p-Selmer Group and Modular Symbols

Ryotaro Sakamoto

Received: May 13, 2022
Revised: July 20, 2022

Communicated by Otmar Venjakob

Abstract. We prove that the dimension of the p-Selmer group of an elliptic curve is controlled by certain analytic quantities associated with modular symbols as conjectured by Kurihara.

2020 Mathematics Subject Classification: 11R23, 11R34, 11G05, 11G40
Keywords and Phrases: p-Selmer group, modular symbols, elliptic curves, Euler systems, Kolyvagin systems, Mazur–Tate conjecture

1 Introduction

In modern number theory, it is an attractive area of research to connect L-values with Selmer groups. For instance, the Birch and Swinnerton-Dyer conjecture relates arithmetic data of an elliptic curve over a number field to the behavior of its L-function at $s = 1$. In the present paper, we prove that the dimension of the (classical) p-Selmer group $\mathrm{Sel}(\mathbb{Q}, E[p])$ of an elliptic curve $E/\mathbb{Q}$ is controlled by certain analytic quantities associated with modular symbols as conjectured by Kurihara in [10].

1.1 Main result

In order to explain the main result in detail, we first introduce some notations and hypotheses. Let $E/\mathbb{Q}$ be an elliptic curve and let $S_{\mathrm{bad}}(E)$ denote the set of primes at which E has bad reduction. For each prime $\ell \in S_{\mathrm{bad}}(E)$, we denote by $\mathrm{Tam}_\ell(E) := [E(\mathbb{Q}_\ell) \colon E^0(\mathbb{Q}_\ell)]$ the Tamagawa number for $E/\mathbb{Q}_\ell$. As in the paper [10] of Kurihara, we consider a prime $p > 3$ satisfying the following conditions:

(a) p is a good ordinary prime for E.

(b) The action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $E[p]$ is surjective.

(c) $p \nmid \# E(\mathbb{F}_p) \prod_{\ell \in S_{\mathrm{bad}}(E)} \mathrm{Tam}_\ell(E)$.

Let $\mathcal{P}_{1,0}$ denote the set of Kolyvagin primes, that is,

$$\mathcal{P}_{1,0} := \{\ell \notin S_{\mathrm{bad}}(E) \mid E(\mathbb{F}_\ell)[p] \cong \mathbb{F}_p \text{ and } \ell \equiv 1 \pmod{p}\}.$$

We define $\mathcal{N}_{1,0}$ to be the set of square-free products in $\mathcal{P}_{1,0}$. We fix a generator $h_\ell \in \mathrm{Gal}(\mathbb{Q}(\mu_\ell)/\mathbb{Q})$ for each prime $\ell \in \mathcal{P}_{1,0}$, and we obtain a surjective homomorphism (induced by the discrete logarithm to the base h_ℓ)

$$\overline{\log}_{h_\ell} \colon \mathrm{Gal}(\mathbb{Q}(\mu_\ell)/\mathbb{Q}) \xrightarrow{\sim} \mathbb{Z}/(\ell-1) \longrightarrow \mathbb{F}_p;\ h_\ell^a \mapsto a \bmod p.$$

Let f_E denote the newform of weight 2 associated with $E/\mathbb{Q}$. Take an integer $d \in \mathcal{N}_{1,0}$. For any integer a with $(a,d)=1$, we write $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\mu_d)/\mathbb{Q})$ for the element satisfying $\sigma_a(\zeta) = \zeta^a$ for any $\zeta \in \mu_d$ and put

$$[a/d] := 2\pi\sqrt{-1}\int_{\sqrt{-1}\infty}^{a/d} f_E(z)\,\mathrm{d}z.$$

The assumption (b) implies that $\mathrm{Re}([a/d])/\Omega_E^+ \in \mathbb{Z}_p$, where Ω_E^+ is the Néron period of E (cf. [23]). Following Kurihara in [10], we define an analytic quantity $\widetilde{\delta}_d$ which relates to L-values by

$$\widetilde{\delta}_d := \sum_{\substack{a=1 \\ (a,d)=1}}^{d} \frac{\mathrm{Re}([a/d])}{\Omega_E^+} \cdot \prod_{\ell \mid d} \overline{\log}_{h_\ell}(\sigma_a) \in \mathbb{F}_p, .$$

Kurihara remarked in [10] that it is easy to compute the analytic quantity $\widetilde{\delta}_d$ (see [10, §5.3]), and gave the following conjecture.

Conjecture 1.1 ([10, Conjecture 1]). *There is an integer $d \in \mathcal{N}_{1,0}$ with $\widetilde{\delta}_d \neq 0$.*

Concerning this conjecture, Kurihara proved in [10] that the non-degeneracy of the p-adic height pairing and the Iwasawa main conjecture for $E/\mathbb{Q}$ imply Conjecture 1.1. In the paper [5], Chan-Ho Kim, Myoungil Kim, and Hae-Sang Sun called $\widetilde{\delta}_d$ Kurihara number at d and gave a simple and efficient numerical criterion to verify the Iwasawa main conjecture for $E/\mathbb{Q}$ by using $\widetilde{\delta}_d$, namely, they proved in [5] that Conjecture 1.1 implies the Iwasawa main conjecture for $E/\mathbb{Q}$. Moreover, Chan-Ho Kim and Nakamura in [6] generalized this numerical criterion to the additive reduction case. In the present paper, we give the following answer to Conjecture 1.1.

Theorem 1.2 (Corollary 4.3). *Conjecture 1.1 is equivalent to the Iwasawa main conjecture for $E/\mathbb{Q}$.*

Remark 1.3. Skinner and Urban proved in [22] that if there exists a prime $q \neq p$ such that $\mathrm{ord}_q(N_E) = 1$ and $E[p]$ is ramified at q, then the Iwasawa main conjecture for E is valid. Here N_E is the conductor of $E/\mathbb{Q}$.

Next, let us explain the relation between the structure of the p-Selmer group $\mathrm{Sel}(\mathbb{Q}, E[p])$ and the analytic quantities $\widetilde{\delta}_d$. For that, we use the following terminology of Kurihara in [10].

Definition 1.4. *We say that an integer $d \in \mathcal{N}_{1,0}$ is δ-minimal if $\widetilde{\delta}_d \neq 0$ and $\widetilde{\delta}_e = 0$ for any positive proper divisor e of d.*

Recall that, by the definition of the p-Selmer group, the localization map at ℓ induces a natural homomorphism

$$\mathrm{Sel}(\mathbb{Q}, E[p]) \longrightarrow E(\mathbb{Q}_\ell) \otimes_{\mathbb{Z}} \mathbb{F}_p.$$

Let $d \in \mathcal{N}_{1,0}$ be a δ-minimal integer. Kurihara proved in [10] that the natural homomorphism

$$\mathrm{Sel}(\mathbb{Q}, E[p]) \hookrightarrow \bigoplus_{\ell \mid d} E(\mathbb{Q}_\ell) \otimes_{\mathbb{Z}} \mathbb{F}_p \tag{1}$$

is injective (see Remark 4.5), and he conjectured in [10, Conjecture 2] that the homomorphism (1) is an isomorphism. By the definition of $\mathcal{P}_{1,0}$, we have

$$\dim_{\mathbb{F}_p}(E(\mathbb{Q}_\ell) \otimes_{\mathbb{Z}} \mathbb{F}_p) = 1$$

for each prime divisor $\ell \mid d$, and hence this conjecture is equivalent to that

$$\dim_{\mathbb{F}_p}(\mathrm{Sel}(\mathbb{Q}, E[p])) = \nu(d),$$

where $\nu(d)$ denotes the number of distinct prime divisors of d. Kurihara showed in [10, Theorem 4] that (1) is an isomorphism in some special cases. In the present paper, we solve this conjecture.

Theorem 1.5 (Theorem 4.8). *For any δ-minimal integer $d \in \mathcal{N}_{1,0}$, we have the natural isomorphism*

$$\mathrm{Sel}(\mathbb{Q}, E[p]) \xrightarrow{\sim} \bigoplus_{\ell \mid d} E(\mathbb{Q}_\ell) \otimes_{\mathbb{Z}} \mathbb{F}_p,$$

and hence $\dim_{\mathbb{F}_p}(\mathrm{Sel}(\mathbb{Q}, E[p])) = \nu(d)$.

Remark 1.6. Theorem 1.5 implies that for any integer $d \in \mathcal{N}_{1,0}$ with $\widetilde{\delta}_d \neq 0$, we have

$$\dim_{\mathbb{F}_p}(\mathrm{Sel}(\mathbb{Q}, E[p])) \leq \nu(d).$$

Note that the analytic quantity $\widetilde{\delta}_d$ is computable, as the author mentioned above.

Remark 1.7. After the author had got almost all the results in the present paper, Chan-Ho Kim told the author that he also proved the same result (see [7]).

Remark 1.8. The analogue of Theorem 1.5 for ideal class groups does not hold. Kurihara has given a counter-example in [10, §5.4]. In Remark 4.9, we explain an important property to prove Theorem 1.5.

By using the functional equation for modular symbols (see [13, (1.6.1)]), Kurihara showed in [10, Lemma 4] that $w_E = (-1)^{\nu(d)}$ for any δ-minimal integer $d \in \mathcal{N}_{1,0}$. Here w_E denotes the (global) root number of $E/\mathbb{Q}$. Hence, as an application of Theorem 1.5, we obtain the following result concerning the parity of the order of vanishing of L-function $L(E/\mathbb{Q}, s)$ at $s = 1$:

COROLLARY 1.9. *Suppose that the Iwasawa main conjecture for $E/\mathbb{Q}$ holds true. Then we have*

$$\dim_{\mathbb{F}_p}(\mathrm{Sel}(\mathbb{Q}, E[p])) \equiv \mathrm{ord}_{s=1}(L(E/\mathbb{Q}, s)) \pmod 2.$$

Moreover, if the p-primary part of the Tate–Shafarevich group for $E/\mathbb{Q}$ is finite, then we have

$$\mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q})) \equiv \mathrm{ord}_{s=1}(L(E/\mathbb{Q}, s)) \pmod 2.$$

Proof. Since we assume that the Iwasawa main conjecture for $E/\mathbb{Q}$ holds true, Theorem 1.2 shows that there is a δ-minimal integer $d \in \mathcal{N}_{1,0}$. Then, Theorem 1.5, combined with the fact that $w_E = (-1)^{\nu(d)}$, implies that $w_E = (-1)^{\dim_{\mathbb{F}_p}(\mathrm{Sel}(\mathbb{Q},E[p]))}$. Since $w_E = (-1)^{\mathrm{ord}_{s=1}(L(E/\mathbb{Q},s))}$, we have $\dim_{\mathbb{F}_p}(\mathrm{Sel}(\mathbb{Q}, E[p])) \equiv \mathrm{ord}_{s=1}(L(E/\mathbb{Q}, s)) \pmod 2$. □

Remark 1.10. Corollary 1.9 has already been proved by Nekovář in [14] (see also [15]), assuming only the condition (a). However, the proof of Corollary 1.9 is completely different from that of [14, Theorem A].

The proof of Theorem 1.5 is based on the theory of Kolyvagin systems of rank 0 developed in [21]. In §2, we introduce the theory of Kolyvagin systems. In §3, we construct a Kolyvagin system of rank 0 from modular symbols. In §4, we discuss the relation between this Kolyvagin system and the set of the analytic quantities $\{\widetilde{\delta}_d\}_{d \in \mathcal{N}_{1,0}}$, and we give a proof of Theorem 1.5. Moreover, by using the Kolyvagin system constructed in §3, we construct an explicit basis of the p-Selmer group (see Corollary 4.10).

1.2 A mod p analog of the Mazur–Tate refined conjecture of BSD type

As in the previous subsection, let $E/\mathbb{Q}$ be an elliptic curve satisfying the conditions (a), (b), and (c). For each integer $d \in \mathcal{N}_{1,0}$, the Mazur–Tate modular element $\widetilde{\theta}_{\mathbb{Q}(\mu_d)}$ is defined by

$$\widetilde{\theta}_{\mathbb{Q}(\mu_d)} := \sum_{\substack{a=1 \\ (a,d)=1}}^{d} \frac{\mathrm{Re}([a/d])}{\Omega_E^+} \sigma_a \in \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\mu_d)/\mathbb{Q})],$$

and Mazur and Tate conjectured in [13] a refined Birch and Swinnerton-Dyer conjecture consisting of two parts, by using $\widetilde{\theta}_{\mathbb{Q}(\mu_d)}$. One of the two parts concerns the order of vanishing of $\widetilde{\theta}_{\mathbb{Q}(\mu_d)}$ (the rank-part). More precisely, the following is the rank-part of the Mazur-Tate conjecture.

Conjecture 1.11 (Mazur–Tate). *Let* $\mathcal{I}_d := \ker(\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\mu_d)/\mathbb{Q})] \longrightarrow \mathbb{Z}_p)$. *Then*

$$\widetilde{\theta}_{\mathbb{Q}(\mu_d)} \in (\mathcal{I}_d)^{r_E},$$

where $r_E := \mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q}))$.

Remark 1.12.

(1) Under the validity of the $\mu = 0$ conjecture, Kurihara proved Conjecture 1.11 (see [10, Remark 2] and [13, Proposition 3]).

(2) Since we only consider integers in $\mathcal{N}_{1,0}$ in the present paper, Conjecture 1.11 is proved by Ota when $p \geq r_E$ (see [16, Theorem 1.2]).

By using Ota's results in [16], we show the following theorem which is a mod p analog of Conjecture 1.11.

Theorem 1.13. *Let* $\overline{\mathcal{I}}_d := \ker(\mathbb{F}_p[\mathrm{Gal}(\mathbb{Q}(\mu_d)/\mathbb{Q})] \longrightarrow \mathbb{F}_p)$. *We have*

$$\widetilde{\theta}_{\mathbb{Q}(\mu_d)} \bmod p \in (\overline{\mathcal{I}}_d)^{r_p},$$

where $r_p := \dim_p(\mathrm{Sel}(\mathbb{Q}, E[p]))$.

Proof. Note that $r_p - 1 \leq \dim_p(\ker(\mathrm{Sel}(\mathbb{Q}, E[p]) \longrightarrow E(\mathbb{Q}_p)/p))$ since $E(\mathbb{Q}_p)/p \cong \mathbb{F}_p$. Then by [16, Proposition 3.3, Theorem 4.9, Corollary 5.13], we have

$$\widetilde{\theta}_{\mathbb{Q}(\mu_d)} \bmod p \in (\overline{\mathcal{I}}_d)^{r_p - 1}.$$

Moreover, the p-parity conjecture (see [14]) and the functional equation of the modular element $\widetilde{\theta}_{\mathbb{Q}(\mu_d)}$ (see [16, Proposition 5.16]) show that

$$\widetilde{\theta}_{\mathbb{Q}(\mu_d)} \bmod p \in (\overline{\mathcal{I}}_d)^{r_p}$$

(see the proof of [16, Theorem 5.17]). □

Remark 1.14. In the statement of [16, Theorem 4.9], there is the assumption that $\max_{\ell | S}\{e_\ell(D)\} < p$. This assumption is only used to prove [16, Lemma 3.1], which states a certain relation between Darmon–Kolyvagin derivatives. However, since $q = p$ in our case, [16, Lemma 3.1] holds true without any assumption, and hence the conclusion of [16, Theorem 4.9] is valid without the assumption that $\max_{\ell | S}\{e_\ell(D)\} < p$.

Theorem 1.13 is equivalent to that the maximum value of the set of the vanishing orders of $\widetilde{\theta}_{\mathbb{Q}(\mu_d)}$ mod p is at least r_p, namely,

$$r_p \leq \max\{r \geq 0 \mid \widetilde{\theta}_{\mathbb{Q}(\mu_d)} \bmod p \in (\overline{\mathcal{I}}_d)^r \text{ for any } d \in \mathcal{N}_{1,0}\}.$$

As a corollary of the main result of the present paper, we show the opposite inequality.

