Abstract. In this paper, we prove that the dimension of the \( p \)-Selmer group for an elliptic curve is controlled by certain analytic quantities associated with modular symbols, which is conjectured by Kurihara.

Contents

1. Introduction 1
Acknowledgement 4
2. The theory of Kolyvagin system 4
2.1. Selmer structures 4
2.2. Structure of local points 6
2.3. Kolyvagin systems of rank 1 8
2.4. Kolyvagin systems of rank 0 9
2.5. Map from Kolyvagin systems of rank 1 to Kolyvagin systems of rank 0 10
3. Construction of the Kolyvagin system of rank 0 from modular symbols 12
3.1. Modular symbols 12
3.2. Coleman maps 13
3.3. Euler systems 14
3.4. Construction of \( \kappa_{\xi,m,n} \) 15
3.5. Properties of \( \kappa_{\xi,m,n} \) 18
4. Main results 18
4.1. Proof of Theorem 1.2 18
4.2. Proof of Theorem 1.5 19
Appendix A. Remarks on \( p = 3 \) 21
A.1. Application of the Chebotarev density theorem 22
A.2. Connectedness of the graph \( A^0 \) 23
A.3. Kolyvagin systems 26
References 28

1. Introduction

In modern number theory, it is an attractive area of research to connect \( L \)-values with Selmer groups. In the present paper, we prove that the dimension of the (classical) \( p \)-Selmer group \( \text{Sel}(\mathbb{Q}, E[p]) \) for an elliptic curve \( E/\mathbb{Q} \) is controlled by certain analytic quantities associated with modular symbols, which is conjectured by Kurihara in [6].

In order to explain this result in detail, we introduce some notations and hypotheses. Let \( E/\mathbb{Q} \) be an elliptic curve and let \( S_{\text{bad}}(E) \) denote the set of primes at which \( E \) has bad reduction. For any integer \( n \geq 0 \), let \( \mathbb{Q}_n \) denote the \( n \)-th layer of the cyclotomic \( \mathbb{Z}_p \)-extension of \( \mathbb{Q} \). As in the paper [6] of Kurihara, we consider a prime \( p \geq 3 \) satisfying the following conditions:

The author was supported by JSPS KAKENHI Grant Number 20J00456.
element satisfying \( \sigma \) (induced by the discrete logarithm to the base \( \ell \in \mathbb{N} \)).

Let \( f \) be a newform of weight 2 associated with \( E/\mathbb{Q} \), and we obtain a surjective homomorphism (induced by the discrete logarithm to the base \( h_\ell \))

\[
\log_{h_\ell} : \text{Gal}(\mathbb{Q}(\mu_\ell)/\mathbb{Q}) \rightarrow \mathbb{Z}/(\ell - 1) \rightarrow \mathbb{F}_p;\ h_\ell^a \mapsto a \mod p.
\]

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 \( \sigma_a \in \text{Gal}(\mathbb{Q}(\mu_d)/\mathbb{Q}) \) for the element satisfying \( \sigma_a(\zeta) = \zeta^a \) for any \( \zeta \in \mu_d \) and put

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

Following Kurihara in [6], we define an analytic quantity \( \tilde{\delta}_d \) which relates to \( L \)-values by

\[
\tilde{\delta}_d := \sum_{\substack{a=1 \atop (a,d)=1}}^d \frac{\text{Re}([a/d])}{\Omega_E^{+}}, \prod_{\ell \in \mathcal{P}} \log_{h_\ell}(\sigma_a) \in \mathbb{F}_p,
\]

where \( \Omega_E^{+} \) is the Néron period of \( E \). Kurihara remarked in [6] that it is easy to compute the analytic quantity \( \tilde{\delta}_d \) (see [6, §5.3]), and gave the following conjecture.

**Conjecture 1.1** ([6, Conjecture 1]). There is an integer \( d \in \mathcal{N}_{1,0} \) with \( \tilde{\delta}_d \neq 0 \).

