$\widehat{E}^-(\mathfrak{m}_n) := \left\{P \in \widehat{E}(\mathfrak{m}_n) : \mathrm{Tr}_{n/m+1}(P) \in \widehat{E}(\mathfrak{m}_m) \text{ for odd } m\ (0 \le m < n)\right\},$$

where $\mathrm{Tr}_{n/m+1} : \widehat{E}(\mathfrak{m}_n) \to \widehat{E}(\mathfrak{m}_{m+1})$ is the trace map.

### 3.1.3 *±-Selmer groups*

Following [12, Definition 1.1] and [8, Definition 3.1], we define the **±-Selmer groups of $E$ over $\mathbb{Q}_n$** by

$$\begin{aligned}
&\mathrm{Sel}^{\pm}(\mathbb{Q}_n, E[p^\infty]) \\
&:= \ker\left(\mathrm{Sel}(\mathbb{Q}_n, E[p^\infty]) \to \frac{\mathrm{H}^1(\mathbb{Q}_{n,p}, E[p^\infty])}{E^{\pm}(\mathbb{Q}_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}\right) \\
&= \ker\left(\mathrm{H}^1(\mathbb{Q}_\Sigma/\mathbb{Q}_n, E[p^\infty]) \to \frac{\mathrm{H}^1(\mathbb{Q}_{n,p}, E[p^\infty])}{E^{\pm}(\mathbb{Q}_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \times \prod_{w \mid \ell, \ell \in \Sigma, \ell \neq p} \frac{\mathrm{H}^1(\mathbb{Q}_{n,w}, E[p^\infty])}{E(\mathbb{Q}_{n,w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}\right)
\end{aligned}$$

and the **±-Selmer groups of $E$ over $\mathbb{Q}_\infty$** by

$$\mathrm{Sel}^{\pm}(\mathbb{Q}_\infty, E[p^\infty]) := \varinjlim_n \mathrm{Sel}^{\pm}(\mathbb{Q}_n, E[p^\infty]),$$

respectively. Note that ±-Selmer groups are also independent of the choice of $\Sigma$ as usual Selmer groups are since the local conditions at the places above $p$ are only changed. Also, it is easy to see

$$\mathrm{Sel}_0(\mathbb{Q}_n, E[p^\infty]) \subseteq \mathrm{Sel}^{\pm}(\mathbb{Q}_n, E[p^\infty]) \subseteq \mathrm{Sel}(\mathbb{Q}_n, E[p^\infty]),$$

respectively.

### 3.1.4 *±-p-adic L-functions and ±-Coleman maps*

We recall the characterization of **±-$p$-adic $L$-functions** $L_p^{\pm}(\mathbb{Q}_\infty, f) \in \Lambda$ by their interpolation property [29, (10), (11), and (12)]:

$$\begin{aligned}
\chi\left(L_p^{+}(\mathbb{Q}_\infty, f)\right) &= (-1)^{(n+1)/2} \cdot \frac{\tau(\chi)}{\chi(\widetilde{\omega}_n^{+})} \cdot \frac{L(E, \chi^{-1}, 1)}{\Omega_E} && \text{if } \chi \text{ has order } p^n \text{ with } n \text{ odd} \\
\chi\left(L_p^{-}(\mathbb{Q}_\infty, f)\right) &= (-1)^{(n/2)+1} \cdot \frac{\tau(\chi)}{\chi(\widetilde{\omega}_n^{-})} \cdot \frac{L(E, \chi^{-1}, 1)}{\Omega_E} && \text{if } \chi \text{ has order } p^n > 1 \text{ with } n \text{ even} \\
\mathbf{1}\left(L_p^{+}(\mathbb{Q}_\infty, f)\right) &= (p-1) \cdot \frac{L(E, 1)}{\Omega_E} \\
\mathbf{1}\left(L_p^{-}(\mathbb{Q}_\infty, f)\right) &= 2 \cdot \frac{L(E, 1)}{\Omega_E},
\end{aligned}$$

where $\chi$ is a character of $\Gamma$, $\mathbf{1}$ is the trivial character, and $\tau(\chi)$ is the Gauss sum of $\chi$.

We also recall **±-Coleman maps**. Our sign convention follows that of [18].

**Theorem 3.2** ([12, Theorem 6.2, Theorem 6.3, and §8], [18, §1.1]). There exist maps

$$\mathrm{Col}_n^{\pm} : \mathrm{H}^1\left(\mathbb{Q}_{n,p}, T\right) \to \Lambda_n/\omega_n^{\mp}$$

such that

(1) $\mathrm{Col}_n^{\pm} : \mathrm{H}^1\left(\mathbb{Q}_{n,p}, T\right)/\ker \mathrm{Col}_n^{\pm} \simeq \Lambda_n/\omega_n^{\mp}$ and
(2) $\mathrm{Col}_n^{\pm}\left(\mathrm{loc}\ \mathbf{z}_{\mathrm{Kato},n}\right) = L_p^{\pm}(\mathbb{Q}_n, f)$,

where $\mathbf{z}_{\mathrm{Kato},n} \in \mathrm{H}^1(\mathbb{Q}_n, T)$ is Kato's zeta element at $\mathbb{Q}_n$ and $L_p^{\pm}(\mathbb{Q}_n, f) := L_p^{\pm}(\mathbb{Q}_\infty, f) \pmod{\omega_n^{\mp}}$. By taking the inverse limit with respect to $n$, we have maps

$$\mathrm{Col}^{\pm} : \mathbb{H}^1_{\mathrm{loc}}(T) \to \Lambda$$

such that

(1) $\mathrm{Col}^{\pm}$ are surjective and
(2) $\mathrm{Col}^{\pm}(\mathrm{loc}\ \mathbf{z}_{\mathrm{Kato}}) = L_p^{\pm}\left(\mathbb{Q}_\infty, f\right)$,

where

$$\mathbb{H}^1_{\mathrm{loc}}(T) := \varprojlim_n \mathrm{H}^1\left(\mathbb{Q}_{n,p}, T\right)$$

is the local Iwasawa cohomology group and $\mathbf{z}_{\mathrm{Kato}} \in \mathrm{H}^1(\mathbb{Q}_\infty, T)$ is Kato's zeta element at $\mathbb{Q}_\infty$.

**Remark 3.3.** The construction of $\mathrm{Col}^{\pm}_n$ in [12] uses certain local points of formal groups of elliptic curves via Honda theory and that in [18] uses the $P_n$-paring defined by the second named author in [13] and Proposition 1.11.

### 3.2 ±-main conjectures

We recall the $\Lambda$-cotorsion property of ±-Selmer groups ([12, Theorem 7.3.ii)], [29, Theorem 6.3]).

**Theorem 3.4.** Let $p$ be an odd prime and $E$ an elliptic curve over $\mathbb{Q}$ with $a_p(E) = 0$. Then both $\mathrm{Sel}^+(\mathbb{Q}_\infty, E[p^\infty])$ and $\mathrm{Sel}^-(\mathbb{Q}_\infty, E[p^\infty])$ are $\Lambda$-cotorsion.

The following statement is the pair of the Iwasawa main conjectures for elliptic curves with supersingular reduction ([12, Even, odd main conjectures, §4]).

**Conjecture 3.5** (±-main conjectures). Let $p$ be an odd prime and $E$ an elliptic curve over $\mathbb{Q}$ with $a_p(E) = 0$. Then

$$\left(L_p^{\mp}(\mathbb{Q}_\infty, f)\right) = \mathrm{char}_\Lambda\left(\mathrm{Sel}^{\pm}(\mathbb{Q}_\infty, E[p^\infty])^\vee\right).$$

As in the ordinary case, the Euler system argument yields the following statement ([12, Theorem 4.1], [29, Theorem in Introduction]).

**Theorem 3.6.** Let $p$ be an odd prime and $E$ an elliptic curve over $\mathbb{Q}$ with $a_p(E) = 0$.

(1) If $E$ has CM, then Conjecture 3.5 holds.

(2) If $E$ has no CM, then we assume $\overline{\rho}$ is surjective. Then

$$\left(L_p^{\mp}(\mathbb{Q}_\infty, f)\right) \subseteq \mathrm{char}_\Lambda\left(\mathrm{Sel}^{\pm}(\mathbb{Q}_\infty, E[p^\infty])^\vee\right).$$

**Remark 3.7.** Even in the non-CM case, there are several approaches to establish Conjecture 3.5 under certain tame level assumptions. Since none of them is published yet, we just record the assumptions they made. More precisely, it is announced that the ±-main conjectures hold if the conditions in Theorem 3.6 and one of the following tame level conditions hold:

[36] there exists a prime $q \| N$ such that $\overline{\rho}$ is ramifed at $q$,

[36] $N$ is square-free and there exist two primes $q \| N$ such that $\overline{\rho}$ is ramified at $q$, or

[37] $N$ is square-free (only assuming the absolute irreducibility of $\overline{\rho}$).

In addition, the numerical criterion of Kim–Kim–Sun described in Theorem 2.4 still works to verify the ±-main conjectures (without these tame level assumptions) in the exactly same way. If the validity of the results in these preprints is confirmed, then the ±-main conjecture assumption in Theorem 1.18 could be removed. Note that any of these results is used in this article. Especially, Theorem 3.6.(2) is strong enough to prove the Mazur–Tate conjecture (Theorem 1.14).

### 3.3 Nonexistence of proper $\Lambda$-submodules of finite index

We recall B.D. Kim's result [8, Theorem 1.1] on the analogue of Theorem 2.5 for the supersingular setting. For the further developments along this direction, see [11].

**Theorem 3.8.** The Selmer groups $\mathrm{Sel}^{+}(\mathbb{Q}_{\infty}, E[p^{\infty}])$ and $\mathrm{Sel}^{-}(\mathbb{Q}_{\infty}, E[p^{\infty}])$ have no proper $\Lambda$-submodule of finite index.

### 3.4 ±-exact control theorems

We recall the ±-version of the control theorem ([12, Theorem 9.3], [6, Theorem 6.8]).

**Theorem 3.9** (±-control theorems). The restriction map

$$\mathrm{Sel}^{\pm}(\mathbb{Q}_{n}, E[p^{\infty}])[\omega_{n}^{\pm}] \to \mathrm{Sel}^{\pm}(\mathbb{Q}_{\infty}, E[p^{\infty}])[\omega_{n}^{\pm}]$$

is injective with the finite cokernel whose size is bounded independently of $n$. If we further assume that $p \nmid \mathrm{Tam}(E)$, then the restriction map is an isomorphism.