THEOREM 1.15. *Suppose that the Iwasawa main conjecture for $E/\mathbb{Q}$ holds true. Then we have*

$$r_p = \max\{r \geq 0 \mid \widetilde{\theta}_{\mathbb{Q}(\mu_d)} \bmod p \in (\overline{\mathcal{I}}_d)^r \textit{ for any } d \in \mathcal{N}_{1,0}\}.$$

Proof. Since we assume the validity of the Iwasawa main conjecture for $E/\mathbb{Q}$, we have a δ-minimal integer $d \in \mathcal{N}_{1,0}$ by Theorem 1.2. Then

$$\nu(d) = r_p$$

by Theorem 1.5. Hence it suffices to show that $\widetilde{\theta}_{\mathbb{Q}(\mu_d)} \bmod p \notin (\overline{\mathcal{I}}_d)^{\nu(d)+1}$. This fact follows from the definition of the δ-minimality, Remark 3.1, and Lemmas 3.13 and 3.14. $\square$

ACKNOWLEDGEMENT

The author would like to thank Masato Kurihara for his careful reading of the paper and his many helpful suggestions. The author would also like to thank Chan-Ho Kim for helpful comments. The author would like to thank the referee for helpful comments and suggestions. The author was supported by JSPS KAKENHI Grant Number 20J00456.

2 THE THEORY OF KOLYVAGIN SYSTEM

In this section, we recall the theory of Kolyvagin systems. The contents of this section are based on [11, 21].

Let $p > 3$ be a prime satisfying the hypotheses (a), (b) and (c). For notational simplicity, we put

$$M/p^m := M/p^m M$$

for any abelian group M. Fix integers $n \geq 0$ and $m \geq 1$. Let $\mathbb{Q}_n$ denote the n-th layer of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. We then put

$$R := \mathbb{Z}_p/p^m[\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})] \quad \text{and} \quad T := \mathrm{Ind}_{G_{\mathbb{Q}_n}}^{G_{\mathbb{Q}}}(E[p^m]).$$

Note that T satisfies the hypotheses (H.0) – (H.3) in [11, §3.5]. However, T does not satisfy the hypothesis (H.4) in [11, §3.5] when $p = 3$.

2.1 Selmer structures

We introduce two Selmer structures on T. Recall that a Selmer structure $\mathcal{F}$ on T is a collection of the following data:

- a finite set $S(\mathcal{F})$ of rational primes containing $S_{\mathrm{bad}}(E) \cup \{p\}$,
- a choice of R-submodule $H^1_{\mathcal{F}}(G_{\mathbb{Q}_\ell}, T)$ of $H^1(G_{\mathbb{Q}_\ell}, T)$ for each prime $\ell \in S(\mathcal{F})$.

Here, for any field K, we denote by $\overline{K}$ a separable closure of K and set $G_K := \mathrm{Gal}(\overline{K}/K)$. For each prime $\ell \notin S(\mathcal{F})$, we set

$$H^1_{\mathcal{F}}(G_{\mathbb{Q}_\ell}, T) := H^1_{\mathrm{ur}}(\mathbb{Q}_\ell, T) := \ker\left(H^1(G_{\mathbb{Q}_\ell}, T) \longrightarrow H^1(G_{\mathbb{Q}_\ell^{\mathrm{ur}}}, T)\right),$$

where $\mathbb{Q}_\ell^{\mathrm{ur}}$ denotes the maximal unramified extension of $\mathbb{Q}_\ell$. We define the Selmer module $H^1_{\mathcal{F}}(G_{\mathbb{Q}}, T)$ by

$$H^1_{\mathcal{F}}(G_{\mathbb{Q}}, T) := \ker\left(H^1(G_{\mathbb{Q}}, T) \longrightarrow \bigoplus_{\ell} H^1(G_{\mathbb{Q}_\ell}, T)/H^1_{\mathcal{F}}(G_{\mathbb{Q}_\ell}, T)\right).$$

Set $T^\vee(1) := \mathrm{Hom}(T, \mu_{p^\infty})$. For each prime ℓ, we define

$$H^1_{\mathcal{F}^*}(G_{\mathbb{Q}_\ell}, T^\vee(1)) \subset H^1(G_{\mathbb{Q}_\ell}, T^\vee(1))$$

to be the orthogonal complement of $H^1_{\mathcal{F}}(G_{\mathbb{Q}_\ell}, T)$ with respect to the local Tate pairing. Hence we obtain the dual Selmer structure $\mathcal{F}^*$ on $T^\vee(1)$. Throughout this paper, we regard $\mathcal{F}^*$ as a Selmer structure on T by using the isomorphism $T \cong T^\vee(1)$ induced by the Weil pairing.

Theorem 2.1 ([11, Theorem 2.3.4]). *Let $\mathcal{F}_1$ and $\mathcal{F}_2$ be Selmer structures on T satisfying*

$$H^1_{\mathcal{F}_1}(G_{\mathbb{Q}_\ell}, T) \subset H^1_{\mathcal{F}_2}(G_{\mathbb{Q}_\ell}, T)$$

for all primes ℓ. Then we have an exact sequence of R-modules

$$\begin{aligned} 0 \longrightarrow H^1_{\mathcal{F}_1}(G_{\mathbb{Q}}, T) \longrightarrow H^1_{\mathcal{F}_2}(G_{\mathbb{Q}}, T) \longrightarrow \bigoplus_{\ell} H^1_{\mathcal{F}_2}(G_{\mathbb{Q}_\ell}, T)/H^1_{\mathcal{F}_1}(G_{\mathbb{Q}_\ell}, T) \\ \longrightarrow H^1_{\mathcal{F}_1^*}(G_{\mathbb{Q}}, T)^\vee \longrightarrow H^1_{\mathcal{F}_2^*}(G_{\mathbb{Q}}, T)^\vee \longrightarrow 0, \end{aligned}$$

where ℓ runs over all the rational primes satisfying $H^1_{\mathcal{F}_1}(G_{\mathbb{Q}_\ell}, T) \neq H^1_{\mathcal{F}_2}(G_{\mathbb{Q}_\ell}, T)$. Here $(-)^\vee := \mathrm{Hom}(-, \mathbb{Q}_p/\mathbb{Z}_p)$.

Lemma 2.2 ([1, §3.2], [11, Lemma 3.5.3]). *For any Selmer structure $\mathcal{F}$ on T, the canonical map $E[p] \hookrightarrow T$ induces an isomorphism*

$$H^1_{\mathcal{F}^*}(G_{\mathbb{Q}}, E[p]) \xrightarrow{\sim} H^1_{\mathcal{F}^*}(G_{\mathbb{Q}}, T)[\mathfrak{m}_R].$$

Here $\mathfrak{m}_R$ denote the maximal ideal of R. In particular, $H^1_{\mathcal{F}^*}(G_{\mathbb{Q}}, E[p]) = 0$ if and only if $H^1_{\mathcal{F}^*}(G_{\mathbb{Q}}, T) = 0$.

Following Mazur and Rubin, we define the transversal local condition $H^1_{\mathrm{tr}}(G_{\mathbb{Q}_\ell}, T)$ and a Selmer structure $\mathcal{F}^a_b(c)$ on T.

Definition 2.3.

(1) *For any integer d, we write $\mathbb{Q}(d)$ for the maximal p-subextension of $\mathbb{Q}(\mu_d)$.*

(2) *For any prime ℓ, define*

$$H^1_{\mathrm{tr}}(G_{\mathbb{Q}_\ell}, T) := \ker\left(H^1(G_{\mathbb{Q}_\ell}, T) \longrightarrow H^1(G_{\mathbb{Q}(\ell)\otimes\mathbb{Q}_\ell}, T)\right).$$

We also set $H^1_{/*}(G_{\mathbb{Q}_\ell}, T) := H^1(G_{\mathbb{Q}_\ell}, T)/H^1_*(G_{\mathbb{Q}_\ell}, T)$ for $* \in \{\mathrm{ur}, \mathrm{tr}\}$.

(3) *Let a, b, and c be pairwise relatively prime (square-free) integers. Define the Selmer structure $\mathcal{F}^a_b(c)$ on T by the following data:*

– $S(\mathcal{F}^a_b(c)) := S(\mathcal{F}) \cup \{\ell \mid abc\}$,

– $$H^1_{\mathcal{F}^a_b(c)}(G_{\mathbb{Q}_\ell}, T) := \begin{cases} H^1(G_{\mathbb{Q}_\ell}, T) & \text{if } \ell \mid a, \\ 0 & \text{if } \ell \mid b, \\ H^1_{\mathrm{tr}}(G_{\mathbb{Q}_\ell}, T) & \text{if } \ell \mid c, \\ H^1_{\mathcal{F}}(G_{\mathbb{Q}_\ell}, T) & \text{otherwise.} \end{cases}$$

Note that $(\mathcal{F}^a_b(c))^* = (\mathcal{F}^*)^b_a(c)$. For simplicity, we will write $\mathcal{F}^a$, $\mathcal{F}_b$, $\mathcal{F}(c)$, ... instead of $\mathcal{F}^a_1(1)$, $\mathcal{F}^1_b(1)$, $\mathcal{F}^1_1(c)$, ..., respectively.

Definition 2.4 (classical Selmer structure). *We define the classical Selmer structure $\mathcal{F}_{\mathrm{cl}}$ on T by the following:*

- $S(\mathcal{F}_{\mathrm{cl}}) := S_{\mathrm{bad}}(E) \cup \{p\}$,
- $H^1_{\mathcal{F}_{\mathrm{cl}}}(G_{\mathbb{Q}_\ell}, T) := \mathrm{im}\left(\bigoplus_{\mathfrak{l}\mid\ell} E(\mathbb{Q}_{n,\mathfrak{l}})/p^m \longrightarrow H^1(G_{\mathbb{Q}_\ell}, T)\right)$ *for each prime $\ell \in S(\mathcal{F}_{\mathrm{cl}})$.*

By definition, the Selmer module $H^1_{\mathcal{F}_{\mathrm{cl}}}(G_{\mathbb{Q}}, T)$ coincides with the classical p^m-Selmer group $\mathrm{Sel}(\mathbb{Q}_n, E[p^m])$ *associated with the elliptic curve $E/\mathbb{Q}_n$. We also note that $\mathcal{F}_{\mathrm{cl}} = \mathcal{F}^*_{\mathrm{cl}}$.*

Definition 2.5 (canonical Selmer structure). *We define the canonical Selmer structure $\mathcal{F}_{\mathrm{can}}$ on T by*

$$\mathcal{F}_{\mathrm{can}} = \mathcal{F}^p_{\mathrm{cl}}.$$

Lemma 2.6. *For any prime $\ell \neq p$, we have*

$$H^1_{\mathcal{F}_{\mathrm{can}}}(G_{\mathbb{Q}_\ell}, T) = H^1_{\mathcal{F}_{\mathrm{cl}}}(G_{\mathbb{Q}_\ell}, T) = H^1_{\mathrm{ur}}(G_{\mathbb{Q}_\ell}, T).$$

Proof. By definition, it suffices to show that $E(K)/p^m = H^1_{\mathrm{ur}}(G_K, E[p^m])$ for any unramified p-extension $K/\mathbb{Q}_\ell$. Note that $\#H^1_{\mathrm{ur}}(G_K, E[p^m]) = \#H^0(G_K, E[p^m]) = \#E(K)/p^m$ since $\ell \neq p$. Hence it suffices to show that $E(K)/p^m \subset H^1_{\mathrm{ur}}(G_K, E[p^m])$. Since we assume that $\ell \neq p$ and $p \nmid \mathrm{Tam}_\ell(E)$, we have $E(\mathbb{Q}^{\mathrm{ur}}_\ell)/p^m = \widetilde{E}(\overline{\mathbb{F}}_\ell)/p^m = 0$, where $\widetilde{E}$ denotes the reduction of E at ℓ. This fact implies $E(K)/p^m \subset H^1_{\mathrm{ur}}(G_K, E[p^m])$. □

Remark 2.7. Let $K/\mathbb{Q}_\ell$ be an unramified extension. The assumption that $p \nmid \mathrm{Tam}_\ell(E)$ implies that $E(\mathbb{Q}_\ell^{\mathrm{ur}})[p^\infty]$ is divisible. This fact shows that

$$H^1_{\mathrm{ur}}(G_K, T_p(E)) = \ker(H^1(G_K, T_p(E)) \longrightarrow H^1(G_{\mathbb{Q}_\ell^{\mathrm{ur}}}, T_p(E)) \otimes \mathbb{Q}_p)$$

and $\mathrm{im}\left(H^1_{\mathrm{ur}}(G_K, T_p(E)) \longrightarrow H^1(G_K, E[p^m])\right) = H^1_{\mathrm{ur}}(G_K, E[p^m])$. Therefore, by Lemma 2.6, the canonical Selmer structure in the present paper is the same as the Selmer structure induced by the canonical Selmer structure defined in [11, Definition 3.2.1].

Note that we have the canonical injection $E[p] \hookrightarrow T$.

DEFINITION 2.8. *We say that a Selmer structure $\mathcal{F}$ on T is cartesian if the homomorphism*

$$\mathrm{coker}\left(H^1_{\mathcal{F}}(G_{\mathbb{Q}_\ell}, T) \longrightarrow H^1(G_{\mathbb{Q}_\ell}, E[p])\right) \longrightarrow H^1(G_{\mathbb{Q}_\ell}, T)/H^1_{\mathcal{F}}(G_{\mathbb{Q}_\ell}, T)$$

induced by $E[p] \hookrightarrow T$ is injective for any prime $\ell \in S(\mathcal{F})$.

PROPOSITION 2.9. *The Selmer structure $\mathcal{F}_{\mathrm{can}}$ on T is cartesian.*

Proof. Since we assume $p \nmid \#E(\mathbb{F}_p)$, we have $H^2(G_{\mathbb{Q}_p}, E[p]) \cong H^0(G_{\mathbb{Q}_p}, E[p]) = 0$. This fact implies $\mathrm{coker}\left(H^1_{\mathcal{F}_{\mathrm{can}}}(G_{\mathbb{Q}_p}, T) \longrightarrow H^1(G_{\mathbb{Q}_p}, E[p])\right) = 0$.
Take a prime $\ell \in S_{\mathrm{bad}}(E)$. Since $\mathbb{Q}_n/\mathbb{Q}$ is unramified at ℓ, Lemma 2.6 shows that there are natural injections

$$\mathrm{coker}\left(H^1_{\mathcal{F}_{\mathrm{can}}}(G_{\mathbb{Q}_\ell}, T) \longrightarrow H^1(G_{\mathbb{Q}_\ell}, E[p])\right) \hookrightarrow H^1(G_{\mathbb{Q}_\ell^{\mathrm{ur}}}, E[p])$$

and

$$H^1(G_{\mathbb{Q}_\ell}, T)/H^1_{\mathcal{F}_{\mathrm{can}}}(G_{\mathbb{Q}_\ell}, T) \hookrightarrow H^1(G_{\mathbb{Q}_\ell^{\mathrm{ur}}}, T) \cong \bigoplus_{\mathfrak{l} \mid \ell} H^1(G_{\mathbb{Q}_\ell^{\mathrm{ur}}}, E[p^m]).$$

Since $p \nmid \mathrm{Tam}_\ell(E)$, the module $E(\mathbb{Q}_\ell^{\mathrm{ur}})[p^\infty]$ is divisible. Hence $E(\mathbb{Q}_\ell^{\mathrm{ur}})[p^m] \xrightarrow{\times p} E(\mathbb{Q}_\ell^{\mathrm{ur}})[p^{m-1}]$ is surjective, and $H^1(G_{\mathbb{Q}_\ell^{\mathrm{ur}}}, E[p]) \longrightarrow H^1(G_{\mathbb{Q}_\ell^{\mathrm{ur}}}, E[p^m])$ is injective. This completes the proof. $\square$

2.2 STRUCTURE OF LOCAL POINTS

Let $K/\mathbb{Q}$ be a finite abelian p-extension and put

$$G := \mathrm{Gal}(K/\mathbb{Q}).$$

Let $\widehat{E}$ denote the formal group associated with $E/\mathbb{Q}_p$ and put

$$\widehat{E}(\mathfrak{m}_{K_p}) := \bigoplus_{\mathfrak{p} \mid p} \widehat{E}(\mathfrak{m}_{K_\mathfrak{p}}).$$

Here $\mathfrak{m}_L$ denotes the maximal ideal of the ring of integers of L for any algebraic extension $L/\mathbb{Q}_p$.

Lemma 2.10. *We have* $\widehat{E}(\mathfrak{m}_{\mathbb{Q}_p})/p = (\widehat{E}(\mathfrak{m}_{K_p})/p)^G$.