Concerning this conjecture, Kurihara proved in [6] 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 [13], Chan-Ho Kim, Myoungil Kim, and Hae-Sang Sun called \( \delta_d \) Kurihara number at \( d \) and gave a simple and efficient numerical criterion to verify the Iwasawa main conjecture for \( E/\mathbb{Q} \) by using \( \delta_d \), namely, they proved in [13] that Conjecture 1.1 implies the Iwasawa main conjecture for \( E/\mathbb{Q} \). Moreover, Chan-Ho Kim and Nakamura in [14] 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 [20] that if there exists a prime \( q \neq p \) such that \( \text{ord}_q(N_E) = 1 \) 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 \( \text{Sel}(\mathbb{Q}, E[p]) \) and the analytic quantities \( \delta_d \). For that, we use the following terminology of Kurihara in [6].

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

Recall that, by the definition of the \( p \)-Selmer group, the localization map at \( \ell \) induces a natural homomorphism

\[
\text{Sel}(\mathbb{Q}, E[p]) \longrightarrow E(\mathbb{Q}_\ell) \otimes \mathbb{F}_p.
\]
Let \( d \in \mathcal{N}_{1,0} \) be a \( \delta \)-minimal integer. Kurihara proved in [6] that the natural homomorphism
\[
\text{Sel}(\mathbb{Q}, E[p]) \hookrightarrow \bigoplus_{\ell \mid d} E(\mathbb{Q}_\ell) \otimes_{\mathbb{Z}} \mathbb{F}_p
\]
is injective (see Remark 4.5), and he conjectured in [6, Conjecture 2] that this 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
\[
\dim_{\mathbb{F}_p}(\text{Sel}(\mathbb{Q}, E[p])) = \nu(d),
\]
where \( \nu(d) \) denotes the number of distinct prime divisors of \( d \). Kurihara showed in [6, 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 \( \delta \)-minimal integer \( d \in \mathcal{N}_{1,0} \), we have the natural isomorphism
\[
\text{Sel}(\mathbb{Q}, E[p]) \xrightarrow{\sim} \bigoplus_{\ell \mid d} E(\mathbb{Q}_\ell) \otimes_{\mathbb{Z}} \mathbb{F}_p
\]
and hence \( \dim_{\mathbb{F}_p}(\text{Sel}(\mathbb{Q}, E[p])) = \nu(d) \).

**Remark 1.6.** Theorem 1.5 implies that for any integer \( d \in \mathcal{N}_{1,0} \) with \( \tilde{\Delta}_d \neq 0 \), we have
\[
\dim_{\mathbb{F}_p}(\text{Sel}(\mathbb{Q}, E[p])) \leq \nu(d).
\]
Note that the analytic quantity \( \tilde{\Delta}_d \) 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 [15]).

**Remark 1.8.** The analogue of Theorem 1.5 for ideal class groups does not hold as Kurihara gave in [6, §5.4] a counter-example. In Remark 4.9, we explain what is an important property in order to prove Theorem 1.5.

By using the functional equation for modular symbols (see [9, (1.6.1)]), Kurihara showed in [6, Lemma 4] that \( w_E = (-1)^{\nu(d)} \) for any \( \delta \)-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 \( L(E/\mathbb{Q}, s) \) at \( s = 1 \):

**Corollary 1.9.** Suppose that the Iwasawa main conjecture for \( E/\mathbb{Q} \) holds true. Then we have
\[
\dim_{\mathbb{F}_p}(\text{Sel}(\mathbb{Q}, E[p])) \equiv \text{ord}_{s=1}(L(E/\mathbb{Q}, s)) \pmod{2}.
\]
Moreover, if the \( p \)-primary part of the Tate–Shafarevich group for \( E/\mathbb{Q} \) is finite, then we have
\[
\text{rank}_{\mathbb{Z}}(E(\mathbb{Q})) \equiv \text{ord}_{s=1}(L(E/\mathbb{Q}, s)) \pmod{2}.
\]

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

**Remark 1.10.** Corollary 1.9 has already been proved by Nekovář in [10] (see also [11]), assuming only the condition (a). However, the proof of Corollary 1.9 is completely different from that of [10, Theorem A].
The proof of Theorem 1.5 is based on the theory of Kolyvagin systems of rank 0 developed in [19]. 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 \( \{ \tilde{\delta}_d \} \), 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).