**Proof.** The $a_p(E) = 0$ condition ensures that $E(\mathbb{Q})[p]$ is trivial, and it implies that the restriction map is injective as in [12, Lemma 9.1]. The failure of the surjectivity comes only from prime-to-$p$ local conditions; thus, the situation coincides with the ordinary case. The $p \nmid \mathrm{Tam}(E)$ condition ensures that the failure vanishes. See [12, Theorem 9.3] and [4, Proposition 3.8] for details. ■

### 3.5 The consequence

**Corollary 3.10.** Let $p$ be an odd prime and $E$ an elliptic curve over $\mathbb{Q}$ with $a_p(E) = 0$. Assume $\overline{\rho}$ is surjective if $E$ has no CM. Then we have

$$\left(\widetilde{\omega}_n^{\mp} \cdot L_p^{\mp}(\mathbb{Q}_\infty, f) \pmod{\omega_n}\right) \subseteq \widetilde{\omega}_n^{\mp} \cdot \mathrm{Fitt}_{\Lambda_n}\left(\mathrm{Sel}^{\pm}(\mathbb{Q}_n, E[p^\infty])^\vee\right)$$

in $\Lambda_n$, respectively.

**Proof.** By Theorem 3.4, Theorem 3.6, Theorem 3.8, and Lemma A.7, we have

$$\left(L_p^{\mp}(\mathbb{Q}_\infty, f)\right) \subseteq \mathrm{Fitt}_{\Lambda}\left(\mathrm{Sel}^{\pm}(\mathbb{Q}_\infty, E[p^\infty])^\vee\right)$$

under the conditions of Theorem 3.6. Taking the quotient by $\omega_n^{\pm}$, we obtain

$$\left(L_p^{\mp}(\mathbb{Q}_\infty, f) \pmod{\omega_n^{\pm}}\right) \subseteq \mathrm{Fitt}_{\Lambda_n/\omega_n^{\pm}}\left(\left(\mathrm{Sel}^{\pm}(\mathbb{Q}_\infty, E[p^\infty])[\omega_n^{\pm}]\right)^\vee\right)$$

in $\Lambda_n/\omega_n^{\pm}$, respectively. By Theorem 3.9 and Lemma A.1, we obtain

$$\left(L_p^{\mp}(\mathbb{Q}_\infty, f) \pmod{\omega_n^{\pm}}\right) \subseteq \mathrm{Fitt}_{\Lambda_n/\omega_n^{\pm}}\left(\left(\mathrm{Sel}^{\pm}(\mathbb{Q}_n, E[p^\infty])[\omega_n^{\pm}]\right)^\vee\right)$$

in $\Lambda_n/\omega_n^{\pm}$, respectively. Since we have the following equality:

$$\mathrm{Fitt}_{\Lambda_n/\omega_n^{\pm}}\left(\left(\mathrm{Sel}^{\pm}(\mathbb{Q}_n, E[p^\infty])\left[\omega_n^{\pm}\right]\right)^\vee\right) = \frac{\mathrm{Fitt}_{\Lambda_n}\left(\mathrm{Sel}^{\pm}(\mathbb{Q}_n, E[p^\infty])^\vee\right) + \left(\omega_n^{\pm}\right)}{(\omega_n^{\pm})}$$

in $\Lambda_n/\omega_n^{\pm}$ by Lemma A.6, we have inclusions

$$\left(L_p^{\mp}(\mathbb{Q}_\infty, f) \pmod{\omega_n}\right) + (\omega_n^{\pm}) \subseteq \mathrm{Fitt}_{\Lambda_n}\left(\mathrm{Sel}^{\pm}(\mathbb{Q}_n, E[p^\infty])^\vee\right) + (\omega_n^{\pm})$$

in $\Lambda_n$, respectively. Multiplying $\widetilde{\omega}_n^{\mp}$, the conclusion immediately follows. ■

**Remark 3.11.** If we further assume $p \nmid \mathrm{Tam}(E)$ and the ±-main conjectures, then the inclusion in Corollary 3.10 becomes an equality.

## 4 Comparison of Local Conditions at $p$

Consider the exact sequence of $\Lambda_n$-modules (cf. [11, (4.2)])

$$\left(\frac{E(\mathbb{Q}_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}{E^{\pm}(\mathbb{Q}_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}\right)^{\vee} \xrightarrow{\iota^{\pm}} \mathrm{Sel}(\mathbb{Q}_n, E[p^{\infty}])^{\vee} \longrightarrow \mathrm{Sel}^{\pm}(\mathbb{Q}_n, E[p^{\infty}])^{\vee} \longrightarrow 0.$$

Then we have

$$\mathrm{Fitt}_{\Lambda_n}\left(\left(\frac{E(\mathbb{Q}_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}{E^{\pm}(\mathbb{Q}_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}\right)^{\vee} / \ker(\iota^{\pm})\right) \cdot \mathrm{Fitt}_{\Lambda_n}\left(\mathrm{Sel}^{\pm}(\mathbb{Q}_n, E[p^{\infty}])^{\vee}\right) \subseteq \mathrm{Fitt}_{\Lambda_n}\left(\mathrm{Sel}(\mathbb{Q}_n, E[p^{\infty}])^{\vee}\right)$$

by Lemma A.2. By Lemma A.1, we also have

$$\mathrm{Fitt}_{\Lambda_n}\left(\left(\frac{E(\mathbb{Q}_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}{E^{\pm}(\mathbb{Q}_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}\right)^{\vee}\right) \subseteq \mathrm{Fitt}_{\Lambda_n}\left(\left(\frac{E(\mathbb{Q}_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}{E^{\pm}(\mathbb{Q}_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}\right)^{\vee} / \ker(\iota^{\pm})\right).$$

We observe that

$$\begin{aligned}\left(\frac{E(\mathbb{Q}_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}{E^{\pm}(\mathbb{Q}_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}\right)^{\vee} &\simeq \left(\frac{\widehat{E}(\mathfrak{m}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p}{\widehat{E}^{\pm}(\mathfrak{m}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p}\right)^{\vee} \qquad \text{[11, Lemma 3.14]} \\ &\simeq \left(\frac{\widehat{E}(\mathfrak{m}_n)}{\widehat{E}^{\pm}(\mathfrak{m}_n)} \otimes \mathbb{Q}_p/\mathbb{Z}_p\right)^{\vee}.\end{aligned}$$

Due to [6, Proposition 4.11], we have the following exact sequence:

$$\begin{tikzcd}
0 \arrow[r] & \widehat{E}(p\mathbb{Z}_p) \arrow[r, "f"] \arrow[d, "\simeq"'] & \widehat{E}^{+}(\mathfrak{m}_n) \oplus \widehat{E}^{-}(\mathfrak{m}_n) \arrow[r, "g"] \arrow[d, "\simeq"'] & \widehat{E}(\mathfrak{m}_n) \arrow[r] \arrow[d, "\simeq"', "{[6, \text{Proposition } 5.8]}"] & 0 \\
0 \arrow[r] & \widetilde{\omega}_n^{+}\widetilde{\omega}_n^{-}\Lambda_n \arrow[r] & \widetilde{\omega}_n^{-}\Lambda_n \oplus \widetilde{\omega}_n^{+}\Lambda_n \arrow[r] & \left(\widetilde{\omega}_n^{+}, \widetilde{\omega}_n^{-}\right)\Lambda_n \arrow[r] & 0,
\end{tikzcd}$$

where $f$ is the diagonal embedding and $g : (a, b) \mapsto a - b$. Note that $\widetilde{\omega}_n^{+}\widetilde{\omega}_n^{-}\Lambda_n \simeq \Lambda_n/X\Lambda_n \simeq \mathbb{Z}_p$. This implies that

$$\widehat{E}(\mathfrak{m}_n)/\widehat{E}^{\pm}(\mathfrak{m}_n) \simeq \left(\widetilde{\omega}_n^{+}, \widetilde{\omega}_n^{-}\right)\Lambda_n/\widetilde{\omega}_n^{\mp}\Lambda_n.$$

Then

$$\mathrm{Fitt}_{\Lambda_n}\left(\left(\frac{\left(\widetilde{\omega}_n^{+}, \widetilde{\omega}_n^{-}\right)\Lambda_n}{\widetilde{\omega}_n^{\mp}\Lambda_n} \otimes \mathbb{Q}_p/\mathbb{Z}_p\right)^{\vee}\right) = \mathrm{Fitt}_{\Lambda_n}\left(\left(\left(\widehat{E}(\mathfrak{m}_n)/\widehat{E}^{\pm}(\mathfrak{m}_n)\right) \otimes \mathbb{Q}_p/\mathbb{Z}_p\right)^{\vee}\right).$$

The following proposition is due to R. Pollack.

**Proposition 4.1.**

$$\mathrm{Fitt}_{\Lambda_n}\left(\left(\frac{\left(\widetilde{\omega}_n^{+},\widetilde{\omega}_n^{-}\right)\Lambda_n}{\widetilde{\omega}_n^{\mp}\Lambda_n}\otimes\mathbb{Q}_p/\mathbb{Z}_p\right)^{\vee}\right)=\widetilde{\omega}_n^{\mp}\Lambda_n.$$

**Proof.** Since the multiplication by $\omega_n^{\pm}$ induces an isomorphism $\Lambda_n/\widetilde{\omega}_n^{\mp}\Lambda_n \simeq \omega_n^{\pm}\Lambda_n$, we have

$$\Lambda_n/\widetilde{\omega}_n^{\mp}\simeq\frac{\left(\widetilde{\omega}_n^{+},\widetilde{\omega}_n^{-}\right)\Lambda_n}{\widetilde{\omega}_n^{\mp}\Lambda_n}.$$

We compute

$$\begin{aligned}\left(\frac{\left(\widetilde{\omega}_n^{+},\widetilde{\omega}_n^{-}\right)\Lambda_n}{\widetilde{\omega}_n^{\mp}\Lambda_n}\otimes\mathbb{Q}_p/\mathbb{Z}_p\right)^{\vee}&\simeq\mathrm{Hom}_{\mathbb{Z}_p}\left(\frac{\left(\widetilde{\omega}_n^{+},\widetilde{\omega}_n^{-}\right)\Lambda_n}{\widetilde{\omega}_n^{\mp}\Lambda_n}\otimes\mathbb{Q}_p/\mathbb{Z}_p,\mathbb{Q}_p/\mathbb{Z}_p\right)\\&\simeq\mathrm{Hom}_{\mathbb{Z}_p}\left(\Lambda_n/\widetilde{\omega}_n^{\mp},\mathbb{Z}_p\right).\end{aligned}$$

A direct calculation shows the following identities:

$$\begin{aligned}\widetilde{\omega}_n^{+,\iota}&:=\prod_{2\leq m\leq n,m:\text{even}}\Phi_m\left(\frac{1}{1+X}\right)\\&=\prod_{2\leq m\leq n,m:\text{even}}\left(\Phi_m(1+X)\cdot(1+X)^{-p^{m-1}(p-1)}\right)\\&=\left(\prod_{2\leq m\leq n,m:\text{even}}(1+X)^{-p^{m-1}(p-1)}\right)\cdot\widetilde{\omega}_n^{+},\end{aligned}$$

and

$$\begin{aligned}\widetilde{\omega}_n^{-,\iota}&:=\prod_{1\leq m\leq n,m:\text{odd}}\Phi_m\left(\frac{1}{1+X}\right)\\&=\prod_{1\leq m\leq n,m:\text{odd}}\left(\Phi_m(1+X)\cdot(1+X)^{-p^{m-1}(p-1)}\right)\\&=\left(\prod_{1\leq m\leq n,m:\text{odd}}(1+X)^{-p^{m-1}(p-1)}\right)\cdot\widetilde{\omega}_n^{-}.\end{aligned}$$

We write

$$c^{+}=\left(\prod_{2\leq m\leq n,m:\text{ even}}(1+X)^{-p^{m-1}(p-1)}\right),\qquad c^{-}=\left(\prod_{1\leq m\leq n,m:\text{ odd}}(1+X)^{-p^{m-1}(p-1)}\right)$$

and note that they are invertible in $\Lambda_n$.