Proof. Since $p \nmid \#E(\mathbb{F}_p)$, Tan proved in [24, Theorem 2 (a)] that

$$H^1(G_{\mathbb{Q}_p}, \widehat{E}(\mathfrak{m}_{\overline{\mathbb{Q}}_p})) = 0.$$

Take a prime $\mathfrak{p} \mid p$ of K and put $G_\mathfrak{p} := \mathrm{Gal}(K_\mathfrak{p}/\mathbb{Q}_p)$. The injectivity of the inflation map $H^1(G_\mathfrak{p}, \widehat{E}(\mathfrak{m}_{K_\mathfrak{p}})) \longrightarrow H^1(G_{\mathbb{Q}_p}, \widehat{E}(\mathfrak{m}_{\overline{\mathbb{Q}}_p}))$ implies $H^1(G_\mathfrak{p}, \widehat{E}(\mathfrak{m}_{K_\mathfrak{p}})) = 0$. Since $K_\mathfrak{p}/\mathbb{Q}_p$ is a p-extension and $E(\mathbb{Q}_p)[p] = 0$, the module $E(K_\mathfrak{p})$ is p-torsion-free. Hence the vanishing of $H^1(G_\mathfrak{p}, \widehat{E}(\mathfrak{m}_{K_\mathfrak{p}}))$ implies

$$\widehat{E}(\mathfrak{m}_{\mathbb{Q}_p})/p = (\widehat{E}(\mathfrak{m}_{K_\mathfrak{p}})/p)^{G_\mathfrak{p}}.$$

Since

$$\widehat{E}(\mathfrak{m}_{K_p})/p \cong \widehat{E}(\mathfrak{m}_{K_\mathfrak{p}})/p \otimes_{\mathbb{F}_p} \mathbb{F}_p[G/G_\mathfrak{p}],$$

we see that $\widehat{E}(\mathfrak{m}_{\mathbb{Q}_p})/p = (\widehat{E}(\mathfrak{m}_{K_p})/p)^G$. □

Proposition 2.11. *The* $\mathbb{Z}_p[G]$*-module* $\widehat{E}(\mathfrak{m}_{K_p})$ *is free of rank* 1.

Proof. For any finitely generated $\mathbb{F}_p[G]$-module M, put $M^* := \mathrm{Hom}_{\mathbb{F}_p[G]}(M, \mathbb{F}_p[G])$. Since $\mathbb{F}_p[G]$ is a zero-dimensional Gorenstein local ring, we have $M \cong M^{**}$ by Matlis duality. Applying this fact to $((\widehat{E}(\mathfrak{m}_{K_p})/p)^*)_G$ and $\widehat{E}(\mathfrak{m}_{K_p})/p$, we obtain

$$\begin{aligned} ((\widehat{E}(\mathfrak{m}_{K_p})/p)^*)_G &\cong (((\widehat{E}(\mathfrak{m}_{K_p})/p)^*)_G)^{**} \\ &\cong ((\widehat{E}(\mathfrak{m}_{K_p})/p)^{**})^G)^* \\ &\cong (\widehat{E}(\mathfrak{m}_{K_p})/p)^G)^*. \end{aligned}$$

By Lemma 2.10, we have $((\widehat{E}(\mathfrak{m}_{K_p})/p)^G)^* = (\widehat{E}(\mathfrak{m}_{\mathbb{Q}_p})/p)^* \cong (\mathbb{F}_p)^* \cong \mathbb{F}_p$. Hence $(\widehat{E}(\mathfrak{m}_{K_p})/p)^*$ is a cyclic $\mathbb{F}_p[G]$-module. Furthermore, the fact that $\widehat{E}(\mathfrak{m}_{K_p}) \cong \mathbb{Z}_p^{[K:\mathbb{Q}]}$ as $\mathbb{Z}_p$-modules implies that

$$(\widehat{E}(\mathfrak{m}_{K_p})/p)^* \cong \mathbb{F}_p[G].$$

Therefore, $\widehat{E}(\mathfrak{m}_{K_p})/p$ is also free of rank 1, and the $\mathbb{Z}_p[G]$-module $\widehat{E}(\mathfrak{m}_{K_p})$ is cyclic. Since $\widehat{E}(\mathfrak{m}_{K_p}) \cong \mathbb{Z}_p^{[K:\mathbb{Q}]}$, we conclude that $\widehat{E}(\mathfrak{m}_{K_p}) \cong \mathbb{Z}_p[G]$. □

Definition 2.12. *For any integer* $m \geq 1$*, we put*

$$H^1_f(G_{\mathbb{Q}_p}, \mathrm{Ind}_{G_K}^{G_\mathbb{Q}}(E[p^m])) := \mathrm{im}\left(\widehat{E}(\mathfrak{m}_{K_p})/p^m \hookrightarrow H^1(G_{\mathbb{Q}_p}, \mathrm{Ind}_{G_K}^{G_\mathbb{Q}}(E[p^m]))\right).$$

We also define $H^1_{/f}(G_{\mathbb{Q}_p}, \mathrm{Ind}_{G_K}^{G_\mathbb{Q}}(E[p^m]))$ *to be*

$$H^1(G_{\mathbb{Q}_p}, \mathrm{Ind}_{G_K}^{G_\mathbb{Q}}(E[p^m]))/H^1_f(G_{\mathbb{Q}_p}, \mathrm{Ind}_{G_K}^{G_\mathbb{Q}}(E[p^m])).$$

Remark 2.13. Since we assme $p \nmid \#E(\mathbb{F}_p)$, we have $H^1_f(G_{\mathbb{Q}_p}, T) = H^1_{\mathcal{F}_{\mathrm{cl}}}(G_{\mathbb{Q}_p}, T)$ when $K = \mathbb{Q}_n$.

Corollary 2.14.

(1) *The $\mathbb{Z}_p/p^m[G]$-modules*

$$H^1_f(G_{\mathbb{Q}_p}, \mathrm{Ind}_{G_K}^{G_{\mathbb{Q}}}(E[p^m])) \quad \textit{and} \quad H^1_{/f}(G_{\mathbb{Q}_p}, \mathrm{Ind}_{G_K}^{G_{\mathbb{Q}}}(E[p^m]))$$

are free of rank 1.

(2) *For any subfield $K' \subset K$, we have natural isomorphisms*

$$H^1_f(G_{\mathbb{Q}_p}, \mathrm{Ind}_{G_K}^{G_{\mathbb{Q}}}(E[p^m]))_{\mathrm{Gal}(K/K')} \xrightarrow{\sim} H^1_f(G_{\mathbb{Q}_p}, \mathrm{Ind}_{G_{K'}}^{G_{\mathbb{Q}}}(E[p^m])),$$
$$H^1_{/f}(G_{\mathbb{Q}_p}, \mathrm{Ind}_{G_K}^{G_{\mathbb{Q}}}(E[p^m]))_{\mathrm{Gal}(K/K')} \xrightarrow{\sim} H^1_{/f}(G_{\mathbb{Q}_p}, \mathrm{Ind}_{G_{K'}}^{G_{\mathbb{Q}}}(E[p^m])).$$

Proof. For simplicity, we put $T_K := \mathrm{Ind}_{G_K}^{G_{\mathbb{Q}}}(T_p(E))$. We note that $T_K/p^m \cong \mathrm{Ind}_{G_K}^{G_{\mathbb{Q}}}(E[p^m])$. Since $H^2(G_{\mathbb{Q}_p}, E[p]) \cong H^0(G_{\mathbb{Q}_p}, E[p]) = 0$ and $\mathbf{R}\Gamma(G_{\mathbb{Q}_p}, T_K) \otimes^{\mathbb{L}}_{\mathbb{Z}_p[G]} \mathbb{F}_p \cong \mathbf{R}\Gamma(G_{\mathbb{Q}_p}, E[p])$, the perfect complex $\mathbf{R}\Gamma(G_{\mathbb{Q}_p}, T_K)$ is of perfect amplitude in $[1, 1]$. Hence, for any ideal I of $\mathbb{Z}_p[G]$, we have

$$H^1(G_{\mathbb{Q}_p}, T_K) \otimes_{\mathbb{Z}_p[G]} \mathbb{Z}_p[G]/I \xrightarrow{\sim} H^1(G_{\mathbb{Q}_p}, T_K/IT_K).$$

Furthermore, the local Euler characteristic formula implies that $H^1(G_{\mathbb{Q}_p}, T_K/IT_K)$ is a free $\mathbb{Z}_p[G]/I$-module of rank 2. By Proposition 2.11, the $\mathbb{Z}_p/p^m[G]$-module $H^1_f(G_{\mathbb{Q}_p}, T_K/p^m)$ is free of rank 1. Since $\mathbb{Z}_p/p^m[G]$ is a self-injective ring, $H^1_{/f}(G_{\mathbb{Q}_p}, T_K/p^m)$ is also free of rank 1.
Let us show the claim (2). By claim (1), the exact sequence of $\mathbb{Z}_p/p^m[G]$-modules

$$0 \longrightarrow H^1_f(G_{\mathbb{Q}_p}, T_K/p^m) \longrightarrow H^1(G_{\mathbb{Q}_p}, T_K/p^m) \longrightarrow H^1_{/f}(G_{\mathbb{Q}_p}, T_K/p^m) \longrightarrow 0$$

is split. Hence we obtain the exact sequence of free $\mathbb{Z}_p/p^m[\mathrm{Gal}(K'/\mathbb{Q})]$-modules

$$\begin{aligned} 0 \longrightarrow H^1_f(G_{\mathbb{Q}_p}, T_K/p^m)_{\mathrm{Gal}(K/K')} \longrightarrow & H^1(G_{\mathbb{Q}_p}, T_K/p^m)_{\mathrm{Gal}(K/K')} \\ & \longrightarrow H^1_{/f}(G_{\mathbb{Q}_p}, T_K/p^m)_{\mathrm{Gal}(K/K')} \longrightarrow 0. \end{aligned}$$

Since $H^1(G_{\mathbb{Q}_p}, T_K/p^m)_{\mathrm{Gal}(K/K')} \xrightarrow{\sim} H^1(G_{\mathbb{Q}_p}, T_{K'}/p^m)$, the homomorphism

$$H^1_f(G_{\mathbb{Q}_p}, T_K/p^m)_{\mathrm{Gal}(K/K')} \longrightarrow H^1_f(G_{\mathbb{Q}_p}, T_{K'}/p^m)$$

is injective. Hence by claim (1), we obtain isomorphisms

$$H^1_f(G_{\mathbb{Q}_p}, T_K/p^m)_{\mathrm{Gal}(K/K')} \xrightarrow{\sim} H^1_f(G_{\mathbb{Q}_p}, T_{K'}/p^m)$$
$$H^1_{/f}(G_{\mathbb{Q}_p}, T_K/p^m)_{\mathrm{Gal}(K/K')} \xrightarrow{\sim} H^1_{/f}(G_{\mathbb{Q}_p}, T_{K'}/p^m).$$

□

Corollary 2.15. *The Selmer structure $\mathcal{F}_{\mathrm{cl}}$ on T is cartesian.*

Proof. By Proposition 2.9, it suffices to show that the homomorphism

$$H^1_{/f}(G_{\mathbb{Q}_p}, E[p]) \longrightarrow H^1_{/f}(G_{\mathbb{Q}_p}, T)$$

is injective. Note that this map factors through $H^1_{/f}(G_{\mathbb{Q}_p}, E[p^m])$. By Corollary 2.14, the canonical homomorphism $H^1_{/f}(G_{\mathbb{Q}_p}, E[p^m]) \longrightarrow H^1_{/f}(G_{\mathbb{Q}_p}, T)$ is injective. Let us show that $H^1_{/f}(G_{\mathbb{Q}_p}, E[p]) \longrightarrow H^1_{/f}(G_{\mathbb{Q}_p}, E[p^m])$ is injective. Since $H^1(G_{\mathbb{Q}_p}, E[p^m])$ is a free $\mathbb{Z}_p/p^m$-module and $H^1(G_{\mathbb{Q}_p}, E[p^m]) \otimes \mathbb{F}_p \cong H^1(G_{\mathbb{Q}_p}, E[p])$, the canonical homomorphism $H^1(G_{\mathbb{Q}_p}, E[p]) \longrightarrow H^1(G_{\mathbb{Q}_p}, E[p^m])$ is injective. By definition, we have

$$H^1_f(G_{\mathbb{Q}_p}, E[p^m]) \otimes \mathbb{F}_p = \widehat{E}(\mathfrak{m}_{\mathbb{Q}_p})/p^m \otimes \mathbb{F}_p = \widehat{E}(\mathfrak{m}_{\mathbb{Q}_p})/p = H^1_f(G_{\mathbb{Q}_p}, E[p]).$$

Since $H^1_f(G_{\mathbb{Q}_p}, E[p^m]) \cong \mathbb{Z}_p/p^m$ by Corollary 2.14, we see that the canonical homomorphism $H^1_{/f}(G_{\mathbb{Q}_p}, E[p]) \longrightarrow H^1_{/f}(G_{\mathbb{Q}_p}, E[p^m])$ is injective. □

2.3 Kolyvagin systems of rank 1

In this subsection, we recall the definition of Kolyvagin systems of rank 1 introduced by Mazur and Rubin in [11]. We set

$$\mathcal{P}_{m,n} := \{\ell \notin S_{\mathrm{bad}}(E) \mid E(\mathbb{F}_\ell)[p^m] \cong \mathbb{Z}/p^m \text{ and } \ell \equiv 1 \pmod{p^{\max\{m,n+1\}}}\}.$$

For any prime $\ell \in \mathcal{P}_{m,n}$, the R-module $H^1_{\mathrm{ur}}(G_{\mathbb{Q}_\ell}, T) \cong T/(\mathrm{Fr}_\ell - 1)T$ is free of rank 1. Moreover, by [11, Lemmas 1.2.1, 1.2.3 and 1.2.4], we have

$$H^1(G_{\mathbb{Q}_\ell}, T) = H^1_{\mathrm{ur}}(G_{\mathbb{Q}_\ell}, T) \oplus H^1_{\mathrm{tr}}(G_{\mathbb{Q}_\ell}, T)$$

and the R-modules $H^1_{\mathrm{tr}}(G_{\mathbb{Q}_\ell}, T)$, $H^1_{/\mathrm{ur}}(G_{\mathbb{Q}_\ell}, T)$, and $H^1_{/\mathrm{tr}}(G_{\mathbb{Q}_\ell}, T)$ are free of rank 1. Let $\mathcal{N}_{m,n}$ denote the set of square-free products in $\mathcal{P}_{m,n}$. For each integer $d \in \mathcal{N}_{m,n}$, we put

$$G_d := \bigotimes_{\ell \mid d} \mathrm{Gal}(\mathbb{Q}(\ell)/\mathbb{Q}).$$

For any prime $\ell \in \mathcal{P}_{m,n}$, we have two homomorphisms

$$v_\ell \colon H^1(G_{\mathbb{Q}}, T) \xrightarrow{\mathrm{loc}_\ell} H^1(G_{\mathbb{Q}_\ell}, T) \longrightarrow H^1_{/\mathrm{ur}}(G_{\mathbb{Q}_\ell}, T),$$

$$\varphi_\ell^{\mathrm{fs}} \colon H^1(G_{\mathbb{Q}}, T) \xrightarrow{\mathrm{loc}_\ell} H^1(G_{\mathbb{Q}_\ell}, T) \xrightarrow{\mathrm{pr}_{\mathrm{ur}}} H^1_{\mathrm{ur}}(G_{\mathbb{Q}_\ell}, T) \xrightarrow{\phi_\ell^{\mathrm{fs}}} H^1_{/\mathrm{ur}}(G_{\mathbb{Q}_\ell}, T) \otimes_{\mathbb{Z}} G_\ell.$$

Here ϕ_ℓ^{fs} is the finite-singular comparison map defined in [11, Definition 1.2.2] and $\mathrm{pr}_{\mathrm{ur}}$ denotes the projection map with respect to the decomposition $H^1(G_{\mathbb{Q}_\ell}, T) = H^1_{\mathrm{ur}}(G_{\mathbb{Q}_\ell}, T) \oplus H^1_{\mathrm{tr}}(G_{\mathbb{Q}_\ell}, T)$.