In our case, the theory of Kolyvagin systems developed in [19] does not work when \( p = 3 \). In Appendix A, we discuss this problem and extend the theory of Kolyvagin systems so that it can be used even when \( p = 3 \).

Acknowledgement. The authors 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.

2. The theory of Kolyvagin system

In this section, we recall the theory of Kolyvagin systems. The contents of this section are based on [7, 19].

Let \( p \geq 3 \) be a primes 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

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

Note that \( T \) satisfies the hypotheses (H.0) – (H.3) in [7, §3.5]. However, \( T \) does not satisfy the hypothesis (H.4) in [7, §3.5] when \( p = 3 \).

2.1. Selmer structures. We introduce two Selmer structures on \( T \). Recall that a Selmer structure \( F \) on \( T \) is a collection of the following data:

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

Here, for any field \( K \), we denote by \( \overline{K} \) a separable closure of \( K \) and set \( G_K := \text{Gal}(\overline{K}/K) \). For each prime \( \ell \not\in S(F) \), we set

\[
H^1_{\overline{\ell}}(G_{\mathbb{Q}_n}, T) := H^1_{\text{ur}}(\mathbb{Q}_{\ell}, T) := \ker \left( H^1(\mathbb{Q}_{\ell}, T) \longrightarrow H^1(G_{\mathbb{Q}_{3\ell}'}, T) \right),
\]

where \( G_{\mathbb{Q}_{3\ell}} \) denotes the maximal unramified extension of \( \mathbb{Q}_{\ell} \). We define the Selmer module \( H^1_{\overline{\ell}}(G_{\mathbb{Q}_n}, T) \) by

\[
H^1_{\overline{\ell}}(G_{\mathbb{Q}_n}, T) := \ker \left( H^1(G_{\mathbb{Q}_n}, T) \longrightarrow \bigoplus_{\ell} H^1(G_{\mathbb{Q}_{3\ell}'}, T)/H^1_{\overline{\ell}}(G_{\mathbb{Q}_n}, T) \right).
\]

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

\[
H^1_{\overline{\ell}}(G_{\mathbb{Q}_n}, T^\vee(1)) \subset H^1(G_{\mathbb{Q}_n}, T^\vee(1))
\]

to be the orthogonal complement of \( H^1_{\overline{\ell}}(G_{\mathbb{Q}_n}, T) \) with respect to the local Tate pairing. Hence we obtain the dual Selmer structure \( F^* \) on \( T^\vee(1) \). Throughout this paper, we regard \( F^* \) as a Selmer structure on \( T \) by using the isomorphism \( T \cong T^\vee(1) \) induced by the Weil pairing.
Lemma 2.6. Let \( F_1 \) and \( F_2 \) be Selmer structures on \( T \) satisfying
\[
H^1_{F_1}(G_{\mathbb{Q}}, T) \subset H^1_{F_2}(G_{\mathbb{Q}}, T)
\]
for all prime \( \ell \). Then we have an exact sequence of \( R \)-modules
\[
0 \rightarrow H^1_{F_1}(G_{\mathbb{Q}}, T) \rightarrow H^1_{F_2}(G_{\mathbb{Q}}, T) \rightarrow \bigoplus_{\ell} H^1_{F_1}(G_{\mathbb{Q}}, T)/H^1_{F_2}(G_{\mathbb{Q}}, T)
\]
\[
\rightarrow H^1_{F_1}(G_{\mathbb{Q}}, T)^{\vee} \rightarrow H^1_{F_2}(G_{\mathbb{Q}}, T)^{\vee} \rightarrow 0,
\]
where \( \ell \) runs over all the rational primes satisfying \( H^1_{F_1}(G_{\mathbb{Q}}, T) \neq H^1_{F_2}(G_{\mathbb{Q}}, T) \).
Here \((-)^{\vee} := \text{Hom}(-, \mathbb{Q}_p/\mathbb{Z}_p) \).