We consider a perfect pairing $\Lambda_n \times \Lambda_n \to \mathbb{Z}_p$ defined by $(\sigma, \tau) = 1$ if $\tau = \sigma^{-1}$ and $(\sigma, \tau) = 0$ otherwise, where $\sigma, \tau \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$. Then the pairing induces an isomorphism

$$\mathrm{Hom}_{\mathbb{Z}_p}(\Lambda_n, \mathbb{Z}_p) \simeq \Lambda_n$$

with the reversed $\Lambda_n$-action. Then we have

$$\begin{aligned}
\mathrm{Hom}_{\mathbb{Z}_p}\left(\Lambda_n/\widetilde{\omega}_n^{\mp}, \mathbb{Z}_p\right) &\simeq \mathrm{Hom}_{\mathbb{Z}_p}(\Lambda_n, \mathbb{Z}_p)\left[\widetilde{\omega}_n^{\mp}\right] \\
&\simeq \Lambda_n\left[\widetilde{\omega}_n^{\mp,\iota}\right] \\
&\simeq \Lambda_n\left[\widetilde{\omega}_n^{\mp}\right] && \left(c_n^{\mp} \in \Lambda_n^{\times}\right) \\
&\simeq \omega_n^{\pm}\Lambda_n.
\end{aligned}$$

■

To sum up, we have

$$\begin{aligned}
\widetilde{\omega}_n^{\mp} \cdot \mathrm{Fitt}_{\Lambda_n}\left(\mathrm{Sel}^{\pm}(\mathbb{Q}_n, E[p^\infty])^\vee\right) &= \mathrm{Fitt}_{\Lambda_n}\left(\left(\frac{\left(\widetilde{\omega}_n^{+}, \widetilde{\omega}_n^{-}\right)\Lambda_n}{\widetilde{\omega}_n^{\mp}\Lambda_n} \otimes \mathbb{Q}_p/\mathbb{Z}_p\right)^\vee\right) \\
&\quad \cdot \mathrm{Fitt}_{\Lambda_n}\left(\mathrm{Sel}^{\pm}(\mathbb{Q}_n, E[p^\infty])^\vee\right) \\
&= \mathrm{Fitt}_{\Lambda_n}\left(\left(\widehat{E}(\mathfrak{m}_n)/\widehat{E}^{\pm}(\mathfrak{m}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p\right)^\vee\right) \\
&\quad \cdot \mathrm{Fitt}_{\Lambda_n}\left(\mathrm{Sel}^{\pm}(\mathbb{Q}_n, E[p^\infty])^\vee\right) \\
&\subseteq \mathrm{Fitt}_{\Lambda_n}\left(\left(\frac{E(\mathbb{Q}_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}{E^{\pm}(\mathbb{Q}_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}\right)^\vee /\ker(\iota^{\pm})\right) \\
&\quad \cdot \mathrm{Fitt}_{\Lambda_n}\left(\mathrm{Sel}^{\pm}(\mathbb{Q}_n, E[p^\infty])^\vee\right) \\
&\subseteq \mathrm{Fitt}_{\Lambda_n}\left(\mathrm{Sel}(\mathbb{Q}_n, E[p^\infty])^\vee\right).
\end{aligned}$$

By Corollary 3.10, we have

$$\left(\widetilde{\omega}_n^{\mp} \cdot L_p^{\mp}(\mathbb{Q}_\infty, f) \pmod{\omega_n}\right) \subseteq \mathrm{Fitt}_{\Lambda_n}\left(\mathrm{Sel}(\mathbb{Q}_n, E[p^\infty])^\vee\right).$$

Then Theorem 1.14 immediately follows from Proposition 1.11. Notably, the weak main conjecture of Mazur–Tate holds.

## 5 Towards the Strong Main Conjecture

The goal of this section is to prove the inclusion

$$\mathrm{Fitt}_{\Lambda_n}\left(\mathrm{Err}_n\right)\cdot\mathrm{Fitt}_{\Lambda_n}\left(\mathrm{Sel}(\mathbb{Q}_n, E[p^\infty])^\vee\right)\subseteq\left(\theta_n(f), \nu_{n-1,n}\left(\theta_{n-1}(f)\right)\right)$$

in Theorem 1.18. Note that the inclusion gives us a lower bound of Selmer groups (up to some error). Throughout this section, we assume

(1) $\overline{\rho}$ is surjective ($\Rightarrow$ $E$ is automatically non-CM),
(2) $p$ does not divide $\mathrm{Tam}(E)$, and
(3) the $\pm$-main conjectures (Conjecture 3.5).

### 5.1 Kato's main conjecture and fine Selmer groups

Let $j : \mathrm{Spec}(\mathbb{Q}_n) \to \mathrm{Spec}(\mathcal{O}_{\mathbb{Q}_n}[1/p])$ be the natural map. Let

$$\mathbb{H}^i_{\mathrm{glob}}(T) := \varprojlim_n \mathrm{H}^i_{\acute{e}t}\left(\mathrm{Spec}(\mathcal{O}_{\mathbb{Q}_n}[1/p]), j_*T\right), \qquad \mathbb{H}^i_{\mathrm{glob}}(V) := \mathbb{H}^i_{\mathrm{glob}}(T)\otimes\mathbb{Q}_p,$$

where $\mathrm{H}^i_{\acute{e}t}(\mathrm{Spec}(\mathcal{O}_{\mathbb{Q}_n}[1/p]), j_*T)$ is the étale cohomology group. It is well known that $\mathbb{H}^1_{\mathrm{glob}}(T) \simeq \varprojlim_n \mathrm{H}^1(\mathbb{Q}_\Sigma/\mathbb{Q}_n, T)$. See [13, §6] and [12, Proposition 7.1.(i)] for details.

The following theorem is due to Kato ([7, Theorem 12.4.(1) and (3)]).

**Theorem 5.1.** Assume that $\overline{\rho}$ is surjective. Then

(1) $\mathbb{H}^2_{\mathrm{glob}}(T)$ is a finitely generated torsion module over $\Lambda$.
(2) $\mathbb{H}^1_{\mathrm{glob}}(T)$ is free of rank one over $\Lambda$.

We recall the Iwasawa main conjecture without $p$-adic zeta functions à la Kato and Perrin-Riou ([7, Conjecture 12.10]).

**Conjecture 5.2** (Kato's main conjecture).

$$\mathrm{char}_\Lambda\left(\left(\mathbb{H}^1_{\mathrm{glob}}(T)/\Lambda\mathbf{z}_{\mathrm{Kato}}\right)_{\mathrm{tors}}\right) = \mathrm{char}_\Lambda\left(\mathbb{H}^2_{\mathrm{glob}}(T)\right),$$

where $M_{\mathrm{tors}}$ is the $\Lambda$-torsion submodule of $M$.

Note that we crucially use Conjecture 5.2 in the argument.

**Remark 5.3.**

(1) If $a_p(E) = 0$, then Kato's main conjecture (Conjecture 5.2) and the ±-main conjectures (Conjecture 3.5) are equivalent due to [12, Theorem 7.4].

(2) Also, $\mathbb{H}^2_{\mathrm{glob}}(T)$ and $\mathrm{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^\vee$ are pseudo-isomorphic as $\Lambda$-modules. See [13, §6] and [12, Theorem 7.1.ii)] for details.

### 5.2 Selmer groups and fine Selmer groups in finite layers

Let

$$\mathcal{Y}'_n := \operatorname{coker}\left(\mathbb{H}^1_{\mathrm{glob}}(T)_{\Gamma_n} \to \frac{\mathrm{H}^1(\mathbb{Q}_{n,p}, T)}{E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p}\right),$$

$$\mathcal{Y}_n := \operatorname{coker}\left(\mathrm{H}^1(\mathbb{Q}_\Sigma/\mathbb{Q}_n, T) \to \frac{\mathrm{H}^1(\mathbb{Q}_{n,p}, T)}{E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p}\right),$$

and

$$\mathcal{Z}_n := \operatorname{im}\left(\mathrm{H}^1(\mathbb{Q}_\Sigma/\mathbb{Q}_n, T) \to \frac{\mathrm{H}^1(\mathbb{Q}_{n,p}, T)}{E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p}\right).$$

Consider the following commutative diagram

$$\begin{tikzcd}
& \ker g_n \arrow[r] \arrow[d] & 0 \arrow[r] \arrow[d] & \ker f_n \arrow[d] & \\
& \left(\mathbb{H}^1_{\mathrm{glob}}(T)\right)_{\Gamma_n} \arrow[r] \arrow[d, "g_n"'] & \frac{\mathrm{H}^1(\mathbb{Q}_{n,p},T)}{E(\mathbb{Q}_{n,p})\otimes\mathbb{Z}_p} \arrow[r] \arrow[d, "\simeq"] & \mathcal{Y}'_n \arrow[r] \arrow[d, "f_n"] & 0 \\
0 \arrow[r] & \mathcal{Z}_n \arrow[r] \arrow[d] & \frac{\mathrm{H}^1(\mathbb{Q}_{n,p},T)}{E(\mathbb{Q}_{n,p})\otimes\mathbb{Z}_p} \arrow[r] \arrow[d] & \mathcal{Y}_n \arrow[r] \arrow[d] & 0 \\
& \operatorname{coker} g_n \arrow[r] & 0 \arrow[r] & 0 &
\end{tikzcd} \tag{5.1}$$

with

$$\ker f_n \simeq \operatorname{coker} g_n$$

by snake lemma.