Definition 2.16. *We define the module* $\mathrm{KS}_1(T, \mathcal{F}_{\mathrm{can}})$ *of Kolyvagin systems of rank* 1 *to be the set of elements*

$$(\kappa_d)_{d \in \mathcal{N}_{m,n}} \in \prod_{d \in \mathcal{N}_{m,n}} H^1_{\mathcal{F}_{\mathrm{can}}(d)}(G_{\mathbb{Q}}, T) \otimes_{\mathbb{Z}} G_d$$

satisfying the finite-singular relation

$$v_\ell(\kappa_d) = \varphi_\ell^{\mathrm{fs}}(\kappa_{d/\ell})$$

for any integer $d \in \mathcal{N}_{m,n}$ *and any prime* $\ell \mid d$.

For any integer d, we denote by $\nu(d) \in \mathbb{Z}_{\geq 0}$ the number of prime divisors of d.

Lemma 2.17. *Let* $a, b, c \in \mathcal{N}_{m,n}$ *be pairwise relatively prime integers with* $\nu(a) - \nu(b) \geq 1$. *If* $H^1_{(\mathcal{F}^*_{\mathrm{can}})^b_a(c)}(G_{\mathbb{Q}}, E[p]) = 0$, *then the* R*-module* $H^1_{(\mathcal{F}_{\mathrm{can}})^a_b(c)}(G_{\mathbb{Q}}, T)$ *is free of rank* $\nu(a) - \nu(b) + 1$.

Proof. Since $\mathcal{F}_{\mathrm{can}}$ is cartesian by Proposition 2.9, so is $(\mathcal{F}_{\mathrm{can}})^a_b(c)$ by [19, Corollary 3.18]. By [11, Proposition 6.2.2], we have

$$\chi(\mathcal{F}_{\mathrm{can}}) := \dim_{\mathbb{F}_p}(H^1_{\mathcal{F}_{\mathrm{can}}}(G_{\mathbb{Q}}, E[p])) - \dim_{\mathbb{F}_p}(H^1_{\mathcal{F}^*_{\mathrm{can}}}(G_{\mathbb{Q}}, E[p])) = 1,$$

and [19, Corollary 3.21] implies $\chi((\mathcal{F}_{\mathrm{can}})^a_b(c)) = \nu(a) - \nu(b) + 1$. Hence this lemma follows from [19, Lemma 4.6]. $\square$

2.4 Kolyvagin systems of rank 0

In this subsection, we recall the definition of Kolyvagin system of rank 0 in our previous paper [21]. Fix an isomorphism

$$H^1_{/\mathrm{ur}}(G_{\mathbb{Q}_\ell}, T) \cong R$$

for each prime $\ell \in \mathcal{P}_{m,n}$. We then have homomorphisms

$$v_\ell \colon H^1(G_{\mathbb{Q}_\ell}, T) \longrightarrow H^1_{/\mathrm{ur}}(G_{\mathbb{Q}_\ell}, T) \cong R,$$
$$\varphi_\ell^{\mathrm{fs}} \colon H^1(G_{\mathbb{Q}_\ell}, T) \longrightarrow H^1_{/\mathrm{ur}}(G_{\mathbb{Q}_\ell}, T) \otimes_{\mathbb{Z}} G_\ell \cong R \otimes_{\mathbb{Z}} G_\ell.$$

We put $\mathcal{M}_{m,n} := \{(d, \ell) \in \mathcal{N}_{m,n} \times \mathcal{P}_{m,n} \mid \ell \text{ is coprime to } d\}$.

Definition 2.18. *A Kolyvagin system of rank* 0 *is an element*

$$(\kappa_{d,\ell})_{(d,\ell) \in \mathcal{M}_{m,n}} \in \prod_{(d,\ell) \in \mathcal{M}_{m,n}} H^1_{\mathcal{F}^\ell_{\mathrm{cl}}(d)}(G_{\mathbb{Q}}, T) \otimes_{\mathbb{Z}} G_d$$

which satisfies the following relations for any elements $(d, \ell), (d, q), (d\ell, q) \in \mathcal{M}_{m,n}$:

$$v_\ell(\kappa_{d\ell,q}) = \varphi_\ell^{\mathrm{fs}}(\kappa_{d,q}),$$
$$v_\ell(\kappa_{1,\ell}) = v_q(\kappa_{1,q}),$$
$$v_q(\kappa_{d\ell,q}) = -\varphi_\ell^{\mathrm{fs}}(\kappa_{d,\ell}).$$

We denote by $\mathrm{KS}_0(T, \mathcal{F}_{\mathrm{cl}})$ *the module of Kolyvagin systems of rank* 0*. For any Kolyvagin system* $\kappa \in \mathrm{KS}_0(T, \mathcal{F}_{\mathrm{cl}})$ *and any element* $(d, \ell) \in \mathcal{M}_{m,n}$*, we put*

$$\delta(\kappa)_d := v_\ell(\kappa_{d,\ell}) \in R \otimes_{\mathbb{Z}} G_d.$$

Note that, by the definition of Kolyvagin system of rank 0*, the element* $\delta(\kappa)_d$ *is independent of the choice of the prime* $\ell \nmid d$*. Hence we obtain a homomorphism*

$$\delta\colon \mathrm{KS}_0(T, \mathcal{F}_{\mathrm{cl}}) \longrightarrow \prod_{d \in \mathcal{N}_{m,n}} R \otimes_{\mathbb{Z}} G_d.$$

Note that $\mathcal{F}_{\mathrm{cl}} = \mathcal{F}_{\mathrm{cl}}^*$.

Lemma 2.19. *Let* $a, b, c \in \mathcal{N}_{m,n}$ *be pairwise relatively prime integers with* $\nu(a) \geq \nu(b)$*. If* $H^1_{(\mathcal{F}_{\mathrm{cl}})_a^b(c)}(G_{\mathbb{Q}}, E[p]) = 0$*, then the* R*-module* $H^1_{(\mathcal{F}_{\mathrm{cl}})_b^a(c)}(G_{\mathbb{Q}}, T)$ *is free of rank* $\nu(a) - \nu(b)$*.*

Proof. Since $H^1_{(\mathcal{F}_{\mathrm{cl}})_a^b(c)}(G_{\mathbb{Q}}, E[p]) = 0$, Lemma 2.2 shows that $H^1_{(\mathcal{F}_{\mathrm{cl}})_a^b(c)}(G_{\mathbb{Q}}, T) = 0$. Hence applying Theorem 2.1 with $\mathcal{F}_1 = (\mathcal{F}_{\mathrm{cl}})_b^a(c)$ and $\mathcal{F}_2 = (\mathcal{F}_{\mathrm{can}})_b^a(c)$, we obtain an exact sequence

$$0 \longrightarrow H^1_{(\mathcal{F}_{\mathrm{cl}})_b^a(c)}(G_{\mathbb{Q}}, T) \longrightarrow H^1_{(\mathcal{F}_{\mathrm{can}})_b^a(c)}(G_{\mathbb{Q}}, T) \longrightarrow H^1_{/f}(G_{\mathbb{Q}_p}, T) \longrightarrow 0.$$

Hence this lemma follows from Corollary 2.14 and Lemma 2.17. □

Since $\mathcal{F}_{\mathrm{cl}}$ is cartesian by Corollary 2.15, the following theorem is proved in [21, Proposition 5.6, Theorem 5.8].

Theorem 2.20.

(1) For any element $(d, \ell) \in \mathcal{M}_{m,n}$ *satisfying* $H^1_{(\mathcal{F}_{\mathrm{cl}})_\ell(d)}(G_{\mathbb{Q}}, E[p]) = 0$*, the projection map*

$$\mathrm{KS}_0(T, \mathcal{F}_{\mathrm{cl}}) \longrightarrow H^1_{\mathcal{F}_{\mathrm{cl}}^\ell(d)}(G_{\mathbb{Q}}, T) \otimes_{\mathbb{Z}} G_d$$

is an isomorphism. In particular, the R*-module* $\mathrm{KS}_0(T, \mathcal{F}_{\mathrm{cl}})$ *is free of rank* 1*.*

(2) For any basis $\kappa \in \mathrm{KS}_0(T, \mathcal{F}_{\mathrm{cl}})$ *and any integer* $d \in \mathcal{N}_{m,n}$*, we have*

$$R \cdot \delta(\kappa)_d = \mathrm{Fitt}_R^0(H^1_{\mathcal{F}_{\mathrm{cl}}(d)}(G_{\mathbb{Q}}, T)^\vee).$$

Remark 2.21. For any Selmer structure $\mathcal{F}$ on $E[p]$ with $\chi(\mathcal{F}) \geq 0$, there are infinitely many integers $d \in \mathcal{N}_{m,n}$ satisfying $H^1_{\mathcal{F}^*(d)}(G_{\mathbb{Q}}, E[p]) = 0$ (see [11, Corollary 4.1.9]).

Corollary 2.22. *The homomorphism* δ *is injective.*

Proof. Take an integer $d \in \mathcal{N}_{m,n}$ with $H^1_{\mathcal{F}_{\mathrm{cl}}(d)}(G_{\mathbb{Q}}, E[p]) = 0$. Then by Theorem 2.20, we have $\delta(\kappa)_d \in R^\times$. Since the R-module $\mathrm{KS}_0(T, \mathcal{F}_{\mathrm{cl}})$ is free of rank 1 by Theorem 2.20, the map δ is injective. □

2.5 Map from Kolyvagin systems of rank 1 to Kolyvagin systems of rank 0

Fix an isomorphism

$$H^1_{/f}(G_{\mathbb{Q}_p}, T) \cong R.$$

Then we obtain a homomorphism $\varphi\colon H^1(G_{\mathbb{Q}}, T) \longrightarrow H^1_{/f}(G_{\mathbb{Q}_p}, T) \cong R$. We also denote by $\varphi\colon \mathrm{KS}_1(T, \mathcal{F}_{\mathrm{can}}) \longrightarrow \prod_{d \in \mathcal{N}_{m,n}} R \otimes_{\mathbb{Z}} G_d$ the homomorphism induced by φ. In this subsection, we construct a natural map $\mathrm{KS}_1(T, \mathcal{F}_{\mathrm{can}}) \longrightarrow \mathrm{KS}_0(T, \mathcal{F}_{\mathrm{cl}})$ such that the diagram

$$\begin{tikzcd} \mathrm{KS}_1(T, \mathcal{F}_{\mathrm{can}}) \arrow[r] \arrow[dr, "\varphi"'] & \mathrm{KS}_0(T, \mathcal{F}_{\mathrm{cl}}) \arrow[d, "\delta"] \\ & \prod_{d \in \mathcal{N}_{m,n}} R \otimes_{\mathbb{Z}} G_d \end{tikzcd} \tag{2}$$

commutes. In order to construct this map, we introduce the module of Stark systems.

For any R-module M, we put

$$M^* := \mathrm{Hom}_R(M, R) \;\text{ and }\; \bigcap\nolimits_R^r M := \left(\bigwedge\nolimits_R^r M^*\right)^*$$

for any integer $r \geq 0$. Since the functor $M \mapsto M^*$ is exact, an R-homomorphism $\phi\colon M \longrightarrow F$, where F is free of rank 1, induces a natural homomorphism

$$\phi\colon \bigcap\nolimits_R^{r+1} M \longrightarrow F \otimes_R \bigcap\nolimits_R^r \ker(\phi).$$

Definition 2.23. *Let $\mathcal{F}$ be a Selmer structure on T. For any integers $d \in \mathcal{N}_{m,n}$ and $r \geq 0$, define*

$$W_d := \bigoplus_{\ell \mid d} H^1_{/\mathrm{ur}}(G_{\mathbb{Q}_\ell}, T)^*,$$
$$X_d^r(T, \mathcal{F}) := \bigcap\nolimits_R^{r+\nu(d)} H^1_{\mathcal{F}^d}(G_{\mathbb{Q}}, T) \otimes_R \det(W_d).$$

Then for any positive divisor e of d, the exact sequence

$$0 \longrightarrow H^1_{\mathcal{F}^e}(G_{\mathbb{Q}}, T) \longrightarrow H^1_{\mathcal{F}^d}(G_{\mathbb{Q}}, T) \longrightarrow \bigoplus_{\ell \mid \frac{d}{e}} H^1_{/\mathrm{ur}}(G_{\mathbb{Q}_\ell}, T)$$

induces a natural homomorphism

$$\Phi_{d,e}\colon X_d^r(T, \mathcal{F}) \longrightarrow X_e^r(T, \mathcal{F})$$

(see [19, Definition 2.3]). If $f \mid e \mid d$, then we have $\Phi_{d,f} = \Phi_{e,f} \circ \Phi_{d,e}$ (see [19, Proposition 2.4]), and we obtain the module of Stark systems of rank r

$$\mathrm{SS}_r(T, \mathcal{F}) := \varprojlim_{d \in \mathcal{N}_{m,n}} X_d^r(T, \mathcal{F}).$$

Since we have the isomorphisms

$$H^1_{\mathrm{ur}}(G_{\mathbb{Q}_\ell}, T) \xrightarrow{\phi_\ell^{\mathrm{fs}}} H^1_{/\mathrm{ur}}(G_{\mathbb{Q}_\ell}, T) \otimes_{\mathbb{Z}} G_\ell \quad \text{and} \quad H^1_{\mathrm{ur}}(G_{\mathbb{Q}_\ell}, T) \xrightarrow{\sim} H^1_{/\mathrm{tr}}(G_{\mathbb{Q}_\ell}, T)$$

for any prime $\ell \mid d$, we see that the exact sequence

$$0 \longrightarrow H^1_{\mathcal{F}_{\mathrm{can}}(d)}(G_{\mathbb{Q}}, T) \longrightarrow H^1_{\mathcal{F}^d_{\mathrm{can}}}(G_{\mathbb{Q}}, T) \longrightarrow \bigoplus_{\ell \mid d} H^1_{/\mathrm{tr}}(G_{\mathbb{Q}_\ell}, T)$$

induces a natural homomorphism

$$\Pi_d \colon X^1_d(T, \mathcal{F}_{\mathrm{can}}) \longrightarrow {\bigcap}^1_R H^1_{\mathcal{F}_{\mathrm{can}}(d)}(G_{\mathbb{Q}}, T) \otimes_{\mathbb{Z}} G_d = H^1_{\mathcal{F}_{\mathrm{can}}(d)}(G_{\mathbb{Q}}, T) \otimes_{\mathbb{Z}} G_d,$$

and we obtain

$$\mathrm{Reg}_1 \colon \mathrm{SS}_1(T, \mathcal{F}_{\mathrm{can}}) \longrightarrow \mathrm{KS}_1(T, \mathcal{F}_{\mathrm{can}});\ (\epsilon_d)_{d \in \mathcal{N}_{m,n}} \mapsto ((-1)^{\nu(d)} \Pi_d(\epsilon_d))_{d \in \mathcal{N}_{m,n}}$$

(see [2, Proposition 4.3] or [12, Proposition 12.3]). The following important proposition is proved by Mazur and Rubin in [12, Proposition 12.4] (see also [1, Theorem 5.2(i)] and [20, Theorem 3.17]).

Theorem 2.24. *The map*

$$\mathrm{Reg}_1 \colon \mathrm{SS}_1(T, \mathcal{F}_{\mathrm{can}}) \longrightarrow \mathrm{KS}_1(T, \mathcal{F}_{\mathrm{can}})$$

is an isomorphism.