Lemma 2.2 ([1, §3.2], [7, Lemma 3.5.3]). For any Selmer structure \( F \) on \( T \), the canonical map \( E[p] \rightarrow T \) induces an isomorphism
\[
H^1_{F}(G_{\mathbb{Q}}, E[p]) \sim \sim H^1_{F}(G_{\mathbb{Q}}, T) [m_R].
\]
Here \( m_R \) denote the maximal ideal of \( R \). In particular, \( H^1_{F}(G_{\mathbb{Q}}, E[p]) = 0 \) if and only if \( H^1_{F}(G_{\mathbb{Q}}, T) = 0 \).

Following Mazur and Rubin, we define the transversal local condition \( H^1_{cl}(G_{\mathbb{Q}}, T) \) and a Selmer structure \( F^0(c) \) 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 \( \ell \), define
\[
H^1_{tr}(G_{\mathbb{Q}}, T) := \ker \left( H^1(G_{\mathbb{Q}}, T) \rightarrow H^1(G_{\mathbb{Q}} \otimes \mathbb{Q}, T) \right).
\]
We also set \( H^1_{tr_*}(G_{\mathbb{Q}}, T) := H^1(G_{\mathbb{Q}}, T)/H^1_{tr}(G_{\mathbb{Q}}, T) \) for \( * \in \{ur, tr\} \).
(3) Let \( a \), \( b \), and \( c \) be pairwise relatively prime (square-free) integers. Define the Selmer structure \( F^0(c) \) on \( T \) by the following data:
\[
S(F^0(c)) := S(F) \cup \{ \ell \mid abc \},
\]
\[
H^1_{F^0(c)}(G_{\mathbb{Q}}, T) := \begin{cases} H^1(G_{\mathbb{Q}}, T) & \text{if } \ell \mid a, \\ 0 & \text{if } \ell \mid b, \\ H^1_{tr}(G_{\mathbb{Q}}, T) & \text{if } \ell \mid c, \\ H^1_{F^0(c)}(G_{\mathbb{Q}}, T) & \text{otherwise}. \end{cases}
\]
Note that \( (F^0(c))^* = (F^0)^0(c) \). For simplicity, we will write \( F^a, F_b, F(c), \ldots \) instead of \( F^1(1), F^1(1), F^1(1), \ldots \), respectively.

Definition 2.4 (classical Selmer structure). We define the classical Selmer structure \( F_{cl} \) on \( T \) by the following:
\[
S(F_{cl}) := S_{\text{bad}}(E) \cup \{ \ell \},
\]
\[
H^1_{F_{cl}}(G_{\mathbb{Q}}, T) := \left( \bigoplus_{\ell \in S(F_{cl})} E(Q_{\mathbb{Q},1}) / p^m \rightarrow H^1(G_{\mathbb{Q}}, T) \right)
\]
for each prime \( \ell \in S(F_{cl}) \).
By definition, the Selmer module \( H^1_{F_{cl}}(G_{\mathbb{Q}}, T) \) coincides with the classical \( p^{\text{er}} \)-Selmer group \( \text{Sel}(\mathbb{Q}, E[p^m]) \) associated with the elliptic curve \( E/\mathbb{Q} \). We also note that \( F_{cl} = F_{cl} \).

Definition 2.5 (canonical Selmer structure). We define the canonical Selmer structure \( F_{can} \) on \( T \) by
\[
F_{can} = F_{cl}^p.
\]
Lemma 2.6. For any prime \( \ell \neq p \), we have
\[
H^1_{F_{can}}(G_{\mathbb{Q}}, T) = H^1_{F_{cl}}(G_{\mathbb{Q}}, T) = H^1_{ur}(G_{\mathbb{Q}}, T).
\]
Lemma 2.10. We have \( L/\text{extension} \) since the Selmer structure 

\[ \text{Remark 2.7} \]

Since we assume \( \text{induced by} \) that there are natural injections 

\[ \text{This fact implies coker} \]

\[ \text{Note that we have the canonical injection} \]

\[ E[p]\hookrightarrow T. \]

Definition 2.8. We say that a Selmer structure \( F \) on \( T \) is cartesian if the homomorphism 

\[ \text{coker} \left( H^1_f(G_{\mathbb{Q}_\ell}, T) \longrightarrow H^1(G_{\mathbb{Q}_\ell}, E[p]) \right) \twoheadrightarrow H^1(G_{\mathbb{Q}_\ell}, E[p])/H^1_f(G_{\mathbb{Q}_\ell}, T) \]

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

Proposition 2.9. The Selmer structure \( F_{\text{can}} \) on \( T \) is cartesian.