**Remark 5.4.** Here, coker $g_n$ is exactly $\mathrm{Err}_n$. We use the notation coker $g_n$ in this and the next sections.

Let $\mathcal{Y}'_n/\mathrm{coker}\, g_n := \mathcal{Y}'_n/\ker f_n \subseteq \mathcal{Y}_n$. Then we have

$$\mathrm{Fitt}_{\Lambda_n}\left(\mathcal{Y}_n\right) \subseteq \mathrm{Fitt}_{\Lambda_n}\left(\mathcal{Y}'_n/\mathrm{coker}\, g_n\right)$$

by Lemma A.10. Using the Poitou–Tate sequence ([27, A.3.2.Proposition], [12, (7.18)]), we have the following exact sequence with splitting:

$$\begin{tikzcd}
\mathrm{H}^1(\mathbb{Q}_\Sigma/\mathbb{Q}_n, T) \arrow[r] & \frac{\mathrm{H}^1(\mathbb{Q}_{n,p},T)}{E(\mathbb{Q}_{n,p})\otimes\mathbb{Z}_p} \arrow[rr] \arrow[dr] & & \mathrm{Sel}(\mathbb{Q}_n, E[p^\infty])^\vee \arrow[r] & \mathrm{Sel}_0(\mathbb{Q}_n, E[p^\infty])^\vee \arrow[r] & 0 \\
& & \mathcal{Y}_n \arrow[ur] \arrow[dr] & & & \\
& 0 \arrow[ur] & & 0. & &
\end{tikzcd} \tag{5.2}$$

### 5.3 A presentation of the difference between Selmer groups and fine Selmer groups

It would be desirable to compute a presentation matrix of $\mathcal{Y}_n$ from the following exact sequence:

$$\mathrm{H}^1(\mathbb{Q}_\Sigma/\mathbb{Q}_n, T) \longrightarrow \frac{\mathrm{H}^1(\mathbb{Q}_{n,p},T)}{E(\mathbb{Q}_{n,p})\otimes\mathbb{Z}_p} \longrightarrow \mathcal{Y}_n \longrightarrow 0.$$

Unfortunately, it seems out of reach with current techniques; instead, we compute a slightly easier version, a presentation matrix of $\mathcal{Y}'_n$ from the following exact sequence:

$$\mathbb{H}^1_{\mathrm{glob}}(T)_{\Gamma_n} \longrightarrow \frac{\mathrm{H}^1(\mathbb{Q}_{n,p},T)}{E(\mathbb{Q}_{n,p})\otimes\mathbb{Z}_p} \longrightarrow \mathcal{Y}'_n \longrightarrow 0.$$

We regard $\mathcal{Y}'_n$ as the quotient of $\mathrm{H}^1(\mathbb{Q}_{n,p}, T)$ by local constraint $E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p$ and global constraint $\mathbb{H}^1_{\mathrm{glob}}(T)_{\Gamma_n}$.

#### 5.3.1 *The generators*

Let $\mathbb{H}^1_{\mathrm{loc}}(T)$ be the local Iwasawa cohomology group (defined in Theorem 3.2). Since $E$ is supersingular at $p$, $E[p]$ is irreducible as a $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-module. Then $\mathbb{H}^1_{\mathrm{loc}}(T)$ is free of rank 2 over $\Lambda$ since $\mathrm{H}^1(\mathbb{Q}_p, T)$ is free of rank 2 over $\mathbb{Z}_p$.

**Proposition 5.5** ([18, Proposition 1.2]). Let $\mathrm{Col} := \mathrm{Col}^+ \oplus \mathrm{Col}^-$. The following sequence:

$$0 \longrightarrow \mathbb{H}^1_{\mathrm{loc}}(T) \xrightarrow{\quad\mathrm{Col}\quad} \Lambda \oplus \Lambda \xrightarrow{\ r\ } \mathbb{Z}_p \longrightarrow 0$$

is exact, where $r(h(X), k(X)) := h(0) - \frac{p-1}{2} \cdot k(0)$.

We pick a $\Lambda$-basis $(e_1, e_2)$ of $\mathbb{H}^1_{\mathrm{loc}}(T) = \ker(r)$ by

$$\mathrm{Col}(e_1) = \left(\frac{p-1}{2}, 1\right), \qquad \mathrm{Col}(e_2) = (X, 0).$$

Then

$$\begin{aligned}\mathbb{H}^1_{\mathrm{loc}}(T) &= \Lambda e_1 \oplus \Lambda e_2 \\ &\simeq \Lambda \mathrm{Col}(e_1) \oplus \Lambda \mathrm{Col}(e_2) \\ &\subseteq \Lambda \oplus \Lambda.\end{aligned}$$

By the irreducibility of $E[p]$ as a $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-module, we have

$$\begin{aligned}\mathbb{H}^1_{\mathrm{loc}}(T)_{\Gamma_n} &= \mathrm{H}^1(\mathbb{Q}_{n,p}, T) \\ &= \Lambda_n e_1 \oplus \Lambda_n e_2.\end{aligned}$$

5.3.2 *The local constraint*

Consider the exact sequence

$$\begin{tikzcd}
0 \arrow[r] & \dfrac{\mathrm{H}^1(\mathbb{Q}_{n,p}, T)}{E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p} \arrow[r] \arrow[dr, hook] & \dfrac{\mathrm{H}^1(\mathbb{Q}_{n,p}, T)}{\ker(\mathrm{Col}^+_n)} \oplus \dfrac{\mathrm{H}^1(\mathbb{Q}_{n,p}, T)}{\ker(\mathrm{Col}^-_n)} \arrow[r] \arrow[d, "\mathrm{Col}_n := \mathrm{Col}^+_n \oplus \mathrm{Col}^-_n", "\simeq"'] & \dfrac{\mathrm{H}^1(\mathbb{Q}_p, T)}{E(\mathbb{Q}_p) \otimes \mathbb{Z}_p} \arrow[r] & 0 \\
& & \Lambda_n/\omega^-_n \oplus \Lambda_n/\omega^+_n. & &
\end{tikzcd}$$

We investigate the image of $e_1$ and $e_2$ in $\Lambda_n/\omega^-_n \oplus \Lambda_n/\omega^+_n$ under $\mathrm{Col}_n$. Then we naturally obtain the following relations of $\frac{\mathrm{H}^1(\mathbb{Q}_{n,p}, T)}{E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p}$:

$$\begin{aligned}\widetilde{\omega}^-_n \cdot e_2 &= (\widetilde{\omega}^-_n X, 0) \\ &= (\omega^-_n, 0) \\ &= (0,0) \in \Lambda_n/\omega^-_n \oplus \Lambda_n/\omega^+_n\end{aligned}$$

$$\begin{aligned}\omega^+_n \cdot e_1 - \frac{p-1}{2} \cdot \widetilde{\omega}^+_n \cdot e_2 &= \left(\omega^+_n \cdot \frac{p-1}{2}, \omega^+_n\right) - \left(\frac{p-1}{2} \cdot \widetilde{\omega}^+_n \cdot X, 0\right) \\ &= \left(0, \omega^+_n\right) \\ &= (0,0) \in \Lambda_n/\omega^-_n \oplus \Lambda_n/\omega^+_n.\end{aligned}$$

Also, since $E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p$ is generated by two elements over $\Lambda_n$ via a formal group argument as in [6, Proposition 4.11], we know that $\frac{\mathrm{H}^1(\mathbb{Q}_{n,p},T)}{E(\mathbb{Q}_{n,p})\otimes\mathbb{Z}_p}$ is the module with two generators $e_1, e_2$ and the above two relations (these relations are all).

### 5.3.3 *The global constraint*

Due to Theorem 5.1.(2), we have

$$\mathbb{H}^1_{\mathrm{glob}}(T) \simeq \Lambda$$

and let $b$ be a $\Lambda$-generator of $\mathbb{H}^1_{\mathrm{glob}}(T)$. Then $b$ is also a $\Lambda_n$-generator of $\mathbb{H}^1_{\mathrm{glob}}(T)_{\Gamma_n} \simeq \Lambda_n$. We write the image of $b$ by $(b_1, b_2)$ under the map

$$\begin{tikzcd}
\mathbb{H}^1_{\mathrm{glob}}(T) \arrow[r, "\mathrm{loc}"] & \mathbb{H}^1_{\mathrm{loc}}(T) \arrow[r, "\mathrm{Col}^+\oplus\mathrm{Col}^-"] & \Lambda \oplus \Lambda \\
b \arrow[rr, mapsto] & & (b_1, b_2).
\end{tikzcd}$$

Since

$$\frac{\mathrm{H}^1(\mathbb{Q}_{n,p}, T)}{E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p} \hookrightarrow \Lambda_n/\omega_n^- \oplus \Lambda_n/\omega_n^+,$$

we have

$$\mathcal{Y}'_n = \frac{\mathrm{H}^1(\mathbb{Q}_{n,p}, T)}{E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p + \mathrm{im}\,\mathbb{H}^1_{\mathrm{glob}}(T)} \hookrightarrow \frac{\Lambda_n/\omega_n^- \oplus \Lambda_n/\omega_n^+}{(b_1, b_2)},$$

where $\mathrm{im}\,\mathbb{H}^1_{\mathrm{glob}}(T)$ is the image of $\mathbb{H}^1_{\mathrm{glob}}(T)$ in $\mathrm{H}^1(\mathbb{Q}_{n,p}, T)$ and it is a quotient of $\mathbb{H}^1_{\mathrm{glob}}(T)_{\Gamma_n}$. Then

$$\begin{aligned}
b_2 e_1 - \frac{b_1 - \frac{p-1}{2} b_2}{X} e_2 &= b_2 (\frac{p-1}{2}, 1) + \frac{b_1 - \frac{p-1}{2} b_2}{X} (X, 0) \\
&= (b_1, b_2) \\
&= (0, 0) \in \mathcal{Y}'_n.
\end{aligned}$$

### 5.3.4 *A presentation matrix*

Using all the above discussion on generators and relations arising from

$$\begin{tikzcd}
\mathbb{H}^1_{\mathrm{glob}}(T)_{\Gamma_n} \arrow[r] & \frac{\mathrm{H}^1(\mathbb{Q}_{n,p},T)}{E(\mathbb{Q}_{n,p})\otimes\mathbb{Z}_p} \arrow[r] & \mathcal{Y}'_n \arrow[r] & 0,
\end{tikzcd}$$

we know there are two generators and three relations. Now we describe a presentation matrix $A$ of $\mathcal{Y}'_n$ over $\Lambda_n$

$$(\Lambda_n)^{\oplus 3} \xrightarrow{A} \Lambda \mathrm{Col}(e_1) \oplus \Lambda \mathrm{Col}(e_2) \longrightarrow \mathcal{Y}'_n \longrightarrow 0$$

by

$$A = \begin{pmatrix} 0 & \omega_n^+ & b_2 \\ \widetilde{\omega}_n^- & -\frac{p-1}{2}\widetilde{\omega}_n^+ & \frac{b_1 - \frac{p-1}{2} b_2}{X} \end{pmatrix}.$$

A direct computation of minors of the above matrix $A$ yields the following statement.