For any integer $d \in \mathcal{N}_{m,n}$, the exact sequence

$$0 \longrightarrow H^1_{\mathcal{F}_{\mathrm{cl}}(d)}(G_{\mathbb{Q}}, T) \longrightarrow H^1_{\mathcal{F}^d_{\mathrm{cl}}}(G_{\mathbb{Q}}, T) \longrightarrow \bigoplus_{\ell \mid d} H^1_{/\mathrm{tr}}(G_{\mathbb{Q}_\ell}, T)$$

induces a natural homomorphism

$$\Pi'_d \colon X^0_d(T, \mathcal{F}_{\mathrm{cl}}) \longrightarrow {\bigcap}^0_R H^1_{\mathcal{F}_{\mathrm{cl}}(d)}(G_{\mathbb{Q}}, T) \otimes_{\mathbb{Z}} G_d = R \otimes_{\mathbb{Z}} G_d.$$

Hence we obtain a homomorphism

$$\psi \colon \mathrm{SS}_0(T, \mathcal{F}_{\mathrm{cl}}) \longrightarrow \prod_{d \in \mathcal{N}_{m,n}} R \otimes_{\mathbb{Z}} G_d;\ (\epsilon_d)_{d \in \mathcal{N}_{m,n}} \mapsto (\Pi'_d(\epsilon_d))_{d \in \mathcal{N}_{m,n}}.$$

In [21, §5.2], we construct the canonical homomorphism

$$\mathrm{Reg}_0 \colon \mathrm{SS}_0(T, \mathcal{F}_{\mathrm{cl}}) \longrightarrow \mathrm{KS}_0(T, \mathcal{F}_{\mathrm{cl}})$$

such that the diagram

$$\begin{tikzcd} \mathrm{SS}_0(T, \mathcal{F}_{\mathrm{cl}}) \arrow[r, "\mathrm{Reg}_0"] \arrow[dr, "\psi"'] & \mathrm{KS}_0(T, \mathcal{F}_{\mathrm{cl}}) \arrow[d, "\delta"] \\ & \prod_{d \in \mathcal{N}_{m,n}} R \otimes_{\mathbb{Z}} G_d \end{tikzcd} \tag{3}$$

commutes.
For any integer $d \in \mathcal{N}_{m,n}$, we have an exact sequece

$$0 \longrightarrow H^1_{\mathcal{F}^d_{\mathrm{cl}}}(G_{\mathbb{Q}}, T) \longrightarrow H^1_{\mathcal{F}^d_{\mathrm{can}}}(G_{\mathbb{Q}}, T) \xrightarrow{\varphi} R.$$

This exact sequence induces a homomorphism $X^1_d(T, \mathcal{F}_{\mathrm{can}}) \longrightarrow X^0_d(T, \mathcal{F}_{\mathrm{cl}})$, and we obtain a homomorphism $\mathrm{SS}_1(T, \mathcal{F}_{\mathrm{can}}) \longrightarrow \mathrm{SS}_0(T, \mathcal{F}_{\mathrm{cl}})$. By construction, the diagram

$$\begin{tikzcd}
\mathrm{SS}_1(T, \mathcal{F}_{\mathrm{can}}) \arrow[r] \arrow[d, "\mathrm{Reg}_1"] & \mathrm{SS}_0(T, \mathcal{F}_{\mathrm{cl}}) \arrow[d, "\psi"] \\
\mathrm{KS}_1(T, \mathcal{F}_{\mathrm{can}}) \arrow[r, "\varphi"] & \prod_{d \in \mathcal{N}_{m,n}} R \otimes_{\mathbb{Z}} G_d
\end{tikzcd} \tag{4}$$

commutes. Since Reg_1 is an isomorphism, by using the commutative diagrams (3) and (4), we obtain the homomorphism $\mathrm{KS}_1(T, \mathcal{F}_{\mathrm{can}}) \longrightarrow \mathrm{KS}_0(T, \mathcal{F}_{\mathrm{cl}})$ such that the diagram (2) commutes.

3 Construction of the Kolyvagin system of rank 0 from modular symbols

Let $p \geq 3$ be a prime satisfying the hypotheses (a), (b), and (c). For any finite abelian extension $K/\mathbb{Q}$, we put

$$R_K := \mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})] \quad \text{and} \quad T_K := \mathrm{Ind}^{G_{\mathbb{Q}}}_{G_K}(T_p(E)).$$

3.1 Modular sysmbols

We recall the definition of the Mazur–Tate elements. For any integer $d \geq 1$, we define the modular element $\widetilde{\theta}_{\mathbb{Q}(\mu_d)}$ by

$$\widetilde{\theta}_{\mathbb{Q}(\mu_d)} := \sum_{\substack{a=1 \\ (a,d)=1}}^{d} \frac{\mathrm{Re}([a/d])}{\Omega^+_E} \sigma_a \in \mathbb{Q}[\mathrm{Gal}(\mathbb{Q}(\mu_d)/\mathbb{Q})].$$

Here $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\mu_d)/\mathbb{Q})$ is the element satisfying $\sigma_a(\zeta) = \zeta^a$ for any $\zeta \in \mu_d$. For any integer $e \mid d$, we put

$$\nu_{d,e} \colon R_{\mathbb{Q}(\mu_e)} \longrightarrow R_{\mathbb{Q}(\mu_d)};\, x \mapsto \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_d)/\mathbb{Q}(\mu_e))} \sigma x.$$

Define $\mathcal{P} := \{\ell \neq p \mid E \text{ has good reduction at } \ell\}$ and $\mathcal{N}$ denotes the set of square-free products in $\mathcal{P}$. Since $G_{\mathbb{Q}} \longrightarrow \mathrm{GL}(E[p])$ is surjective, for any integers $d \in \mathcal{N}$ and $n \geq 1$, we have

$$\widetilde{\theta}_{\mathbb{Q}(\mu_{dp^n})} \in R_{\mathbb{Q}(\mu_{dp^n})}$$

(see [23]). Let $\alpha \in \mathbb{Z}_p^\times$ be the unit root of $x^2 - a_p x + p = 0$, where $a_p := p + 1 - \#E(\mathbb{F}_p)$. We set

$$\vartheta_{\mathbb{Q}(\mu_{dp^n})} := \alpha^{-n}(\widetilde{\theta}_{\mathbb{Q}(\mu_{dp^n})} - \alpha^{-1}\nu_{dp^n,dp^{n-1}}(\widetilde{\theta}_{\mathbb{Q}(\mu_{dp^{n-1}})})) \in R_{\mathbb{Q}(\mu_{dp^n})}.$$

Then the set $\{\vartheta_{\mathbb{Q}(\mu_{dp^n})}\}_{n\geq 1}$ is a projective system and we get an element

$$\vartheta_{\mathbb{Q}(\mu_{dp^\infty})} := \varprojlim_n \vartheta_{\mathbb{Q}(\mu_{dp^n})} \in \varprojlim_n R_{\mathbb{Q}(\mu_{dp^n})} =: \Lambda_{\mathbb{Q}(\mu_{dp^\infty})}.$$

Remark 3.1. Note that for any positive integer $p \nmid d$, we have

$$\vartheta_{\mathbb{Q}(\mu_d)} = \left(1 - \alpha^{-1}\sigma_p\right)\left(1 - \alpha^{-1}\sigma_p^{-1}\right)\widetilde{\theta}_{\mathbb{Q}(\mu_d)}.$$

The assumption (c) shows that $\alpha \not\equiv 1 \pmod p$, and $\left(1 - \alpha^{-1}\sigma_p\right)\left(1 - \alpha^{-1}\sigma_p^{-1}\right)$ is a unit in $R_{\mathbb{Q}(\mu_d)}$.

For any prime ℓ with $\ell \nmid d$, let $\pi_{\ell d,d} \colon \Lambda_{\mathbb{Q}(\mu_{\ell dp^\infty})} \longrightarrow \Lambda_{\mathbb{Q}(\mu_{dp^\infty})}$ denote the natural projection map, and we have

$$\pi_{\ell d,d}(\vartheta_{\mathbb{Q}(\mu_{\ell dp^\infty})}) = (a_\ell - \sigma_\ell - \sigma_\ell^{-1})\vartheta_{\mathbb{Q}(\mu_{dp^\infty})}.$$

Here $a_\ell := \ell + 1 - \#E(\mathbb{F}_\ell)$. Following Kurihara in [10, page 324], for any positive divisor e of d, we put

$$\alpha_{d,e} := \left(\prod_{\ell \mid \frac{d}{e}} (-\sigma_\ell^{-1})\right)\vartheta_{\mathbb{Q}(\mu_{ep^\infty})} \in \Lambda_{\mathbb{Q}(\mu_{ep^\infty})},$$

$$\xi_{\mathbb{Q}(\mu_{dp^\infty})} := \sum_{e \mid d} \nu_{d,e}(\alpha_{d,e}) \in \Lambda_{\mathbb{Q}(\mu_{dp^\infty})}.$$

Here e runs over the set of positive divisors of d. We also put

$$\widetilde{\xi}_{\mathbb{Q}(\mu_{dp^\infty})} := \left(\prod_{\ell \mid d} -\ell^{-1}\sigma_\ell\right)\xi_{\mathbb{Q}(\mu_{dp^\infty})}.$$

Definition 3.2. *For any prime $\ell \in \mathcal{P}$, we define the Frobenius polynomial at ℓ by*

$$P_\ell(t) := \det(1 - t\sigma_\ell^{-1} \mid T_p(E)) = 1 - \ell^{-1}a_\ell t + \ell^{-1}t^2.$$

Proposition 3.3. *For any integer $d \in \mathcal{N}$ and any prime $\ell \in \mathcal{P}$ with $\ell \nmid d$, we have*

$$\pi_{d\ell,d}(\widetilde{\xi}_{\mathbb{Q}(\mu_{\ell dp^\infty})}) = P_\ell(\sigma_\ell^{-1})\widetilde{\xi}_{\mathbb{Q}(\mu_{dp^\infty})}.$$

Proof. Kurihara showed in [10, page 325, (7)] that

$$\begin{aligned}\pi_{d\ell,d}(\xi_{\mathbb{Q}(\mu_{\ell dp^\infty})}) &= (-\sigma_\ell + a_\ell - \ell\sigma_\ell^{-1})\xi_{\mathbb{Q}(\mu_{dp^\infty})}\\ &= (-\ell\sigma_\ell^{-1})P_\ell(\sigma_\ell^{-1})\xi_{\mathbb{Q}(\mu_{dp^\infty})},\end{aligned}$$

which implies $\pi_{d\ell,d}(\widetilde{\xi}_{\mathbb{Q}(\mu_{\ell dp^\infty})}) = P_\ell(\sigma_\ell^{-1})\widetilde{\xi}_{\mathbb{Q}(\mu_{dp^\infty})}$. □

3.2 Coleman maps

Let $K/\mathbb{Q}$ be a finite p-abelian extension at which p is unramified, and we denote by K_∞/K the cyclotomic $\mathbb{Z}_p$-extension. Put

$$\Lambda_{K_\infty} := \mathbb{Z}_p[[\mathrm{Gal}(K_\infty/\mathbb{Q})]] \quad \text{and} \quad \mathbb{T}_{K_\infty} := \varprojlim_n T_{K_n},$$

where K_n denotes the n-th layer of the cyclotomic $\mathbb{Z}_p$-extension K_∞/K. We note that the Λ_{K_∞}-module $H^1_{/f}(G_\mathbb{Q}, \mathbb{T}_{K_\infty}) := \varprojlim_{m,n} H^1_{/f}(G_{\mathbb{Q}_p}, T_{K_n}/p^m)$ is free of rank 1 by Corollary 2.14. Let

$$\widetilde{\xi}_{K_\infty} \in \Lambda_{K_\infty}$$

denote the image of $\widetilde{\xi}_{\mathbb{Q}(\mu_{dp^\infty})}$ under the canonical homomorphism $\Lambda_{\mathbb{Q}(\mu_{dp^\infty})} \longrightarrow \Lambda_{K_\infty}$, where d is the conductor of K.

The following theorem follows from the works of Perrin-Riou in [17] and Kato in [4].

Theorem 3.4 ([4, Theorem 16.4, Theorem 16.6, and Proposition 17.11]). *There exists an isomorphism*

$$\mathfrak{L}_{K_\infty} \colon H^1_{/f}(G_{\mathbb{Q}_p}, \mathbb{T}_{K_\infty}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \xrightarrow{\sim} \Lambda_{K_\infty} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

such that

(i) the diagram

$$\begin{tikzcd}
H^1_{/f}(G_{\mathbb{Q}_p}, \mathbb{T}_{K_\infty}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \arrow[r, "\mathfrak{L}_{K_\infty}"] \arrow[d] & \Lambda_{K_\infty} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \arrow[d] \\
H^1_{/f}(G_{\mathbb{Q}_p}, \mathbb{T}_{L_\infty}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \arrow[r, "\mathfrak{L}_{L_\infty}"] & \Lambda_{L_\infty} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p
\end{tikzcd}$$

commutes for any field $L \subset K$, where the vertical maps are the natural projections,

(ii) $\mathfrak{L}_{\mathbb{Q}_\infty}(H^1_{/f}(G_{\mathbb{Q}_p}, \mathbb{T}_{\mathbb{Q}_\infty})) = \Lambda_{\mathbb{Q}_\infty}$,

(iii) there is an element $z_{K_\infty} \in H^1(G_\mathbb{Q}, \mathbb{T}_{K_\infty})$ such that $\mathfrak{L}_{K_\infty}(\mathrm{loc}_p^{/f}(z_{K_\infty})) = \widetilde{\xi}_{K_\infty}$, where $\mathrm{loc}_p^{/f} \colon H^1(G_\mathbb{Q}, \mathbb{T}_{K_\infty}) \longrightarrow H^1_{/f}(G_{\mathbb{Q}_p}, \mathbb{T}_{K_\infty})$ denotes the localization homomorphism.

Remark 3.5.

(1) The homomorphism $\mathfrak{L}_{K_\infty}$ interpolates the dual exponential maps, however this fact is not used in this paper.

(2) The integrality of the element z_{K_∞} follows from the assumption (b) (see [3, Theorem 6.1]).

(3) There are many papers that use $\widetilde{\theta}^{\#}_{\mathbb{Q}(\mu_d)}$ instead of $\widetilde{\theta}_{\mathbb{Q}(\mu_d)}$, where $(-)^{\#}$ denotes the involution on the group ring that sends each group-like element σ to its inverse σ^{-1}. However, $\widetilde{\theta}_{\mathbb{Q}(\mu_d)}$ has a functional equation (see [13, (1.6.2)]), and hence the difference does not matter.

3.3 Euler systems

In this subsection, we recall the definition of Euler systems.

Definition 3.6.

(1) Let Ω denote the set of fields K in $\overline{\mathbb{Q}}$ such that $K/\mathbb{Q}$ is a finite abelian p-extension and $S_{\mathrm{ram}}(K/\mathbb{Q}) \subset \mathcal{P}$. Here $S_{\mathrm{ram}}(K/\mathbb{Q})$ is the set of primes at which $K/\mathbb{Q}$ is ramified.

(2) We say that $(c_K)_{K\in\Omega} \in \prod_{K\in\Omega} H^1(G_{\mathbb{Q}}, \mathbb{T}_{K_\infty})$ is an Euler system of rank 1 if, for any fields $K_1 \subset K_2$ in Ω, we have

$$\mathrm{Cor}_{K_2/K_1}(c_{K_2}) = \left(\prod_{\ell\in S_{\mathrm{ram}}(K_2/\mathbb{Q})\setminus S_{\mathrm{ram}}(K_1/\mathbb{Q})} P_\ell(\sigma_\ell^{-1})\right) c_{K_1}.$$

Here $\mathrm{Cor}_{K_2/K_1}\colon H^1(G_{\mathbb{Q}}, \mathbb{T}_{K_{2,\infty}}) \longrightarrow H^1(G_{\mathbb{Q}}, \mathbb{T}_{K_{1,\infty}})$ denotes the homomorphism induced by $\mathbb{T}_{K_{2,\infty}} \longrightarrow \mathbb{T}_{K_{1,\infty}}$. Let $\mathrm{ES}_1(T)$ denote the set of Euler systems of rank 1.

(3) We say that $(c_K)_{K\in\Omega} \in \prod_{K\in\Omega} \Lambda_{K_\infty}$ is an Euler system of rank 0 if, for any fields $K_1 \subset K_2$ in Ω, we have

$$\pi_{K_2,K_1}(c_{K_2}) = \left(\prod_{\ell\in S_{\mathrm{ram}}(K_2/\mathbb{Q})\setminus S_{\mathrm{ram}}(K_1/\mathbb{Q})} P_\ell(\sigma_\ell^{-1})\right) c_{K_1}.$$

Here $\pi_{K_2,K_1}\colon \Lambda_{K_{2,\infty}} \longrightarrow \Lambda_{K_{1,\infty}}$ denotes the canonical projection map. Let $\mathrm{ES}_0(T)$ denote the set of Euler systems of rank 0.

Proposition 3.3 implies the following proposition.