Proof. Since we assume \( p \nmid \#E(\mathbb{F}_p) \), we have \( H^2(G_{\mathbb{Q}_\ell}, E[p]) \cong H^0(G_{\mathbb{Q}_\ell}, E[p]) = 0 \). This fact implies coker \( (H^1_{\text{can}}(G_{\mathbb{Q}_\ell}, T) \longrightarrow H^1(G_{\mathbb{Q}_\ell}, E[p])) = 0 \).

Take a prime \( \ell \in S_{\text{bad}}(E) \). Since \( Q_n/\mathbb{Q} \) is unramified at \( \ell \), Lemma 2.6 shows that there are natural injections 

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

and 

\[ H^1(G_{\mathbb{Q}_\ell}, T)/H^1_{\text{can}}(G_{\mathbb{Q}_\ell}, T) \hookrightarrow H^1(G_{\mathbb{Q}_\ell}, E[p]) \cong \bigoplus_{\ell \mid m} H^1(G_{\mathbb{Q}_\ell}, E[p^{m-1}]]. \]

Since \( p \nmid \text{Tam}_r(E) \), the module \( E(\mathbb{Q}_\ell^{ur})[p^\infty] \) is divisible. Hence \( E(\mathbb{Q}_\ell^{ur})[p^m] \xrightarrow{xp} E(\mathbb{Q}_\ell^{ur})[p^{m-1}] \) is surjective, and \( H^1(G_{\mathbb{Q}_\ell}, E[p]) \longrightarrow H^1(G_{\mathbb{Q}_\ell}, E[p^{m-1}]) \) 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 

\[ G := \text{Gal}(K/\mathbb{Q}). \]

Let \( \hat{E} \) denote the formal group associated with \( E/\mathbb{Q}_p \) and put 

\[ \hat{E}(m_{K_p}) := \bigoplus_{p \mid P} \hat{E}(m_{K_p}). \]

Here \( m_L \) denotes the maximal ideal of the ring of integers of \( L \) for any algebraic extension \( L/\mathbb{Q}_p \).

Lemma 2.10. We have \( \hat{E}(m_{Q_p})/p = (\hat{E}(m_{K_p})/p)^G \).

Proof. Since \( p \nmid \#E(\mathbb{F}_p) \), Tan proved in [22, Theorem 2 (a)] that 

\[ H^1(G_{p}, \hat{E}(m_{K_p})) = 0. \]

Take a prime \( p \mid p \) of \( K \) and put \( G_p := \text{Gal}(K_p/\mathbb{Q}_p) \). The injectivity of the inflation map 

\[ H^1(G_p, \hat{E}(m_{K_p})) \longrightarrow H^1(G_{Q_p}, \hat{E}(m_{K_p})) \]

implies \( H^1(G_p, \hat{E}(m_{K_p})) = 0. \) Since
By Proposition 2.11, the $\mathbb{Z} \text{Ind}$
Furthermore, the local Euler characteristic formula implies that $\mathbb{Z}$ is a free $K$ when $K$ 
Definition 2.12.