**Proposition 5.6.**

$$\mathrm{Fitt}_{\Lambda_n}(\mathcal{Y}'_n) = (\widetilde{\omega}_n^+ b_1, \widetilde{\omega}_n^- b_2).$$

### 5.4 Putting it all together

Consider the exact sequence

$$0 \longrightarrow \left(\mathrm{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^\vee\right)_{\mathrm{mft}} \longrightarrow \mathrm{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^\vee \longrightarrow \mathcal{S} \longrightarrow 0,$$

where $M_{\mathrm{mft}}$ is the maximal finite torsion $\Lambda$-submodule of $M$. Then we have

$$\mathrm{char}_\Lambda \left(\left(\mathrm{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^\vee\right)_{\mathrm{mft}}\right) \cdot \mathrm{char}_\Lambda (\mathcal{S}) = \mathrm{char}_\Lambda \left(\mathrm{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^\vee\right).$$

Since $\mathrm{char}_\Lambda \left(\left(\mathrm{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^\vee\right)_{\mathrm{mft}}\right)$ is trivial and the projective dimension of $\mathcal{S}$ over $\Lambda$ is $\leq 1$ (i.e., $\mathrm{pd}_\Lambda \mathcal{S} \leq 1$), we have

$$\begin{aligned} \mathrm{Fitt}_\Lambda (\mathcal{S}) &= \mathrm{char}_\Lambda (\mathcal{S}) \\ &= \mathrm{char}_\Lambda \left(\mathrm{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^\vee\right) \\ &= \mathrm{char}_\Lambda \left(\mathbb{H}^1_{\mathrm{glob}}(T)/\Lambda \mathbf{z}_{\mathrm{Kato}}\right), \end{aligned}$$

where Lemma A.7 and Conjecture 5.2 are used to obtain the 1st and the 3rd equalities, respectively. Then, by Kato's main conjecture (Conjecture 5.2) again, we have

$$\mathrm{Fitt}_\Lambda (\mathcal{S}) = (c) \subseteq \Lambda,$$

where $\mathbf{z}_{\mathrm{Kato}} = c \cdot b$ in $\mathbb{H}^1_{\mathrm{glob}}(T)$ with $b$ the chosen $\Lambda$-generator of $\mathbb{H}^1_{\mathrm{glob}}(T)$ in Section 5.3.3.

By the control theorem for fine Selmer groups ([13, Lemma 4.2 and Remark 4.4]), we have

$$\mathrm{Sel}_0(\mathbb{Q}_n, E[p^\infty])^\vee \simeq \left(\mathrm{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^\vee\right)_{\Gamma_n}.$$

Consider two exact sequences with compatibility

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{Y}_n \arrow[r] \arrow[d, hook] & \mathrm{Sel}(\mathbb{Q}_n, E[p^\infty])^\vee \arrow[r] \arrow[d, equal] & \left(\mathrm{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^\vee\right)_{\Gamma_n} \arrow[r] \arrow[d, two heads] & 0 \\
0 \arrow[r] & \mathcal{A}_n \arrow[r] & \mathrm{Sel}(\mathbb{Q}_n, E[p^\infty])^\vee \arrow[r] & \mathcal{S}_{\Gamma_n} \arrow[r] & 0,
\end{tikzcd}$$

where $\mathcal{A}_n$ is defined to be the kernel of the map $\mathrm{Sel}(\mathbb{Q}_n, E[p^\infty])^\vee \to \mathcal{S}_{\Gamma_n}$.

Since $\mathrm{pd}_\Lambda \mathcal{S} \le 1$, we have $\mathcal{S}$ admits a presentation by a square matrix over $\Lambda$. Thus, $\mathcal{S}_{\Gamma_n}$ also admits a presentation by a square matrix over $\Lambda_n$. Then we have

$$\begin{aligned}
\mathrm{Fitt}_{\Lambda_n}\left(\mathrm{Sel}(\mathbb{Q}_n, E[p^\infty])^\vee\right) &= \mathrm{Fitt}_{\Lambda_n}\left(\mathcal{A}_n\right) \cdot \mathrm{Fitt}_{\Lambda_n}\left(\mathcal{S}_{\Gamma_n}\right) \\
&\subseteq \mathrm{Fitt}_{\Lambda_n}\left(\mathcal{Y}_n\right) \cdot \mathrm{Fitt}_{\Lambda_n}\left(\mathcal{S}_{\Gamma_n}\right),
\end{aligned}$$

where Lemma A.4 and Lemma A.10 are used to obtain the 1st equality and the 2nd inclusion, respectively. Multiplying $\mathrm{Fitt}_{\Lambda_n}\left(\mathrm{coker}\, g_n\right)$, we have

$$\begin{aligned}
\mathrm{Fitt}_{\Lambda_n}\left(\mathrm{coker}\, g_n\right) \cdot \mathrm{Fitt}_{\Lambda_n}\left(\mathrm{Sel}(\mathbb{Q}_n, E[p^\infty])^\vee\right) &\subseteq \mathrm{Fitt}_{\Lambda_n}\left(\mathrm{coker}\, g_n\right) \cdot \mathrm{Fitt}_{\Lambda_n}\left(\mathcal{Y}_n\right) \cdot \mathrm{Fitt}_{\Lambda_n}\left(\mathcal{S}_{\Gamma_n}\right) \\
&\subseteq \mathrm{Fitt}_{\Lambda_n}\left(\mathrm{coker}\, g_n\right) \cdot \mathrm{Fitt}_{\Lambda_n}\left(\mathcal{Y}'_n/\mathrm{coker}\, g_n\right) \\
&\quad \cdot \mathrm{Fitt}_{\Lambda_n}\left(\mathcal{S}_{\Gamma_n}\right) \\
&\subseteq \mathrm{Fitt}_{\Lambda_n}\left(\mathcal{Y}'_n\right) \cdot \mathrm{Fitt}_{\Lambda_n}\left(\mathcal{S}_{\Gamma_n}\right) \\
&= \left(\widetilde{\omega}^+_n b_1, \widetilde{\omega}^-_n b_2\right) \cdot (c) \\
&= \left(\widetilde{\omega}^+_n \mathrm{Col}^+(\mathrm{loc}\, b), \widetilde{\omega}^-_n \mathrm{Col}^-(\mathrm{loc}\, b)\right) \cdot (c) \\
&= \left(\widetilde{\omega}^+_n \mathrm{Col}^+(c \cdot \mathrm{loc}\, b), \widetilde{\omega}^-_n \mathrm{Col}^-(c \cdot \mathrm{loc}\, b)\right) \\
&= \left(\widetilde{\omega}^+_n \mathrm{Col}^+(\mathrm{loc}\, \mathbf{z}_{\mathrm{Kato}}), \widetilde{\omega}^-_n \mathrm{Col}^-(\mathrm{loc}\, \mathbf{z}_{\mathrm{Kato}})\right) \\
&= \left(\widetilde{\omega}^+_n L^+_p(\mathbb{Q}_\infty, f), \widetilde{\omega}^-_n L^-_p(\mathbb{Q}_\infty, f)\right).
\end{aligned}$$

## 6 Vanishing of $\mathbf{Err}_n$

This section is entirely devoted to prove the following proposition in order to obtain Theorem 1.20. We keep all the assumptions in Section 5 in this section.

**Proposition 6.1.** If

(fineNF) $\mathrm{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^\vee$ has no nontrivial finite $\Lambda$-submodule, and

(III) if $\mathrm{char}_\Lambda\left(\mathrm{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^\vee\right) \subseteq \left(\Phi_n(1+X)\right)$, then $\mathrm{rk}_\mathbb{Z} E(\mathbb{Q}_n) > \mathrm{rk}_\mathbb{Z} E(\mathbb{Q}_{n-1})$ (if $n = 0$, then $\Phi_0(1+X) = X$ and this inequality means $\mathrm{rk}_\mathbb{Z} E(\mathbb{Q}) > 0$),

then $\mathrm{coker}\, g_n = 0$.

### 6.1 Reduction

We recall the following exact sequence ([18, (Proof of) Proposition 3.4]):

$$0 \longrightarrow \frac{\mathbb{H}^1_{\mathrm{loc}}(T)}{\mathrm{loc}\ \mathbb{H}^1_{\mathrm{glob}}(T)} \longrightarrow \mathrm{Sel}(\mathbb{Q}_\infty, E[p^\infty])^\vee \longrightarrow \mathrm{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^\vee \longrightarrow 0. \qquad (6.1)$$

By taking the $\Gamma_n$-coinvariant of the above sequence, we have the exact sequence

$$0 \longrightarrow C_n \longrightarrow \frac{\mathrm{H}^1(\mathbb{Q}_{n,p}, T)}{\mathrm{im}\ \mathbb{H}^1_{\mathrm{glob}}(T)} \longrightarrow \left(\mathrm{Sel}(\mathbb{Q}_\infty, E[p^\infty])^\vee\right)_{\Gamma_n} \longrightarrow \mathrm{Sel}_0(\mathbb{Q}_n, E[p^\infty])^\vee \longrightarrow 0, \qquad (6.2)$$

where

$$C_n := \mathrm{coker}\left(\mathrm{Sel}(\mathbb{Q}_\infty, E[p^\infty])^{\vee,\Gamma_n} \to \mathrm{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^{\vee,\Gamma_n}\right)$$

and $\mathrm{im}\ \mathbb{H}^1_{\mathrm{glob}}(T) := \mathrm{im}\left(\mathbb{H}^1_{\mathrm{glob}}(T) \to \mathrm{H}^1(\mathbb{Q}_{n,p}, T)\right)$. We also have an exact sequence

$$0 \longrightarrow \mathcal{Z}_n \longrightarrow \frac{\mathrm{H}^1(\mathbb{Q}_{n,p}, T)}{E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p} \longrightarrow \mathrm{Sel}(\mathbb{Q}_n, E[p^\infty])^\vee \longrightarrow \mathrm{Sel}_0(\mathbb{Q}_n, E[p^\infty])^\vee \longrightarrow 0$$

from Sequence (5.2) and the definition of $\mathcal{Z}_n$.