Proposition 3.7. *We have $(\widetilde{\xi}_{K_\infty})_{K\in\Omega} \in \mathrm{ES}_0(T)$.*

Let $K \in \Omega$ be a field. Then, by Theorem 2.1, for any integers $m \geq 1$ and $n \geq 0$, we have an exact sequence

$$\begin{aligned}0 \longrightarrow \mathrm{Sel}(K_n, E[p^m]) \longrightarrow H^1_{\mathcal{F}_{\mathrm{can}}}&(G_{\mathbb{Q}}, T_{K_n}/p^m)\\ &\longrightarrow H^1_{/f}(G_{\mathbb{Q}_p}, T_{K_n}/p^m) \longrightarrow \mathrm{Sel}(K_n, E[p^m])^\vee.\end{aligned}$$

Here $\mathrm{Sel}(K_n, E[p^m])$ is the p^m-Selmer group of E/K_n and

$$H^1_{\mathcal{F}_{\mathrm{can}}}(G_{\mathbb{Q}}, T_{K_n}/p^m) := \ker\left(H^1(G_{\mathbb{Q}}, T_{K_n}/p^m) \longrightarrow \bigoplus_{\ell\neq p} H^1_{/\mathrm{ur}}(G_{\mathbb{Q}_\ell}, T_{K_n}/p^m)\right).$$

We set

$$\mathrm{Sel}(K_\infty, E[p^\infty]) := \varinjlim_{m,n} \mathrm{Sel}(K_n, E[p^m]).$$

Since $\mathrm{Sel}(K_\infty, E[p^\infty])^\vee$ is a finitely generated torsion Λ_{K_∞}-module, we have

$$\varprojlim_{m,n} \mathrm{Sel}(K_n, E[p^m]) = 0.$$

Moreover, [18, Proposition B.3.4] implies

$$H^1(G_{\mathbb{Q}}, \mathbb{T}_{K_\infty}) = \varprojlim_{m,n} H^1_{\mathcal{F}_{\mathrm{can}}}(G_{\mathbb{Q}}, T_{K_n}/p^m).$$

Hence we get an exact sequence of Λ_{K_∞}-modules

$$0 \longrightarrow H^1(G_{\mathbb{Q}}, \mathbb{T}_{K_\infty}) \xrightarrow{\mathrm{loc}_p^{/f}} H^1_{/f}(G_{\mathbb{Q}_p}, \mathbb{T}_{K_\infty}) \longrightarrow \mathrm{Sel}(K_\infty, E[p^\infty])^\vee. \tag{5}$$

For each field $K \in \Omega$, we put

$$M_{K_\infty} := (\mathrm{loc}_p^{/f})^{-1}(H^1(G_{\mathbb{Q}_p}, \mathbb{T}_{K_\infty}) \cap \mathfrak{L}_{K_\infty}^{-1}(\Lambda_{K_\infty})),$$

and we obtain an injection

$$\mathfrak{L}\colon \mathrm{ES}_1(T) \cap \prod_{K\in\Omega} M_{K_\infty} \hookrightarrow \mathrm{ES}_0(T); (c_K)_{K\in\Omega} \mapsto (\mathrm{loc}_p^{/f}(\mathfrak{L}_{K_\infty}(c_K)))_{K\in\Omega}.$$

Then Theorem 3.4 and the injectivity of $\mathrm{loc}_p^{/f} \circ \mathfrak{L}_{K_\infty}$ imply the following proposition.

Proposition 3.8. *There is an Euler system $z_\xi \in \mathrm{ES}_1(T) \cap \prod_{K\in\Omega} M_{K_\infty}$ such that $\mathfrak{L}(z_\xi) = (\widetilde{\xi}_{K_\infty})_{K\in\Omega}$.*

Remark 3.9. Since our p-adic L function $\widetilde{\xi}_{K_\infty}$ is modified, the Euler system z_ξ differs slightly from that of Kato.

3.4 Construction of $\kappa_{\xi,m,n}$

Fix integers $m \geq 1$ and $n \geq 0$. First, we introduce the Kolyvagin derivative homomorphism (defined by Mazur and Rubin in [11])

$$\mathcal{D}^1_{m,n}\colon \mathrm{ES}_1(T) \longrightarrow \mathrm{KS}_1(T_{\mathbb{Q}_n}/p^m, \mathcal{F}_{\mathrm{can}}).$$

Recall that $\mathbb{Q}(d)$ is the maximal p-subextension of $\mathbb{Q}(\mu_d)$, and note that $\mathbb{Q}_n = \mathbb{Q}(p^{n+1})$. We fix a generator g_ℓ of $G_\ell = \mathrm{Gal}(\mathbb{Q}(\ell)/\mathbb{Q})$ for each prime $\ell \in \mathcal{P}_{1,0}$ and denote by $D_\ell \in \mathbb{Z}[G_\ell]$ the Kolyvagin's derivative operator:

$$D_\ell := \sum_{i=0}^{\#G_\ell - 1} i g_\ell^i.$$

For any integer $d \in \mathcal{N}_{1,0}$, we also set $D_d := \prod_{\ell \mid d} D_\ell \in \mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(d)/\mathbb{Q})]$.
Let $c \in \mathrm{ES}_1(T)$ be an Euler system. For any integer $d \in \mathcal{N}_{m,n}$, we denote by $c_{dp^{n+1}} \in H^1(G_\mathbb{Q}, T_{\mathbb{Q}(dp^{n+1})})$ the image of $c_{\mathbb{Q}(d)} \in H^1(G_\mathbb{Q}, \mathbb{T}_{\mathbb{Q}(d)})$. Then it is well-known that Euler system relations imply

$$\kappa(c)_{d,m,n} := D_d c_{dp^{n+1}} \bmod p^m \in H^1(G_\mathbb{Q}, T_{\mathbb{Q}(dp^{n+1})}/p^m)^{\mathrm{Gal}(\mathbb{Q}(d)/\mathbb{Q})}.$$

(see, for example, [18, Lemma 4.4.2]). Since we have an isomorphism

$$H^1(G_\mathbb{Q}, T_{\mathbb{Q}_n}/p^m) \xrightarrow{\sim} H^1(G_\mathbb{Q}, T_{\mathbb{Q}(dp^{n+1})}/p^m)^{\mathrm{Gal}(\mathbb{Q}(d)/\mathbb{Q})},$$

we can regard $\kappa(c)_{d,m,n}$ as an element of $H^1(G_\mathbb{Q}, T_{\mathbb{Q}_n}/p^m)$. The following theorem is proved by Mazur and Rubin in [11, Appendix A].

Theorem 3.10. *For any Euler system $c \in \mathrm{ES}_1(T)$, we have*

$$\mathcal{D}^1_{m,n}(c) := (\kappa(c)_{d,m,n} \otimes g_d)_{d \in \mathcal{N}_{m,n}} \in \mathrm{KS}_1(T_{\mathbb{Q}_n}/p^m, \mathcal{F}_{\mathrm{can}}).$$

Here $g_d := \prod_{\ell \mid d} g_\ell$. Hence we obtain the Kolyvagin derivative homomorphism

$$\mathcal{D}^1_{m,n} \colon \mathrm{ES}_1(T) \longrightarrow \mathrm{KS}_1(T_{\mathbb{Q}_n}/p^m, \mathcal{F}_{\mathrm{can}}).$$

Remark 3.11. For any prime $\ell \in \mathcal{P}_{m,n}$, we have

$$P_\ell(t) \equiv (t-1)^2 \pmod{p^m}.$$

This fact implies that $P_\ell(\mathrm{Fr}_\ell^{-1})$ vanishes in the module $\mathcal{A}_{\ell,I}/\mathcal{A}^2_{\ell,I}$. Here $\mathcal{A}_{\ell,I}$ denotes the argumentation ideal defined in [11, Definition A.3]. Hence we see that $\kappa(c)_{d,m,n}$ coincides with κ'_n defined in [11, page 80, (33)].

Next let us construct a homomorphism

$$\mathcal{D}^0_{m,n} \colon \mathrm{ES}_0(T) \longrightarrow \prod_{d \in \mathcal{N}_{m,n}} R_{\mathbb{Q}_n}/p^m \otimes_\mathbb{Z} G_d.$$

Let $c \in \mathrm{ES}_0(T)$ be an Euler system and take an integer $d \in \mathcal{N}_{m,n}$. We denote by $c_{dp^{n+1}} \in R_{\mathbb{Q}(dp^{n+1})}$ the image of $c_{\mathbb{Q}(d)} \in \Lambda_{\mathbb{Q}(d)}$.
The following lemma is well-known (see, for example, [18, Lemma 4.4.2]).

Lemma 3.12. *For any integer $d \in \mathcal{N}_{m,n}$, we have*

$$\delta(c)_{d,m,n} := D_d c_{dp^{n+1}} \bmod p^m \in (R_{\mathbb{Q}(dp^{n+1})}/p^m)^{\mathrm{Gal}(\mathbb{Q}(d)/\mathbb{Q})} \xleftarrow{\sim} R_{\mathbb{Q}_n}/p^m.$$

We often regard $\delta(c)_{d,m,n}$ as an element of $R_{\mathbb{Q}_n}/p^m$ by using the isomorphism

$$R_{\mathbb{Q}_n}/p^m \xrightarrow{\sim} (R_{\mathbb{Q}(dp^{n+1})}/p^m)^{\mathrm{Gal}(\mathbb{Q}(d)/\mathbb{Q})}; x \mapsto xN_d.$$

Here $N_d := \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(d)/\mathbb{Q})} \sigma$.

Lemma 3.13. *Let*

$$c = \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(d)/\mathbb{Q})} a_\sigma \sigma \in R_{\mathbb{Q}(dp^{n+1})}/p^m$$

where $a_\sigma \in R_{\mathbb{Q}_n}/p^m$*. If* $D_d c \in (R_{\mathbb{Q}(dp^{n+1})}/p^m)^{\mathrm{Gal}(\mathbb{Q}(d)/\mathbb{Q})}$*, then we have*

$$D_d c = (-1)^{\nu(d)} \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(d)/\mathbb{Q})} a_\sigma \prod_{\ell \mid d} \overline{\log}_{g_\ell}(\sigma).$$

Here we regard $D_d c$ *as an element of* $R_{\mathbb{Q}_n}/p^m$ *by using the isomorphism*

$$R_{\mathbb{Q}_n}/p^m \xrightarrow{\sim} (R_{\mathbb{Q}(dp^{n+1})}/p^m)^{\mathrm{Gal}(\mathbb{Q}(d)/\mathbb{Q})}; x \mapsto xN_d$$

and

$$\overline{\log}_{g_\ell} \colon G_\ell \xrightarrow{\sim} \mathbb{Z}/(\ell-1) \longrightarrow \mathbb{Z}/p^m;\ g_\ell^a \mapsto a \bmod p^m$$

is the surjection induced by the discrete logarithm to the base g_ℓ*.*

Proof. We write $d = \ell_1 \cdots \ell_t$. We put

$$N_{\ell_i} := \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\ell_i)/\mathbb{Q})} \sigma \quad \text{and} \quad X_{\ell_i} := g_{\ell_i} - 1.$$

Note that

$$D_{\ell_i} X_{\ell_i} \equiv -N_{\ell_i} \pmod{p^m} \quad \text{and} \quad D_{\ell_i} X_{\ell_i}^2 \equiv 0 \pmod{p^m}.$$

Hence we have

$$\begin{aligned} D_d \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(d)/\mathbb{Q})} a_\sigma \sigma &= \sum_{i_1=1}^{\#G_{\ell_1}-1} \cdots \sum_{i_t=1}^{\#G_{\ell_t}-1} a_{g_{\ell_1}^{i_1} \cdots g_{\ell_t}^{i_t}} D_d (1+X_{\ell_1})^{i_1} \cdots (1+X_{\ell_t})^{i_t} \\ &= \sum_{i_1=1}^{\#G_{\ell_1}-1} \cdots \sum_{i_t=1}^{\#G_{\ell_t}-1} a_{g_{\ell_1}^{i_1} \cdots g_{\ell_t}^{i_t}} (1 - i_1 N_{\ell_1}) \cdots (1 - i_t N_{\ell_t}) \\ &=: \sum_{i=1}^{t} \sum_{j_i \in \{0,1\}} b_{j_1,\dots,j_t} N_{\ell_1}^{j_1} \cdots N_{\ell_t}^{j_t}. \end{aligned}$$

Since

$$b_{1,\dots,1} = (-1)^{\nu(d)} \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(d)/\mathbb{Q})} a_\sigma \prod_{\ell \mid d} \overline{\log}_{g_\ell}(\sigma),$$

it suffices to show that $b_{j_1,\dots,j_t} = 0$ for any $(j_1,\dots,j_t) \neq (1,\dots,1)$. This follows from the assumption that $D_d c \in (R_{\mathbb{Q}(dp^{n+1})}/p^m)^{\mathrm{Gal}(\mathbb{Q}(d)/\mathbb{Q})}$. In fact, we have $X_{\ell_i} D_d c = 0$ and $X_{\ell_i} N_{\ell_i} = 0$ for any $1 \le i \le t$. Hence we have

$$0 = X_{\ell_1} \cdots X_{\ell_t} D_d c = b_{0,\dots,0} X_{\ell_1} \cdots X_{\ell_t},$$

and $b_{0,\dots,0} = 0$. Moreover, since

$$0 = X_{\ell_2} \cdots X_{\ell_t} D_d c = b_{0,\dots,0} X_{\ell_2} \cdots X_{\ell_t} + b_{1,0,\dots,0} N_{\ell_1} X_{\ell_2} \cdots X_{\ell_t},$$

we have $b_{1,0,\dots,0} = 0$. Similary, we have $b_{0,1,\dots,0} = \cdots = b_{0,\dots,0,1} = 0$. Repeating this argument, we see that $b_{j_1,\dots,j_t} = 0$ for any $(j_1, \dots, j_t) \neq (1, \dots, 1)$. □

The following lemma is used to prove Theorem 1.15.

Lemma 3.14. *Let $\vartheta_{\mathbb{Q}(dp^n)}$ denote the image of $\vartheta_{\mathbb{Q}(\mu_{dp^{n+1}})}$ in $R_{\mathbb{Q}(dp^{n+1})}$. For notational simplicity, we put $c_{d,n} := \vartheta_{\mathbb{Q}(dp^n)} \bmod p^m$.*

(1) We have $D_d c_{d,n} \in (R_{\mathbb{Q}(dp^{n+1})}/p^m)^{\mathrm{Gal}(\mathbb{Q}(d)/\mathbb{Q})}$.

(2) Let $\delta_{d,n}$ denote the element of $R_{\mathbb{Q}_n}/p^m$ satisfying $\delta_{d,n} N_d = D_d c_{d,n}$. Then we have

$$c_{d,n} \equiv (-1)^{\nu(d)} \delta_{d,n} \cdot X_{\ell_1} \cdots X_{\ell_t} \pmod{(p^m, X_{\ell_1}^2, \dots, X_{\ell_t}^2)},$$

where we write $d = \ell_1 \cdots \ell_t$ and $X_{\ell_i} := g_{\ell_i} - 1$.

Proof. For any $\ell \in \mathcal{P}_{m,n}$ and $d \in \mathcal{N}_{m,n}$ with $\ell \nmid d$, we have

$$N_\ell(a_\ell - \sigma_\ell - \sigma_\ell^{-1}) \equiv 0 \pmod{p^m},$$
$$\pi_{\ell d,d}(\vartheta_{\mathbb{Q}(\mu_{\ell d p^\infty})}) = (a_\ell - \sigma_\ell - \sigma_\ell^{-1}) \vartheta_{\mathbb{Q}(\mu_{dp^\infty})}.$$

Hence the claim (1) follows from the same argument as in [18, Lemma 4.4.2]). The claim (2) follows from the same argument as in [8, Lemma 4.4]). □

Definition 3.15. *We define the homomorphism*

$$\mathcal{D}_{m,n}^0 \colon \mathrm{ES}_0(T) \longrightarrow \prod_{d \in \mathcal{N}_{m,n}} R_{\mathbb{Q}_n}/p^m \otimes_{\mathbb{Z}} G_d$$

by $\mathcal{D}_{m,n}^0(c) := (\delta(c)_{d,m,n} \otimes g_d)_{d \in \mathcal{N}_{m,n}}$.