Here $\text{Ind} \mathbb{F}_p(G)$
Proof. Therefore, Proposition 2.11.
The $\mathbb{Z}$
Hence the vanishing of $H^1(G_p, \mathbb{E}m_{K_p})$ implies
\[ \hat{E}(\mathbb{m}_{K_p})/p = (\hat{E}(\mathbb{m}_{K_p})/p)^G. \]
Since
\[ \hat{E}(\mathbb{m}_{K_p})/p \cong \hat{E}(\mathbb{m}_{K_p})/p \otimes \mathbb{F}_p[G/G_p], \]
we see that $\hat{E}(\mathbb{m}_{K_p})/p = (\hat{E}(\mathbb{m}_{K_p})/p)^G$. □

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

Proof. By Lemma 2.10, we have $(\hat{E}(\mathbb{m}_{K_p})/p)^G = \hat{E}(\mathbb{m}_{K_p})/p \cong \mathbb{F}_p$. Since any finitely generated $\mathbb{F}_p[G]$-module is reflexive, we have
\[ ((\hat{E}(\mathbb{m}_{K_p})/p)^*)^G \cong ((\hat{E}(\mathbb{m}_{K_p})/p)^*)^G \cong (\hat{E}(\mathbb{m}_{K_p})/p)^G \cong \mathbb{F}_p. \]
Here $(-)^* := \text{Hom}_{\mathbb{F}_p[G]}(-, \mathbb{F}_p[G])$. Hence $(\hat{E}(\mathbb{m}_{K_p})/p)^*$ is a cyclic $\mathbb{F}_p[G]$-module.
Furthermore, the fact that $\hat{E}(\mathbb{m}_{K_p}) \cong \mathbb{Z}_p^{[k: \mathbb{Q}]}$ as $\mathbb{Z}_p$-modules implies that
\[ (\hat{E}(\mathbb{m}_{K_p})/p)^* \cong \mathbb{F}_p[G]. \]
Therefore, $\hat{E}(\mathbb{m}_{K_p})/p$ is also free of rank 1, and the $\mathbb{Z}_p[G]$-module $\hat{E}(\mathbb{m}_{K_p})$ is cyclic.
Since $\hat{E}(\mathbb{m}_{K_p}) \cong \mathbb{Z}_p^{[k: \mathbb{Q}]}$, we conclude that $\hat{E}(\mathbb{m}_{K_p}) \cong \mathbb{Z}_p[G]$. □

Definition 2.12. For any integer $m \geq 1$, we put
\[ H^1_f(G_{Q_p}, \text{Ind}_{G_{K_p}}^G(E[p^m])) := \text{im} \left( \hat{E}(\mathbb{m}_{K_p})/p^n \rightarrow H^1(G_{Q_p}, \text{Ind}_{G_{K_p}}^G(E[p^m])) \right). \]
\[ H^1_f(G_{Q_p}, \text{Ind}_{G_{K_p}}^G(E[p^m])) := H^1(G_{Q_p}, \text{Ind}_{G_{K_p}}^G(E[p^m]))/H^1_f(G_{Q_p}, \text{Ind}_{G_{K_p}}^G(E[p^m])). \]

Remark 2.13. Since we assume $p \nmid \#E(\mathbb{F}_p)$, we have $H^1_f(G_{Q_p}, T) = H^1_f(G_{Q_p}, T)$ when $K = \mathbb{Q}_p$.

Corollary 2.14.
(1) The $\mathbb{Z}_p/p^m[G]$-modules
\[ H^1_f(G_{Q_p}, \text{Ind}_{G_{K_p}}^G(E[p^m])) \text{ and } H^1_f(G_{Q_p}, \text{Ind}_{G_{K_p}}^G(E[p^m])) \]
are free of rank 1.
(2) For any subfield $K' \subset K$, we have natural isomorphisms
\[ H^1_f(G_{Q_p}, \text{Ind}_{G_{K_p}}^G(E[p^m]))_{\text{Gal}(K/K')} \cong H^1_f(G_{Q_p}, \text{Ind}_{G_{K_p}}^G(E[p^m])), \]
\[ H^1_f(G_{Q_p}, \text{Ind}_{G_{K_p}}^G(E[p^m]))_{\text{Gal}(K/K')} \cong H^1_f(G_{Q_p}, \text{Ind}_{G_{K_p}}^G(E[p^m])). \]