Let $\pi_{\mathrm{glob},n} : \mathrm{H}^1(\mathbb{Q}_{n,p}, T) \to \dfrac{\mathrm{H}^1(\mathbb{Q}_{n,p}, T)}{\mathrm{im}\ \mathbb{H}^1_{\mathrm{glob}}(T)}$ be the natural projection and

$$\widetilde{C}_n := \pi^{-1}_{\mathrm{glob},n}(C_n) \subseteq \mathrm{H}^1(\mathbb{Q}_{n,p}, T)$$

be the inverse image of $C_n$ with respect to $\pi_{\mathrm{glob},n}$, and it obviously contains $\mathrm{im}\ \mathbb{H}^1_{\mathrm{glob}}(T)$.

Considering the following commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & \widetilde{C}_n \arrow[r] \arrow[d, two heads] & \mathrm{H}^1(\mathbb{Q}_{n,p}, T) \arrow[d, two heads] \arrow[dr] & E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p \arrow[d] & & \\
0 \arrow[r] & C_n \arrow[r] & \dfrac{\mathrm{H}^1(\mathbb{Q}_{n,p}, T)}{\mathrm{im}\ \mathbb{H}^1_{\mathrm{glob}}(T)} \arrow[r] & \left(\mathrm{Sel}(\mathbb{Q}_\infty, E[p^\infty])^\vee\right)_{\Gamma_n} \arrow[r] \arrow[d, two heads] & \mathrm{Sel}_0(\mathbb{Q}_n, E[p^\infty])^\vee \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & \mathcal{Z}_n \arrow[r] & \dfrac{\mathrm{H}^1(\mathbb{Q}_{n,p}, T)}{E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p} \arrow[r] & \mathrm{Sel}(\mathbb{Q}_n, E[p^\infty])^\vee \arrow[r] & \mathrm{Sel}_0(\mathbb{Q}_n, E[p^\infty])^\vee \arrow[r] & 0,
\end{tikzcd}$$

it is observed that $\widetilde{C}_n$ surjects $\mathcal{Z}_n$ under the natural quotient map

$$\mathrm{H}^1(\mathbb{Q}_{n,p}, T) \twoheadrightarrow \frac{\mathrm{H}^1(\mathbb{Q}_{n,p}, T)}{E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p}$$

since

$$\left(\frac{\mathrm{H}^1(\mathbb{Q}_{n,p}, T)}{\widetilde{C}_n}\right) \Big/ \left(E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p\right) = \left(\frac{\mathrm{H}^1(\mathbb{Q}_{n,p}, T)}{E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p}\right) \Big/ \mathcal{Z}_n$$

as a subgroup of $\mathrm{Sel}(\mathbb{Q}_n, E[p^\infty])^\vee$.

Consider the composition of surjective maps

$$\widetilde{C}_n \twoheadrightarrow \mathcal{Z}_n \twoheadrightarrow \mathrm{coker}\ g_n$$

and then it factors through $C_n$ by definition. Let

$$C_n' := C_n \cap \mathrm{im}\left(E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p \to \frac{\mathrm{H}^1(\mathbb{Q}_{n,p}, T)}{\mathrm{im}\ \mathbb{H}^1_{\mathrm{glob}}(T)}\right) \subseteq \frac{\mathrm{H}^1(\mathbb{Q}_{n,p}, T)}{\mathrm{im}\ \mathbb{H}^1_{\mathrm{glob}}(T)}.$$

Then Sequence (6.2) and the following exact sequence:

$$0 \longrightarrow \mathrm{coker}\ g_n \longrightarrow \frac{\mathrm{H}^1(\mathbb{Q}_{n,p}, T)}{E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p + \mathrm{im}\ \mathbb{H}^1_{\mathrm{glob}}(T)} \longrightarrow \mathrm{Sel}(\mathbb{Q}_n, E[p^\infty])^\vee \longrightarrow \mathrm{Sel}_0(\mathbb{Q}_n, E[p^\infty])^\vee \longrightarrow 0$$

show that $C_n' = \ker\left(C_n \to \mathrm{coker}\ g_n\right)$. Thus, we have the exact sequence

$$0 \longrightarrow C_n' \xrightarrow{\varphi_n} C_n \longrightarrow \mathrm{coker}\ g_n \longrightarrow 0. \tag{6.3}$$

We can easily observe the following statement.

**Proposition 6.2.** The following statements are equivalent:

(1) coker $g_n = 0$.

(2) $\varphi_n : C'_n \to C_n$ is an isomorphism.

(3) All the classes in $C_n$ lie in $\overline{E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p} := \mathrm{im}\left( E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p \to \dfrac{\mathrm{H}^1(\mathbb{Q}_{n,p}, T)}{\mathrm{im}\, \mathbb{H}^1_{\mathrm{glob}}(T)} \right)$.

In particular, if $C_n = 0$, then coker $g_n = 0$.

From now on, we prove Proposition 6.1 using induction on $n$.

### 6.2 When the rank does not grow

In this subsection, we assume that

**Assumption 6.3.** $\Phi_n(1+X)$ does not divide a generator of $\mathrm{char}_\Lambda\left(\mathrm{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^\vee\right)$.

If $n = 0$, then

$$\mathrm{Sel}_0\left(\mathbb{Q}_\infty, E[p^\infty]\right)^{\vee,\Gamma} = 0.$$

Thus by the definition of $C_0$, we have $C_0 = 0$, which implies that coker $g_0 = 0$.

Now we suppose $n > 0$.

**Lemma 6.4.** Let $M$ be a finitely generated torsion $\Lambda$-module with no nontrivial finite $\Lambda$-submodule. Suppose that $\Phi_n(1+X)$ does not divide a generator of $\mathrm{char}_\Lambda(M)$. Then $M^{\Gamma_{n-1}} = M^{\Gamma_n}$.

**Proof.** We may assume $M = M^{\Gamma_n}$, that is, $\omega_n M = 0$. Using the structure theorem for finitely generated $\Lambda$-modules, $M$ is a submodule of $M'$ of finite index with

$$M' \simeq \bigoplus_{i=1}^{m} \Lambda/f_i\Lambda.$$

Since $\omega_n M = 0$, we also have $\omega_n M' = 0$. It shows that each $f_i$ divides $\omega_n$. Since $\Phi_n(1+X)$ does not divide $\mathrm{char}_\Lambda(M') = (\prod_{i=1}^{m} f_i)$, each $f_i$ is prime to $\Phi_n(1+X)$. Thus, each $f_i$ divides $\omega_{n-1} = \omega_n/\Phi_n(1+X)$, and then $\omega_{n-1}M' = 0$. Hence, $\omega_{n-1}M = 0$. ■

By Lemma 6.4, we have

$$\mathrm{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^{\vee,\Gamma_{n-1}} \simeq \mathrm{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^{\vee,\Gamma_n}.$$

Note that Assumption (fineNF) is used here. Thus, the natural map $C_{n-1} \to C_n$ is surjective. Then we have the following commutative diagram:

$$\begin{tikzcd}
C_n \arrow[r, two heads] & \operatorname{coker} g_n \\
C_{n-1} \arrow[u, two heads] \arrow[r, two heads] & \operatorname{coker} g_{n-1} \arrow[u]
\end{tikzcd}$$

and $\operatorname{coker} g_{n-1} = 0$ by the induction hypothesis. Thus, the lower horizontal map $C_{n-1} \to \operatorname{coker} g_{n-1}$ becomes the zero map and then $\operatorname{coker} g_n = 0$.

### 6.3 When the rank grows

In this subsection, we assume that

**Assumption 6.5.** $\Phi_n(1+X)$ divides a generator of $\operatorname{char}_\Lambda\left(\operatorname{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^\vee\right)$.

If $n = 0$, then Assumption (III) implies $\operatorname{rk}_\mathbb{Z} E(\mathbb{Q}) > 0$, so the natural map

$$E(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to E(\mathbb{Q}_p) \otimes \mathbb{Q}_p/\mathbb{Z}_p \tag{6.4}$$

is surjective.

Let

$$M_{\Phi_n} := M/\Phi_n(1+X)M,$$

where $M$ is a $\Lambda_n$-module and $\Phi_n(1+X) \in \Lambda_n$.

Now we suppose $n > 0$. By Assumption (III), we have

$$\operatorname{rk}_\mathbb{Z} E(\mathbb{Q}_n) > \operatorname{rk}_\mathbb{Z} E(\mathbb{Q}_{n-1}).$$

Then the map

$$\left(E(\mathbb{Q}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p\right)_{\Phi_n} \to \left(E(\mathbb{Q}_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p\right)_{\Phi_n} \tag{6.5}$$

is surjective.

First, we explicitly write down the connecting map

$$C_n \to \frac{\mathrm{H}^1(\mathbb{Q}_{n,p}, T)}{\operatorname{im} \mathbb{H}^1_{\mathrm{glob}}(T)}$$

that is obtained by taking the $\Gamma_n$-coinvariant of Sequence (6.1). Let

$$[f] \in C_n = \operatorname{coker}\left(\mathrm{Sel}\big(\mathbb{Q}_\infty, E[p^\infty]\big)^{\vee,\Gamma_n} \to \mathrm{Sel}_0\big(\mathbb{Q}_\infty, E[p^\infty]\big)^{\vee,\Gamma_n}\right)$$

with a representative $f \in \mathrm{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^\vee[\omega_n] \subseteq \mathrm{Sel}_0(\mathbb{Q}_\infty, E[p^\infty])^\vee$. Via Sequence (6.1), we lift $f$ to $\widetilde{f} \in \mathrm{Sel}(\mathbb{Q}_\infty, E[p^\infty])^\vee$. Also, since $\omega_n \widetilde{f}$ maps to $\omega_n f = 0$ in Sequence (6.1), we have

$$\omega_n \widetilde{f} \in \frac{\mathbb{H}^1_{\mathrm{loc}}(T)}{\mathrm{loc}\ \mathbb{H}^1_{\mathrm{glob}}(T)} \subseteq \mathrm{Sel}\big(\mathbb{Q}_\infty, E[p^\infty]\big)^\vee.$$