Recall that we have the isomorphism $\mathfrak{L}_{\mathbb{Q}_\infty} \colon H^1_{/f}(G_{\mathbb{Q}_p}, \mathbb{T}_{\mathbb{Q}_\infty}) \xrightarrow{\sim} \Lambda_{\mathbb{Q}_\infty}$ by Theorem 3.4(ii). Since

$$H^1_{/f}(G_{\mathbb{Q}_p}, \mathbb{T}_{\mathbb{Q}_\infty}) \otimes_{\Lambda_{\mathbb{Q}_\infty}} R_{\mathbb{Q}_n}/p^m \xrightarrow{\sim} H^1_{/f}(G_{\mathbb{Q}_p}, T_{\mathbb{Q}_n}/p^m),$$

the isomorphism $\mathfrak{L}_{\mathbb{Q}_\infty}$ induces an isomorphism

$$\mathfrak{L}_{\mathbb{Q}_n,m} \colon H^1_{/f}(G_{\mathbb{Q}_p}, T_{\mathbb{Q}_n}/p^m) \xrightarrow{\sim} R_{\mathbb{Q}_n}/p^m,$$

and hence we obtain a homomorphism

$$\mathfrak{L}_{\mathbb{Q}_n,m} \colon \mathrm{KS}_1(T_{\mathbb{Q}_n}/p^m, \mathcal{F}_{\mathrm{can}}) \longrightarrow \prod_{d \in \mathcal{N}_{m,n}} R_{\mathbb{Q}_n}/p^m \otimes_{\mathbb{Z}} G_d.$$

By construction, we have the following proposition.

Proposition 3.16. *The diagram*

$$\begin{tikzcd}
\mathrm{ES}_1(T) \cap \prod_{K\in\Omega} M_{K_\infty} \arrow[r, hook, "\mathfrak{L}"] \arrow[d, "\mathcal{D}^1_{m,n}"] & \mathrm{ES}_0(T) \arrow[d, "\mathcal{D}^0_{m,n}"] \\
\mathrm{KS}_1(T_{\mathbb{Q}_n}/p^m, \mathcal{F}_{\mathrm{can}}) \arrow[r, "\mathfrak{L}_{\mathbb{Q}_n,m}"] & \prod_{d\in\mathcal{N}_{m,n}} R_{\mathbb{Q}_n}/p^m \otimes_{\mathbb{Z}} G_d
\end{tikzcd}$$

commutes.

Theorem 3.17. *There is a Kolyvagin system $\kappa_{\xi,m,n} \in \mathrm{KS}_0(T_{\mathbb{Q}_n}/p^m, \mathcal{F}_{\mathrm{cl}})$ satisfying $\delta(\kappa_{\xi,m,n}) = \mathcal{D}^0_{m,n}((\widetilde{\xi}_{K_\infty})_{K\in\Omega})$.*

Proof. Let $z_\xi \in \mathrm{ES}_1(T)$ be the Euler system defined in Proposition 3.8. Note that $\mathfrak{L}(z_\xi) = (\widetilde{\xi}_{K_\infty})_{K\in\Omega}$. We define

$$\kappa_{\xi,m,n} := \Phi \circ \mathcal{D}^1_{m,n}(z_\xi).$$

Here $\Phi\colon \mathrm{KS}_1(T, \mathcal{F}_{\mathrm{can}}) \longrightarrow \mathrm{KS}_0(T, \mathcal{F}_{\mathrm{cl}})$ is the homomorphism associated with the isomorphism $\mathfrak{L}_{\mathbb{Q}_n,m}\colon H^1_{/f}(G_{\mathbb{Q}_p}, T_{\mathbb{Q}_n}/p^m) \xrightarrow{\sim} R_{\mathbb{Q}_n}/p^m$ (see §2.5). The commutative diagram (2) shows that $\delta\circ\Phi = \mathfrak{L}_{\mathbb{Q}_n,m}$. Hence Proposition 3.16 implies

$$\begin{aligned}
\delta(\kappa_{\xi,m,n}) &= \delta \circ \Phi \circ \mathcal{D}^1_{m,n}(z_\xi) \\
&= \mathfrak{L}_{\mathbb{Q}_n,m} \circ \mathcal{D}^1_{m,n}(z_\xi) \\
&= \mathcal{D}^0_{m,n} \circ \mathfrak{L}(z_\xi) \\
&= \mathcal{D}^0_{m,n}((\widetilde{\xi}_{K_\infty})_{K\in\Omega}).
\end{aligned}$$

□

Remark 3.18. The Kolyvagin system $\kappa_{\xi,m,n}$ constructed in Theorem 3.17 is a natural extension of a family of cohomology classes constructed by Kurihara in [10] (see also [9]). More precisely, for any "admissible" pair $(d,\ell) \in \mathcal{M}_{m,n}$, Kurihara constructed a cohomology class $\kappa_{d,\ell}$ such that it satisfies the relations appeared in the definition of Kolyvagin system of rank 0 and that it relates to modular symbols via the map δ. In our construction, we do not need to impose that the pair $(d,\ell) \in \mathcal{N}_{m,n} \times \mathcal{P}_{m,n}$ is admissible.

3.5 Properties of $\kappa_{\xi,m,n}$

Recall that the Iwasawa main conjecture for $E/\mathbb{Q}$ says that

$$\widetilde{\xi}_{\mathbb{Q}_\infty}\Lambda_{\mathbb{Q}_\infty} = \mathrm{char}_{\Lambda_{\mathbb{Q}_\infty}}(\mathrm{Sel}(\mathbb{Q}_\infty, E[p^\infty])^\vee).$$

Proposition 3.19. *The following are equivalent.*

(1) *The Kolyvagin system $\kappa_{\xi,m,n} \in \mathrm{KS}_0(T_{\mathbb{Q}_n}/p^m, \mathcal{F}_{\mathrm{cl}})$ is a basis for some $m \geq 1$ and $n \geq 0$.*

(2) *The Kolyvagin system* $\kappa_{\xi,m,n} \in \mathrm{KS}_0(T_{\mathbb{Q}_n}/p^m, \mathcal{F}_{\mathrm{cl}})$ *is a basis for any* $m \geq 1$ *and* $n \geq 0$.

(3) *There is an integer* $d \in \mathcal{N}_{1,0}$ *satisfying* $\delta(\kappa_{\xi,1,0})_d \neq 0$.

(4) *The Iwasawa main conjecture for* $E/\mathbb{Q}$ *holds true.*

Proof. We put

$$\mathrm{KS}_0(\mathbb{T}_{\mathbb{Q}_\infty}, \mathcal{F}_{\mathrm{cl}}) := \varprojlim_{m,n} \mathrm{KS}_0(T_{\mathbb{Q}_n}/p^m, \mathcal{F}_{\mathrm{cl}}).$$

Then Theorem 2.20 and [19, Lemma 3.25] (see [21, Theorem 6.3]) show that the canonical map $\mathrm{KS}_0(\mathbb{T}_{\mathbb{Q}_\infty}, \mathcal{F}_{\mathrm{cl}}) \longrightarrow \mathrm{KS}_0(T_{\mathbb{Q}_n}/p^m, \mathcal{F}_{\mathrm{cl}})$ is surjective and the $\Lambda_{\mathbb{Q}_\infty}$-module $\mathrm{KS}_0(\mathbb{T}_{\mathbb{Q}_\infty}, \mathcal{F}_{\mathrm{cl}})$ is free of rank 1. By construction,

$$\kappa_\xi := (\kappa_{\xi,m,n})_{m\geq 1, n\geq 0} \in \mathrm{KS}_0(\mathbb{T}_{\mathbb{Q}_\infty}, \mathcal{F}_{\mathrm{cl}}).$$

Since $\delta\colon \mathrm{KS}_0(E[p], \mathcal{F}_{\mathrm{cl}}) \longrightarrow \prod_{d\in\mathcal{N}_{1,0}} \mathbb{F}_p \otimes_{\mathbb{Z}} G_d$ is injective by Corollary 2.22, claims (1), (2) and (3) are equivalent, and it suffices to show that claim (4) is equivalent to that κ_ξ is a basis. We have the canonical homomorphism

$$\delta_1\colon \mathrm{KS}_0(\mathbb{T}_{\mathbb{Q}_\infty}, \mathcal{F}_{\mathrm{cl}}) \longrightarrow \Lambda_{\mathbb{Q}_\infty};\ (\kappa_{m,n})_{m\geq 1,n\geq 0} \mapsto \varprojlim_{m,n} \delta(\kappa_{m,n})_1.$$

By Theorem 3.17, we have

$$\delta_1(\kappa_\xi) = \varprojlim_{m,n} \delta(\kappa_{\xi,m,n})_1 = \varprojlim_{m,n} \mathcal{D}^0_{m,n}((\widetilde{\xi}_{K_\infty})_{K\in\Omega})_1 = \widetilde{\xi}_{\mathbb{Q}_\infty}.$$

Let $\kappa \in \mathrm{KS}_0(\mathbb{T}_{\mathbb{Q}_\infty}, \mathcal{F}_{\mathrm{cl}})$ be a basis and write $\kappa_\xi = a\kappa$ for some $a \in \Lambda_{\mathbb{Q}_\infty}$. Then, by Theorem 2.20 (see [21, Theorem 6.4]), we have

$$\widetilde{\xi}_{\mathbb{Q}_\infty}\Lambda_{\mathbb{Q}_\infty} = a\delta_1(\kappa)\Lambda_{\mathbb{Q}_\infty} = a \cdot \mathrm{char}_{\Lambda_{\mathbb{Q}_\infty}}(\mathrm{Sel}(\mathbb{Q}_\infty.E[p^\infty])^\vee).$$

Since the characteristic ideal $\mathrm{char}_{\Lambda_{\mathbb{Q}_\infty}}(\mathrm{Sel}(\mathbb{Q}_\infty.E[p^\infty])^\vee)$ is non-zero, claim (4) is equivalent to that a is unit, i.e., κ_ξ is a basis. □

4 Main results

4.1 Proof of Theorem 1.2

First, let us discuss the relation between $\delta(\kappa_{\xi,1,0})_d$ and $\widetilde{\delta}_d$. As in §1, for each prime $\ell \in \mathcal{P}_{1,0}$, we fix a generator $h_\ell \in \mathrm{Gal}(\mathbb{Q}(\mu_\ell)/\mathbb{Q})$, and it naturally induces the surjection

$$\overline{\log}_{h_\ell}\colon \mathrm{Gal}(\mathbb{Q}(\mu_\ell)/\mathbb{Q}) \xrightarrow{\sim} \mathbb{Z}/(\ell-1) \longrightarrow \mathbb{F}_p;\ h_\ell^a \mapsto a \bmod p.$$

Recall that, for any integer $d \in \mathcal{N}_{1,0}$, the analytic quantity $\widetilde{\delta}_d \in \mathbb{F}_p$ is defined by

$$\widetilde{\delta}_d := \sum_{\substack{a=1 \\ (a,d)=1}}^{d} \frac{\mathrm{Re}([a/d])}{\Omega_E^+} \cdot \prod_{\ell \mid d} \overline{\log}_{h_\ell}(\sigma_a).$$

We put $e_d := \# \mathrm{Gal}(\mathbb{Q}(\mu_d)/\mathbb{Q}(d))$. Since $p \nmid e_d$, we see that $\widetilde{\delta}_d = 0$ if and only if

$$e_d^{\nu(d)} \widetilde{\delta}_d = \sum_{\substack{a=1 \\ (a,d)=1}}^{d} \frac{\mathrm{Re}([a/d])}{\Omega_E^+} \cdot \prod_{\ell \mid d} \overline{\log}_{h_\ell}(\sigma_a^{e_d}) = 0.$$

Let $\widetilde{\theta}_d = \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(d)/\mathbb{Q})} a_\sigma \sigma$ denote the image of $\widetilde{\theta}_{\mathbb{Q}(\mu_d)}$ in $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(d)/\mathbb{Q})]$ (see §3.1 for the definition of $\widetilde{\theta}_{\mathbb{Q}(\mu_d)}$). Assume for simplicity that the image of $h_\ell^{e_d}$ is the fixed generator $g_\ell \in \mathrm{Gal}(\mathbb{Q}(\ell)/\mathbb{Q})$. Recall that we have the surjection

$$\overline{\log}_{g_\ell} \colon \mathrm{Gal}(\mathbb{Q}(d)/\mathbb{Q}) \xrightarrow{\sim} \mathbb{Z}/(\ell-1) \longrightarrow \mathbb{F}_p.$$

Since $\sigma_a = \sigma_b$ in $\mathrm{Gal}(\mathbb{Q}(d)/\mathbb{Q})$ if $\sigma_a^{e_d} = \sigma_b^{e_d}$, we see that

$$e_d^{\nu(d)} \widetilde{\delta}_d = \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(d)/\mathbb{Q})} a_\sigma \cdot \prod_{\ell \mid d} \overline{\log}_{g_\ell}(\sigma).$$

Since we have

$$D_d \widetilde{\theta}_d \bmod p = (-1)^{\nu(d)} \left(\sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(d)/\mathbb{Q})} a_\sigma \cdot \prod_{\ell \mid d} \overline{\log}_{g_\ell}(\sigma) \right) N_d$$

by Lemmas 3.13 and 3.14, we obtain the following lemma (see also Remark 3.1).

LEMMA 4.1. *For any integer $d \in \mathcal{N}_{1,0}$, the following are equivalent.*

(1) $\widetilde{\delta}_d \neq 0$.

(2) $D_d \widetilde{\theta}_d \bmod p \neq 0$.

LEMMA 4.2. *For any integer $d \in \mathcal{N}_{1,0}$, the following are equivalent.*

(1) $\widetilde{\delta}_d \neq 0$.

(2) $\delta(\kappa_{\xi,1,0})_d \neq 0$.

Proof. Since any prime $\ell \in \mathcal{P}_{1,0}$ is congruent to 1 modulo p, the relation $\delta(\kappa_{\xi,1,0}) = \mathcal{D}^0_{1,0}((\widetilde{\xi}_{K_\infty})_{K \in \Omega})$ in Theorem 3.17 shows that $\delta(\kappa_{\xi,1,0})_d \neq 0$ if and only if $D_d \vartheta_d \bmod p \neq 0$. Hence this lemma follows from Lemma 4.1 and Remark 3.1. □

COROLLARY 4.3 (Theorem 1.2). *Conjecture 1.1 holds true, that is, there is an integer $d \in \mathcal{N}_{1,0}$ satisfying $\widetilde{\delta}_d \neq 0$ if and only if the Iwasawa main conjecture for $E/\mathbb{Q}$ holds true.*

Proof. This corollary follows from Proposition 3.19 and Lemma 4.2. □

4.2 Proof of Theorem 1.5

In this subsection, we give a proof of Theorem 1.5. Recall that an integer $d \in \mathcal{N}_{1,0}$ is δ-minimal if $\widetilde{\delta}_d \neq 0$ and $\widetilde{\delta}_e = 0$ for any positive proper divisor e of d. Note that the existence of a δ-minimal integer implies that the Kolyvagin system $\kappa_{\xi,1,0}$ is a basis of $\mathrm{KS}_0(E[p], \mathcal{F}_{\mathrm{cl}})$ by Proposition 3.19 and Corollary 4.3.

Lemma 4.4. *Let $d \in \mathcal{N}_{1,0}$ be an integer. Then the following are equivalent.*

(1) $\widetilde{\delta}_d \neq 0$.

(2) $H^1_{\mathcal{F}_{\mathrm{cl}}(d)}(G_{\mathbb{Q}}, E[p]) = 0$.

Proof. By Theorem 2.20, we have

$$\mathbb{F}_p \cdot \delta(\kappa_{\xi,1,0})_d = \mathrm{Fitt}^0_{\mathbb{F}_p}(H^1_{\mathcal{F}_{\mathrm{cl}}(d)}(G_{\mathbb{Q}}, E[p])^\vee).$$

Hence this lemma follows from Lemma 4.2. □

Remark 4.5. The injectivity of the homomorphism (1) (proved by Kurihara) follows immediately from Lemma 4.4. In fact, we have

$$\begin{aligned}\ker\left(\mathrm{Sel}(\mathbb{Q}, E[p]) \xrightarrow{(1)} \bigoplus_{\ell \mid d} E(\mathbb{Q}_\ell) \otimes \mathbb{F}_p\right) &= H^1_{(\mathcal{F}_{\mathrm{cl}})_d}(G_{\mathbb{Q}}, E[p]) \\ &\subset H^1_{\mathcal{F}_{\mathrm{cl}}(d)}(G_{\mathbb{Q}}, E[p]).\end{aligned}$$

For any integer $d \in \mathcal{N}_{1,0}$, we set

$$\lambda(d) := \dim_{\mathbb{F}_p}(H^1_{\mathcal{F}_{\mathrm{cl}}(d)}(G_{\mathbb{Q}}, E[p])).$$

Lemma 4.6. *Let $d \in \mathcal{N}_{1,0}$ be an integer and $\ell \in \mathcal{P}_{1,0}$ a prime with $\ell \nmid d$.*

(1) If $H^1_{\mathcal{F}_{\mathrm{cl}}(d)}(G_{\mathbb{Q}}, E[p]) \neq H^1_{(\mathcal{F}_{\mathrm{cl}})_\ell(d)}(G_{\mathbb{Q}}, E[p])$, then $\lambda(d\ell) = \lambda(d) - 1$.