Proof. For simplicity, we put $T_K := \text{Ind}_{G_{K_p}}^G(T_K(E))$. We note that $T_K/p^m \cong \text{Ind}_{G_{K_p}}^G(E[p^m])$. Since $H^2(G_{Q_p}, E[p]) \cong H^0(G_{Q_p}, E[p]) = 0$ and $\text{Rf}(G_{Q_p}, T_K) \otimes_{\mathbb{Z}_p[G]} \mathbb{F}_p \cong \text{Rf}(G_{Q_p}, E[p])$, the perfect complex $\text{Rf}(G_{Q_p}, T_K)$ is of perfect amplitude in $[1, 1]$. Hence, for any ideal $I$ of $\mathbb{Z}_p[G]$, we have
\[ H^1(G_{Q_p}, T_K) \otimes_{\mathbb{Z}_p[G]} \mathbb{Z}_p[G]/I \cong H^1(G_{Q_p}, T_K/IT_K). \]
Furthermore, the local Euler characteristic formula implies that $H^1(G_{Q_p}, T_K/IT_K)$ is a free $\mathbb{Z}_p[G]/I$-module of rank 2.
1) By Proposition 2.11, the $\mathbb{Z}_p/p^m[G]$-module $H^1_f(G_{Q_p}, T_K/p^m)$ is free of rank 1. Since $\mathbb{Z}_p/p^m[G]$ is a self-injective ring, $H^1_f(G_{Q_p}, T_K/p^m)$ is also free of rank 1.
2) By claim (1), the exact sequence of \( \mathbb{Z}_p/p^m[G] \)-modules
\[
0 \rightarrow H_1^f(G_{Q_p}, T_K/p^m) \rightarrow H^1(G_{Q_p}, T_K/p^m) \rightarrow H_1^f(G_{Q_p}, T_K/p^m) \rightarrow 0
\]
is split. Hence we obtain the exact sequence of free \( \mathbb{Z}_p/p^m[\text{Gal}(K'/\mathbb{Q})] \)-modules
\[
0 \rightarrow H_1^f(G_{Q_p}, T_K/p^m)_{\text{Gal}(K'/\mathbb{Q})} \rightarrow H^1(G_{Q_p}, T_K/p^m)_{\text{Gal}(K'/\mathbb{Q})} \rightarrow H_1^f(G_{Q_p}, T_K/p^m)_{\text{Gal}(K'/\mathbb{Q})} \rightarrow 0.
\]
Since \( H^1(G_{Q_p}, T_K/p^m)_{\text{Gal}(K'/\mathbb{Q})} \cong H^1(G_{Q_p}, T_{K'/p^m}) \), the homomorphism
\[
H_1^f(G_{Q_p}, T_K/p^m)_{\text{Gal}(K'/\mathbb{Q})} \rightarrow H^1(G_{Q_p}, T_{K'/p^m})
\]
is injective. Hence by claim (1), we obtain isomorphisms
\[
H_1^f(G_{Q_p}, T_K/p^m)_{\text{Gal}(K'/\mathbb{Q})} \cong H^1(G_{Q_p}, T_{K'/p^m})
\]
Corollary 2.15. The Selmer structure \( F_{cl} \) on \( T \) is cartesian.