This means that there exists an element $P \in \mathbb{H}^1_{\mathrm{loc}}(T)$ such that

$$\omega_n \widetilde{f}(x) = \langle P, j(x)\rangle$$

for any $x \in \mathrm{Sel}(\mathbb{Q}_\infty, E[p^\infty])$, where $j : \mathrm{Sel}(\mathbb{Q}_\infty, E[p^\infty]) \to \mathrm{H}^1(\mathbb{Q}_{\infty,p}, E[p^\infty])$ is the natural localization map and $\langle -, - \rangle$ is the local Tate pairing between $\mathbb{H}^1_{\mathrm{loc}}(T)$ and $\mathrm{H}^1(\mathbb{Q}_{\infty,p}, E[p^\infty])$. Putting $P_n := P \pmod{\omega_n} \in \mathrm{H}^1(\mathbb{Q}_{n,p}, T)$, we have the following diagram:

$$\begin{tikzcd}
\mathbb{H}^1_{\mathrm{loc}}(T) \arrow[r, two heads] \arrow[d, two heads] & \mathrm{H}^1(\mathbb{Q}_{n,p}, T) \arrow[d, two heads] & P \arrow[r, mapsto] \arrow[d, mapsto] & P_n \arrow[d, mapsto] \\
\frac{\mathbb{H}^1_{\mathrm{loc}}(T)}{\mathrm{loc}\ \mathbb{H}^1_{\mathrm{glob}}(T)} \arrow[r, two heads] & \frac{\mathrm{H}^1(\mathbb{Q}_{n,p}, T)}{\mathrm{im}\ \mathbb{H}^1_{\mathrm{glob}}(T)} & \omega_n \widetilde{f} \arrow[r, mapsto] & \overline{P_n} := \omega_n \widetilde{f} \pmod{\omega_n}.
\end{tikzcd}$$

Note that $\overline{P_n} = \omega_n \widetilde{f} \pmod{\omega_n} \in \frac{\mathrm{H}^1(\mathbb{Q}_{n,p},T)}{\mathrm{im}\ \mathbb{H}^1_{\mathrm{glob}}(T)}$ is not necessarily zero since $\widetilde{f}$ may not be contained in $\frac{\mathbb{H}^1_{\mathrm{loc}}(T)}{\mathrm{loc}\ \mathbb{H}^1_{\mathrm{glob}}(T)}$. To sum up, the map

$$C_n \to \frac{\mathrm{H}^1(\mathbb{Q}_{n,p}, T)}{\mathrm{im}\ \mathbb{H}^1_{\mathrm{glob}}(T)}$$

is defined by $[f] \mapsto \overline{P_n}$.

Now we prove that $P_n \in E(\mathbb{Q}_{n,p}) \otimes \mathbb{Z}_p$ in $\mathrm{H}^1(\mathbb{Q}_{n,p}, T)$. By the local Tate duality, it suffices to check

$$\big\langle P_n, E(\mathbb{Q}_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \big\rangle = 0. \tag{6.6}$$

Suppose at first $n = 0$. Since

$$E(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \subseteq \mathrm{Sel}\big(\mathbb{Q}, E[p^\infty]\big) \subseteq \mathrm{Sel}\big(\mathbb{Q}_\infty, E[p^\infty]\big)[\omega_0],$$

we know $\langle P_0, E(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p\rangle = 0$. Since Map (6.4) is surjective, we also have $\langle P_0, E(\mathbb{Q}_p) \otimes \mathbb{Q}_p/\mathbb{Z}_p\rangle = 0$.

Next we consider the case $n > 0$. Consider the exact sequence

$$0 \longrightarrow E(\mathbb{Q}_{n-1,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow E(\mathbb{Q}_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \big(E(\mathbb{Q}_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p\big)_{\Phi_n} \longrightarrow 0. \tag{6.7}$$

By the induction hypothesis, we have coker $g_{n-1} = 0$. Thus, the map in Sequence (6.3)

$$\varphi_{n-1} : C'_{n-1} \to C_{n-1}$$

is an isomorphism, and also $P_{n-1} := P_n \pmod{\omega_{n-1}}$ is contained in $E(\mathbb{Q}_{n-1,p}) \otimes \mathbb{Z}_p$. Therefore,

$$\Big\langle P_n, E(\mathbb{Q}_{n-1,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \Big\rangle = 0. \tag{6.8}$$

By Sequence (6.7), we only need to show that

$$\Big\langle P_n, \Big(E(\mathbb{Q}_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p\Big)_{\Phi_n} \Big\rangle = 0 \tag{6.9}$$

in order to prove (6.6).

As in the case $n = 0$, $\omega_n \widetilde{f}$ vanishes on $E(\mathbb{Q}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ since

$$E(\mathbb{Q}_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \subseteq \mathrm{Sel}\big(\mathbb{Q}_n, E[p^\infty]\big) \subseteq \mathrm{Sel}\big(\mathbb{Q}_\infty, E[p^\infty]\big)[\omega_n].$$

Now we know that the homomorphism (6.5) is surjective, so $\omega_n \widetilde{f}$ vanishes also on $(E(\mathbb{Q}_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)_{\Phi_n}$, and we get Equation (6.9).

Sequence (6.7), Equation (6.8), and Equation (6.9) complete the proof of Equation (6.6).

## Acknowledgments

C.-H.K. thanks M.K. for introducing this subject; Robert Pollack for sharing his ideas, for helpful discussion, and for support; Takenori Kataoka for the suggestion to remove the Tamagawa number assumption; Shinichi Kobayashi for answering questions on ±-Selmer groups; Jaehoon Lee for careful reading of an earlier version; GilYoung Cheong, B.D. Kim, Myoungil Kim, Takahiro Kitajima, Meng Fai Lim, and Kazuto Ota for helpful discussions. C.-H.K. is partially supported by "Overseas Research Program for Young Scientists" through Korea Institute for Advanced Study (KIAS) and by Basic Science Research Program through the National Research Foundation of Korea (NRF-2018R1C1B6007009). M.K. thanks Ralph Greenberg and Robert Pollack for the discussion with them on the subject of this paper (held more than 10 years ago). He also thanks C.-H.K. heartily for letting him come back to this interesting subject through many discussions and questions. M.K. is partially supported by JSPS Core-to-core program, “Foundation of a Global Research Cooperative Center in Mathematics focused on Number Theory and Geometry”. We both thank to anonymous referees for careful reading and comments, which improve the clarification of the exposition significantly.

## Appendix

### A Lemmas on Fitting Ideals

All the modules in this section are finitely presented over their base rings. Let $R$ be a commutative ring with unity.

**Lemma A.1** [21, 1, Appendix]. Let $M \twoheadrightarrow N$ be a surjective map of $R$-modules. Then

$$\mathrm{Fitt}_R(M) \subseteq \mathrm{Fitt}_R(N).$$

**Lemma A.2** [21, 9, Appendix]. Let $0 \to M_1 \to M_2 \to M_3 \to 0$ be an exact sequence of $R$-modules. Then

$$\mathrm{Fitt}_R(M_1) \cdot \mathrm{Fitt}_R(M_3) \subseteq \mathrm{Fitt}_R(M_2).$$

**Lemma A.3** ([23, Theorem 22, Page 80]). Let $0 \to M_1 \to M_2 \to M_3 \to 0$ be an exact sequence of $R$-modules. Assume that $\mathrm{pd}_R M_3 \leq 1$. Then

$$\mathrm{Fitt}_R(M_1) \cdot \mathrm{Fitt}_R(M_3) = \mathrm{Fitt}_R(M_2).$$

**Lemma A.4.** Let $0 \to M_1 \to M_2 \to M_3 \to 0$ be an exact sequence of $R$-modules. Assume that $M_3$ has presentation by a square matrix. Then

$$\mathrm{Fitt}_R(M_1) \cdot \mathrm{Fitt}_R(M_3) = \mathrm{Fitt}_R(M_2).$$

**Proof.** Denote a presentation matrix of $M_i$ by $A_i$ for $i = 1, 2, 3$. In other words,

$$\begin{tikzcd}
R^{\oplus s} \arrow[r, "A_1"] & R^{\oplus r} \arrow[r] & M_1 \arrow[r] & 0 \\
R^{\oplus (s+m)} \arrow[r, "A_2"] & R^{\oplus (r+m)} \arrow[r] & M_2 \arrow[r] & 0 \\
R^{\oplus m} \arrow[r, "A_3"] & R^{\oplus m} \arrow[r] & M_3 \arrow[r] & 0
\end{tikzcd}$$

with $r \le s$. Then we have

$$A_2 = \left( \begin{array}{c|c} A_1 & * \\ \hline 0 & A_3 \end{array} \right) \in \mathrm{M}_{(r+m)\times(s+m)}(R).$$

Considering $(r+m) \times (r+m)$ minors of $A_2$, it is easy to see that the upper-triangular part $(*)$ of $A_2$ does not affect the determinants of the minors. Thus, the conclusion follows. ■

**Remark A.5.** If $R = \mathbb{Z}[G]$ with a finite abelian group $G$, for example, and $M$ is torsion with $\mathrm{pd}_R M \le 1$, then $\mathrm{Fitt}_R(M)$ is a principal ideal generated by a non-zero divisor. Thus, Lemma A.3 is slightly stronger than Lemma A.4 for this case.

**Lemma A.6** [21, 4, Appendix]. Let $M$ be a finitely presented $R$-module. If $I \subset R$ is an ideal, then

$$\mathrm{Fitt}_{R/I}(M/IM) = \pi\left(\mathrm{Fitt}_R(M)\right),$$

where $\pi : A \to A/I$ is the natural quotient map.

The following lemma is the key to replace characteristic ideals by Fitting ideals.

**Lemma A.7.** Let $M$ be a finitely generated torsion $\Lambda$-module. Assume that $M$ has no nontrivial finite $\Lambda$-submodule. Then

$$\mathrm{char}_\Lambda(M) = \mathrm{Fitt}_\Lambda(M).$$

**Proof.** Though several proofs of this lemma are known, we want to give here a new proof. If $M$ has no nontrivial finite $\Lambda$-submodule, then $\mathrm{depth}(M) = 1$, that is, there exists an element $x \in \Lambda$ such that the multiplication by $x$ map on $M$ is injective. By Auslander–Buchsbaum formula, we have

$$\mathrm{pd}_\Lambda(M) + \mathrm{depth}(M) = \mathrm{depth}(\Lambda)$$

with $\mathrm{depth}(M) = 1$, and $\mathrm{depth}(\Lambda) = 2$. Thus, $\mathrm{pd}_\Lambda(M) = 1$. This shows that $M$ is the cokernel of a $\Lambda$-homomorphism $f : \Lambda^n \to \Lambda^n$. Then both the characteristic ideal and the Fitting ideal of $M$ are generated by $\det(f)$, and we get the conclusion. See also [38, Proposition 2.1] and [34, Lemma 1.3.3 and Proposition 1.3.4]. ■

**Remark A.8.** This lemma is an enhanced version of [21, page 327–328, Appendix] removing the $\mu = 0$ assumption. (cf. [14, §1.1].)