(2) If $H^1_{\mathcal{F}_{\mathrm{cl}}(d)}(G_{\mathbb{Q}}, E[p]) = H^1_{(\mathcal{F}_{\mathrm{cl}})_\ell(d)}(G_{\mathbb{Q}}, E[p])$, then $\lambda(d) \leq \lambda(d\ell)$.

In particular, $\lambda(d) \geq \lambda(1) - \nu(d)$.

Proof. If $H^1_{\mathcal{F}_{\mathrm{cl}}(d)}(G_{\mathbb{Q}}, E[p]) \neq H^1_{(\mathcal{F}_{\mathrm{cl}})_\ell(d)}(G_{\mathbb{Q}}, E[p])$, then the localization map

$$H^1_{\mathcal{F}_{\mathrm{cl}}(d)}(G_{\mathbb{Q}}, E[p]) \longrightarrow H^1_{\mathrm{ur}}(G_{\mathbb{Q}_\ell}, E[p])$$

is non-zero. Since $\mathcal{F}_{\mathrm{cl}}(d)^* = \mathcal{F}_{\mathrm{cl}}(d)$, claim (1) follows from [11, Lemma 4.1.7 (iv)]. Claim (2) is trivial since

$$H^1_{\mathcal{F}_{\mathrm{cl}}(d)}(G_{\mathbb{Q}}, E[p]) = H^1_{(\mathcal{F}_{\mathrm{cl}})_\ell(d)}(G_{\mathbb{Q}}, E[p]) \subset H^1_{\mathcal{F}_{\mathrm{cl}}(d\ell)}(G_{\mathbb{Q}}, E[p]).$$

□

Proposition 4.7. *Let $d \in \mathcal{N}_{1,0}$ be an integer satisfying $H^1_{\mathcal{F}_{\mathrm{cl}}(d)}(G_{\mathbb{Q}}, E[p]) = 0$. Then there is a positive divisor e of d such that $\nu(e) = \lambda(1)$ and $\lambda(e) = 0$.*

Proof. When $\lambda(1) = 0$, one can take $e = 1$. Hence we may assume that $\lambda(1) > 0$. If $H^1_{\mathcal{F}_{\mathrm{cl}}}(G_{\mathbb{Q}}, E[p]) = H^1_{(\mathcal{F}_{\mathrm{cl}})_\ell}(G_{\mathbb{Q}}, E[p])$ for any prime $\ell \mid d$, then

$$\begin{aligned} H^1_{\mathcal{F}_{\mathrm{cl}}}(G_{\mathbb{Q}}, E[p]) &= \bigcap_{\ell \mid d} H^1_{(\mathcal{F}_{\mathrm{cl}})_\ell}(G_{\mathbb{Q}}, E[p]) \\ &= H^1_{(\mathcal{F}_{\mathrm{cl}})_d}(G_{\mathbb{Q}}, E[p]) \\ &\subset H^1_{\mathcal{F}_{\mathrm{cl}}(d)}(G_{\mathbb{Q}}, E[p]) \\ &= 0. \end{aligned}$$

However, since we assume $\lambda(1) > 0$, we conclude that there is a prime $\ell_1 \mid d$ such that

$$H^1_{\mathcal{F}_{\mathrm{cl}}}(G_{\mathbb{Q}}, E[p]) \neq H^1_{(\mathcal{F}_{\mathrm{cl}})_{\ell_1}}(G_{\mathbb{Q}}, E[p]).$$

Hence Lemma 4.6 implies $\lambda(\ell_1) = \lambda(1) - 1$. If $\lambda(1) = 1$, then ℓ_1 is a desired divisor of d. Suppose that $\lambda(1) > 1$. Since

$$H^1_{(\mathcal{F}_{\mathrm{cl}})_{d/\ell_1}(\ell_1)}(G_{\mathbb{Q}}, E[p]) \subset H^1_{\mathcal{F}_{\mathrm{cl}}(d)}(G_{\mathbb{Q}}, E[p]) = 0,$$

the same argument shows that there is a prime $\ell_2 \mid d/\ell_1$ satisfying

$$H^1_{\mathcal{F}_{\mathrm{cl}}(\ell_1)}(G_{\mathbb{Q}}, E[p]) \neq H^1_{(\mathcal{F}_{\mathrm{cl}})_{\ell_2}(\ell_1)}(G_{\mathbb{Q}}, E[p]).$$

Then $\lambda(\ell_1\ell_2) = \lambda(\ell_1) - 1$ by Lemma 4.6. By repeating this argument, we obtain a sequence $\ell_1, \ldots, \ell_{\lambda(1)}$ of prime divisors of d such that $\lambda(\ell_1) = \lambda(1) - 1$ and $\lambda(\ell_1 \cdots \ell_{i+1}) = \lambda(\ell_1 \cdots \ell_i) - 1$ for any $1 \leq i < \lambda(1)$. Then $e := \ell_1 \cdots \ell_{\lambda(1)}$ is a desired divisor of d. □

Theorem 4.8 (Theorem 1.5). *For any δ-minimal integer $d \in \mathcal{N}_{1,0}$, we have*

$$\dim_{\mathbb{F}_p}(\mathrm{Sel}(\mathbb{Q}, E[p])) = \nu(d).$$

Proof. Let $d \in \mathcal{N}_{1,0}$ be a δ-minimal integer. Then $H^1_{\mathcal{F}_{\mathrm{cl}}(d)}(G_{\mathbb{Q}}, E[p]) = 0$ by Lemma 4.4. Hence Proposition 4.7 shows that there is a positive divisor e of d such that $\nu(e) = \lambda(1)$ and $\lambda(e) = 0$. Then Lemma 4.4 implies $\widetilde{\delta}_e \neq 0$, and we have $d = e$ by the definition of the δ-minimality. Therefore, we obtain $\nu(d) = \nu(e) = \lambda(1)$. □

Remark 4.9. In the multiplicative group case, under the validity of the analogue of Lemma 4.6, one can show that the analogue of Theorem 1.5 ([10, Conjecture 2]) holds true. However, as mentioned in Remark 1.8, there is a counter-example of the analogue of Theorem 1.5. This shows that the analogue of Lemma 4.6 does not hold in general. In the proof of Lemma 4.6, we use crucially the fact that the Selmer structure $\mathcal{F}_{\mathrm{cl}}$ is self-dual, and hence one can say that the self-duality of the Selmer structure $\mathcal{F}_{\mathrm{cl}}$ is one of the most important ingredients in order to prove Theorem 1.5.

Let $\kappa_{\xi,1,0} = (\kappa_{d,\ell})_{(d,\ell)\in\mathcal{M}_{1,0}} \in \mathrm{KS}_0(E[p],\mathcal{F}_{\mathrm{cl}})$ be the Kolyvagin system constructed in Theorem 3.17. By using the fixed generator $g_\ell \in G_\ell$, we regard G_ℓ as $\mathbb{Z}/\#G_\ell$, and hence one can regard $\kappa_{d,\ell} \in H^1_{\mathcal{F}^\ell_{\mathrm{cl}}(d)}(G_\mathbb{Q}, E[p])$. As discussed by Kurihara in [10, Theorem 3(2)], by using Theorem 4.8, one can construct a basis of the p-Selmer group $\mathrm{Sel}(\mathbb{Q}, E[p])$ from the Kolyvagin system $\kappa_{\xi,1,0}$.

Corollary 4.10. *For any δ-minimal integer $d = \ell_1 \cdots \ell_t \in \mathcal{N}_{1,0}$, the set $\{\kappa_{d/\ell_i,\ell_i} \mid 1 \leq i \leq t\}$ is a basis of* $\mathrm{Sel}(\mathbb{Q}, E[p])$.

Proof. Applying Theorem 2.1 with $\mathcal{F}_1 = (\mathcal{F}_{\mathrm{cl}})_d$ and $\mathcal{F}_2 = \mathcal{F}_{\mathrm{cl}}$, we obtain an exact sequence

$$\begin{aligned} 0 \longrightarrow H^1_{(\mathcal{F}_{\mathrm{cl}})_d}(G_\mathbb{Q}, E[p]) \longrightarrow \mathrm{Sel}(\mathbb{Q}, E[p]) \longrightarrow \bigoplus_{\ell \mid d} H^1_{\mathrm{ur}}(G_\mathbb{Q}, E[p]) \\ \longrightarrow H^1_{\mathcal{F}^d_{\mathrm{cl}}}(G_\mathbb{Q}, E[p])^\vee \longrightarrow \mathrm{Sel}(\mathbb{Q}, E[p])^\vee \longrightarrow 0. \end{aligned}$$

Lemma 4.4 and Theorem 4.8 show that $H^1_{\mathcal{F}^d_{\mathrm{cl}}}(G_\mathbb{Q}, E[p]) = \mathrm{Sel}(\mathbb{Q}, E[p])$, and we have an isomorphism

$$\bigoplus_{\ell \mid d} \varphi^{\mathrm{fs}}_\ell \colon \mathrm{Sel}(\mathbb{Q}, E[p]) \xrightarrow{\sim} \bigoplus_{\ell \mid d} H^1_{\mathrm{ur}}(G_\mathbb{Q}, E[p]) \xrightarrow{\sim} \mathbb{F}_p^t.$$

Here $t := \nu(d)$. In particular, $\kappa_{d/\ell_i,\ell_i} \in \mathrm{Sel}(\mathbb{Q}, E[p])$ for any integer $1 \leq i \leq t$. Take an integer $1 \leq i \leq t$. Since $H^1_{\mathcal{F}^{\ell_i}_{\mathrm{cl}}(d/\ell_i)}(G_\mathbb{Q}, E[p]) \subset \mathrm{Sel}(\mathbb{Q}, E[p])$, we have

$$\begin{aligned} H^1_{\mathcal{F}^{\ell_i}_{\mathrm{cl}}(d/\ell_i)}(G_\mathbb{Q}, E[p]) &= H^1_{\mathcal{F}^{\ell_i}_{\mathrm{cl}}(d/\ell_i)}(G_\mathbb{Q}, E[p]) \cap H^1_{\mathcal{F}_{\mathrm{cl}}}(G_\mathbb{Q}, E[p]) \\ &= H^1_{(\mathcal{F}_{\mathrm{cl}})_{d/\ell_i}}(G_\mathbb{Q}, E[p]). \end{aligned}$$

Since $\kappa_{d/\ell_i,\ell_i} \in H^1_{(\mathcal{F}_{\mathrm{cl}})_{d/\ell_i}}(G_\mathbb{Q}, E[p])$, we have $\varphi^{\mathrm{fs}}_{\ell_j}(\kappa_{d/\ell_i,\ell_i}) = 0$ for any $j \neq i$. The δ-minimality of d and Lemma 4.2 imply that $\varphi^{\mathrm{fs}}_{\ell_i}(\kappa_{d/\ell_i,\ell_i}) = -\delta(\kappa_{\xi,1,0})_d \neq 0$. This shows that the set $\{\kappa_{d/\ell_i,\ell_i} \mid 1 \leq i \leq t\}$ is a basis of $\mathrm{Sel}(\mathbb{Q}, E[p])$. □

References

[1] Burns, David; Sakamoto, Ryotaro; Sano, Takamichi. On the theory of higher rank Euler, Kolyvagin and Stark systems, II. Preprint, 2018. https://arxiv.org/abs/1805.08448.

[2] Burns, David; Sano, Takamichi. On the theory of higher rank Euler, Kolyvagin and Stark systems. Int. Math. Res. Not. IMRN 2021, no. 13, 10118–10206.

[3] Kataoka, Takenori. Equivariant Iwasawa theory for elliptic curves. Math. Z. 298 (2021), no. 3-4, 1653–1725.

[4] Kato, Kazuya. p-adic Hodge theory and values of zeta functions of modular forms. Cohomologies p-adiques et applications arithmétiques. III. Astérisque 295 (2004), 117–290.

[5] Kim, Chan-Ho; Kim, Myoungil; Sun, Hae-Sang. On the indivisibility of derived Kato's Euler systems and the main conjecture for modular forms. Selecta Math. (N.S.) 26 (2020), no. 2, Paper No. 31, 47 pp.

[6] Kim, Chan-Ho; Nakamura, Kentaro. Remarks on Kato's Euler systems for elliptic curves with additive reduction. J. Number Theory 210 (2020), 249–279.

[7] Kim, Chan-Ho. The structure of Selmer groups and the Iwasawa main conjecture for elliptic curves. Preprint, 2022. https://arxiv.org/abs/2203.12159.

[8] Kurihara, Masato. On the structure of ideal class groups of CM-fields. Kazuya Kato's fiftieth birthday. Doc. Math. 2003, Extra Vol., 539–563.

[9] Kurihara, Masato. Refined Iwasawa theory for p-adic representations and the structure of Selmer groups, Münster J. Math. 7 (2014), no. 1, 149–223.

[10] Kurihara, Masato. The structure of Selmer groups of elliptic curves and modular symbols, Iwasawa theory 2012, 317–356. Contrib. Math. Comput. Sci., 7. Springer, Heidelberg, 2014.

[11] Mazur, Barry; Rubin, Karl. Kolyvagin systems, Mem. Amer. Math. Soc. 799 (2004).

[12] Mazur, Barry; Rubin, Karl. Controlling Selmer groups in the higher core rank case, J. Théor. Nombres Bordeaux 28 (2016), 145–183.

[13] Mazur, Barry; Tate, John. Refined conjectures of the "Birch and Swinnerton-Dyer type". Duke Math. J. 54 (1987), no. 2, 711–750.

[14] Nekovář, Jan. On the parity of ranks of Selmer groups. II. C. R. Acad. Sci. Paris Sér. I Math. 332 (2001), no. 2, 99–104.

[15] Nekovář, Jan. Selmer complexes. Astérisque 310 (2006), viii+559 pp.

[16] Ota, Kazuto. Kato's Euler system and the Mazur-Tate refined conjecture of BSD type. Amer. J. Math. 140 (2018), no. 2, 495–542.

[17] Perrin-Riou, Bernadette. Théorie d'Iwasawa des représentations p-adiques sur un corps local. With an appendix by Jean-Marc Fontaine. Invent. Math. 115 (1994), no. 1, 81–161.

[18] Rubin, Karl. Euler systems. Annals of Math. Studies, 147. Princeton Univ. Press, 2000.

[19] Sakamoto, Ryotaro. Stark systems over Gorenstein local rings, Algebra Number Theory 12 (2018), no. 10, 2295–2326.

[20] Sakamoto, Ryotaro. On the theory of higher rank Euler, Kolyvagin and Stark systems: a research announcement, Algebraic Number Theory and Related Topics 2017, RIMS Kôkyûroku Bessatsu B83 (2020), 141–159.

[21] Sakamoto, Ryotaro. On the theory of Kolyvagin systems of rank 0, J. Théor. Nombres Bordeaux 33 (2021), no. 3, pt. 2, 1077–1102.

[22] Skinner, Christopher; Urban, Eric. The Iwasawa main conjectures for GL_2. Invent. Math. 195 (2014), no. 1, 1–277.

[23] Stevens, Glenn. Stickelberger elements and modular parametrizations of elliptic curves. Invent. Math. 98 (1989), no. 1, 75–106.

[24] Tan, Ki-Seng. A generalized Mazur's theorem and its applications. Trans. Amer. Math. Soc. 362 (2010), no. 8, 4433–4450.

Ryotaro Sakamoto
Department of Mathematics
University of Tsukuba
1-1-1 Tennodai
Tsukuba, Ibaraki 305-8571
Japan
rsakamoto@math.tsukuba.ac.jp