**Lemma A.9.** Let $M$ and $N$ be $\Lambda_n$-modules. We assume that $M$ and $N$ have no finite $\Lambda$-torsion submodule provided that we regard $M$ and $N$ as $\Lambda$-modules. If $N \subseteq M$, then

$$\mathrm{Fitt}_{\Lambda_n}(M) \subseteq \mathrm{Fitt}_{\Lambda_n}(N).$$

**Proof.** We regard $M$ and $N$ as $\Lambda$-modules. Then we have

$$\mathrm{Fitt}_{\Lambda}(M) = \mathrm{char}_{\Lambda}(M) \qquad \mathrm{Fitt}_{\Lambda}(N) = \mathrm{char}_{\Lambda}(N)$$

by Lemma A.7. Consider the exact sequence of $\Lambda$-modules

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$$

Then we have

$$\begin{aligned}
\mathrm{Fitt}_{\Lambda}(M) &= \mathrm{char}_{\Lambda}(M) \\
&= \mathrm{char}_{\Lambda}(N) \cdot \mathrm{char}_{\Lambda}(M/N) \\
&= \mathrm{Fitt}_{\Lambda}(N) \cdot \mathrm{char}_{\Lambda}(M/N) \\
&\subseteq \mathrm{Fitt}_{\Lambda}(N).
\end{aligned}$$

By taking the quotient by $\omega_n$ with Lemma A.6, we have

$$\mathrm{Fitt}_{\Lambda_n}(M) \subseteq \mathrm{Fitt}_{\Lambda_n}(N).$$

■

**Lemma A.10.** If $A \subset B$ as finitely generated $\Lambda_n$-modules, then

$$\mathrm{Fitt}_{\Lambda_n}(B) \subseteq \mathrm{Fitt}_{\Lambda_n}(A).$$

**Proof.** Consider the following two exact sequences as $\Lambda$ or $\Lambda_n$-modules with compatibility

$$\begin{tikzcd}
0 \arrow[r] & B_{\mathrm{mft}} \arrow[r] & B \arrow[r] & B' \arrow[r] & 0 \\
0 \arrow[r] & A_{\mathrm{mft}} \arrow[r] \arrow[u, hook] & A \arrow[r] \arrow[u, hook] & A' \arrow[r] \arrow[u, hook] & 0,
\end{tikzcd}$$

where $A_{\mathrm{mft}}$ and $B_{\mathrm{mft}}$ are the maximal finite torsion $\Lambda$-submodules of $A$ and $B$, respectively. Thus, $A'$ and $B'$ have no finite $\Lambda$-submodule and indeed have no finite $\Lambda_n$-

submodule. Then we have

$$\mathrm{Fitt}_{\Lambda_n}(B') \subseteq \mathrm{Fitt}_{\Lambda_n}(A')$$

by Lemma A.9. Also, by Mazur–Wiles [21, Corollary to Proposition 3, Appendix, Page 328], we have

$$\mathrm{Fitt}_{\Lambda_n}\left(B_{\mathrm{mft}}\right) \subseteq \mathrm{Fitt}_{\Lambda_n}\left(A_{\mathrm{mft}}\right).$$

Then Lemma A.3 and Lemma A.6 show us that

$$\mathrm{Fitt}_{\Lambda_n}(A) = \mathrm{Fitt}_{\Lambda_n}\left(A_{\mathrm{mft}}\right) \cdot \mathrm{Fitt}_{\Lambda_n}(A')$$
$$\mathrm{Fitt}_{\Lambda_n}(B) = \mathrm{Fitt}_{\Lambda_n}\left(B_{\mathrm{mft}}\right) \cdot \mathrm{Fitt}_{\Lambda_n}(B').$$

Thus, the conclusion follows. ■

## References

[1] Bley, W. and D. Macias Castillo. “Congruences for critical values of higher derivatives of twisted Hasse-Weil $L$-functions.” *J. Reine Angew. Math.* 722 (2017): 105–35.

[2] Breuil, C., B. Conrad, F. Diamond, and R. Taylor. “On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises.” *J. Amer. Math. Soc.* 14, no. 4 (2001): 843–939.

[3] Emerton, M., R. Pollack, and T. Weston. “Explicit reciprocity laws and Iwasawa theory for modular forms.” (in preparation).

[4] Greenberg, R. “Iwasawa theory for elliptic curves.” *Arithmetic Theory of Elliptic Curves* (Cetraro, 1997) (Berlin), edited by C. Viola. *Lecture Notes in Math.*, vol. 1716, Centro Internazionale Matematico Estivo (C.I.M.E.). Lectures from the 3rd C.I.M.E. Session held in Cetraro, July 12–19, 1997. Florence: Springer, 1999, pp. 51–144.

[5] Hachimori, Y. and K. Matsuno. “On finite$\Lambda$*-submodules of Selmer groups of elliptic curves*.” *Proc. Amer. Math. Soc.* 128, no. 9 (2000): 2539–41.

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

[7] Kato, K. “$p$-adic Hodge theory and values of zeta functions of modular forms.” *Astérisque* 295 (2004): 117–290.

[8] Kim, B. D. “The plus/minus Selmer groups for supersingular primes.” *J. Aust. Math. Soc.* 95, no. 2 (2013): 189–200.

[9] Kim, C.-H. “An anticyclotomic Mazur-Tate conjecture for modular forms.” Preprint arXiv:1612.03743.

[10] Kim, C.-H., M. Kim, and H.-S. Sun. “On the indivisibility of derived Kato’s Euler systems and the main conjecture for modular forms.” Preprint arXiv:1709.05780.

[11] Kitajima, T. and R. Otsuki. “On the plus and the minus Selmer groups for elliptic curves at supersingular primes.” *Tokyo J. Math.* 41, no. 1 (2018): 273–303.

[12] Kobayashi, S. “Iwasawa theory for elliptic curves at supersingular primes.” *Invent. Math.* 152, no. 1 (2003): 1–36.

[13] Kurihara, M. "On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction I." *Invent. Math.* 149, (2002): 195–224.

[14] Kurihara, M. "Iwasawa theory and Fitting ideals." *J. Reine Angew. Math.* 561 (2003): 39–86.

[15] Kurihara, M. "Refined Iwasawa theory for $p$-adic representations and the structure of Selmer groups." *Münster J. Math.* 7, no. 1 (2014): 149–223.

[16] Kurihara, M. "The structure of Selmer groups of elliptic curves and modular symbols." In *Iwasawa Theory 2012: State of the Art and Recent Advances*, edited by T. Bouganis and O. Venjakob. *Contributions in Mathematical and Computational Sciences*, vol. 7. Berlin, Heidelberg: Springer, 2014, 317–56.

[17] Kurihara, M. and R. Otsuki. "On the growth of Selmer groups of an elliptic curve with supersingular reduction in the $\mathbb{Z}_2$-extension of $\mathbb{Q}$." *Pure Appl. Math. Q.* 2, no. 2 (2006): 557–68. (Special Issue: In honor of John H. Coates, Part 2 of 2).

[18] Kurihara, M. and R. Pollack. "Two $p$-adic $L$-functions and rational points on elliptic curves with supersingular reduction." In *L-functions and Galois representations*, edited by D. Burns, K. Buzzard, and J. Nekovář. London Math. Soc. Lecture Note Ser., vol. 320. Cambridge: Cambridge University Press, 2007, 300–32.

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

[20] Mazur, B. and J. Tate. "Refined conjectures of the "Birch and Swinnerton-Dyer type"." *Duke Math. J.* 54, no. 2 (1987): 711–50.

[21] Mazur, B. and A. Wiles. "Class fields of abelian extensions of $\mathbb{Q}$." *Invent. Math.* 76, no. 2 (1984): 179–330.

[22] Milne, J. S. *Arithmetic Duality Theorems*, 2nd ed. BookSurge, LLC, 2006.

[23] Northcott, D. G. *Finite Free Resolutions*. Cambridge Tracts in Math., vol. 71. Cambridge-New York-Melbourne Cambridge University Press, 1976.

[24] Ota, K. "Kato's Euler system and the Mazur–Tate refined conjecture of BSD type." *Amer. J. Math.* 140, no. 2 (2018): 495–542.

[25] Pollack, R. "On the $p$-adic $L$-function of a modular form at a supersingular prime." *Duke Math. J.* 118, no. 3 (2003): 523–58.

[26] Pollack, R. "An algebraic version of a theorem of Kurihara." *J. Number Theory* 110/1 (2005): 164–77. (Special issue in honor of Arnold Ross.).

[27] Perrin-Riou, B. $p$-adic $L$-Functions and $p$-adic Representations. *SMF/AMS Texts and Monographs*, vol. 3. Providence, RI: American Mathematical Society, 2000. Translated by Leila Schneps.

[28] Perrin-Riou, B. "Arithmétique des courbes elliptiques à réduction supersingulèere en $p$." *Exp. Math.* 12, no. 2 (2003): 155–86.

[29] Pollack, R. and K. Rubin. "The main conjecture for CM elliptic curves at supersingular primes." *Ann. of Math. (2)* 159, no. 1 (2004): 447–64.

[30] Rubin, K. "On the main cojecture of Iwasawa theory for imaginary quadratic fields." *Invent. Math.* 93, no. 3 (1988): 701–14.

[31] Rubin, K. “The “main conjectures” of Iwasawa theory for imaginary quadratic fields.” *Invent. Math.* 103, no. 1 (1991): 25–68.

[32] Skinner, C. and E. Urban. “The Iwasawa main conjectures for $\mathrm{GL}_2$.” *Invent. Math.* 195, no. 1 (2014): 1–277.

[33] Sprung, F. “Iwasawa theory for elliptic curves at supersingular primes: a pair of main conjectures.” *J. Number Theory* 132, no. 7 (2012): 1483–506.

[34] Taleb, R. “An equivariant main conjecture in Iwasawa theory and the Coates–Sinnot conjecture.” PhD thesis, McMaster University, 2012. Open Access Dissertations and Theses. Paper 7563, under the supervision of Manfred Kolster.

[35] Wan, X. “The Iwasawa main conjecture for Hilbert modular forms.” *Forum Math. Sigma* 3, (2015): e18 (95 pages).

[36] Wan, X. “Iwasawa main conjecture for non-ordinary modular forms.” (2018): preprint arXiv:1607.07729.

[37] Wan, X. “Iwasawa main conjecture for supersingular elliptic curves.” (2018): preprint arXiv:1411.6352.

[38] Wingberg, K. “Duality theorems for $\Gamma$-extensions of algebraic number fields.” *Compos. Math.* 55, no. 3 (1985): 333–81.