Proof. By Proposition 2.9, it suffices to show that the homomorphism
\[
H_1^f(G_{Q_p}, E[p]) \rightarrow H_1^f(G_{Q_p}, T)
\]
is injective. Note that this map factors through \( H_1^f(G_{Q_p}, E[p^m]) \). By Corollary 2.14, the canonical homomorphism \( H_1^f(G_{Q_p}, E[p^m]) \rightarrow H_1^f(G_{Q_p}, T) \) is injective. Let us show that \( H_1^f(G_{Q_p}, E[p^m]) \rightarrow H_1^f(G_{Q_p}, E[p^m]) \) is injective. Since \( H^1(G_{Q_p}, E[p^m]) \) is a free \( \mathbb{Z}_p/p^m \)-module and \( H^1(G_{Q_p}, E[p^m]) \otimes F_p \cong H^1(G_{Q_p}, E[p]) \), the canonical homomorphism \( H^1(G_{Q_p}, E[p]) \rightarrow H^1(G_{Q_p}, E[p^m]) \) is injective. By definition, we have
\[
H_1^f(G_{Q_p}, E[p^m]) \otimes F_p = \hat{E}(m_{Q_p})/p^m \otimes F_p = \hat{E}(m_{Q_p})/p = H_1^f(G_{Q_p}, E[p]).
\]
Since \( H_1^f(G_{Q_p}, E[p]) \cong \mathbb{Z}_p/p^m \) by Corollary 2.14, we see that the canonical homomorphism \( H_1^f(G_{Q_p}, E[p]) \rightarrow H_1^f(G_{Q_p}, E[p^m]) \) 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 [7]. We set
\[
\mathcal{P}_{m,n} := \{ \ell \notin S_{\text{bad}}(E) \mid E(F_p)[p^m] \cong \mathbb{Z}/p^m \text{ and } \ell \equiv 1 \pmod{p_{\text{max}}(m,n+1)} \}.
\]
For any prime \( \ell \in \mathcal{P}_{m,n} \), the \( R \)-module \( H_{1ur}^1(G_{Q_{\ell}}, T) \cong T/(F_{\ell} - 1)T \) is free of rank 1. Moreover, by [7, Lemmas 1.2.1, 1.2.3 and 1.2.4], we have
\[
H^1(G_{Q_{\ell}}, T) = H_{1ur}^1(G_{Q_{\ell}}, T) \oplus H_{1tr}^1(G_{Q_{\ell}}, T)
\]
and the \( R \)-modules \( H_{1tr}^1(G_{Q_{\ell}}, T) \), \( H_{1ur}^1(G_{Q_{\ell}}, T) \), and \( H_{1tr}^1(G_{Q_{\ell}}, T) \) are free of rank 1. Let \( N_{m,n} \) denote the set of square-free products in \( \mathcal{P}_{m,n} \). For each integer \( d \in N_{m,n} \), we put
\[
G_d := \bigotimes_{\ell \mid d} \text{Gal}(\mathbb{Q}(\ell)/\mathbb{Q}).
\]
For any prime \( \ell \in \mathcal{P}_{m,n} \), we have two homomorphisms
\[
\nu_{\ell} : H^1(G_{Q_{\ell}}, T) \xrightarrow{\text{loc}} H^1(G_{Q_{\ell}}, T) \rightarrow H_{1ur}^1(G_{Q_{\ell}}, T),
\]
\[
\varphi_{\ell} : H^1(G_{Q_{\ell}}, T) \xrightarrow{\text{loc}} H^1(G_{Q_{\ell}}, T) \xrightarrow{\text{pr}_{\text{ur}}} H_{1ur}^1(G_{Q_{\ell}}, T) \phi_{\ell}^p \rightarrow H_{1tr}^1(G_{Q_{\ell}}, T) \oplus_2 G_{\ell}.
\]
Here \( \phi_{\ell}^p \) is the finite-singular comparison map defined in [7, Definition 1.2.2] and \( \text{pr}_{\text{ur}} \) denotes the projection map with respect to the decomposition \( H^1(G_{Q_{\ell}}, T) = H_{1ur}^1(G_{Q_{\ell}}, T) \oplus H_{1tr}^1(G_{Q_{\ell}}, T) \).
Definition 2.16. We define the module $\text{KS}_1(T, F_{\text{can}})$ of Kolyvagin systems of rank 1 to be the set of elements

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

satisfying the finite-singular relation

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

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

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 $H^1_{F_{\text{can}}(c)}(G_{\mathbb{Q}}, E[p]) = 0$, then the $R$-module $H^1_{(F_{\text{can}})^b(c)}(G_{\mathbb{Q}}, T)$ is free of rank $\nu(a) - \nu(b) + 1$.

Proof. Since $F_{\text{can}}$ is cartesian by Proposition 2.9, so is $(F_{\text{can}})^b(c)$ by [17, Corollary 3.18]. By [7, Proposition 6.2.2], we have

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

and [17, Corollary 3.21] implies $\chi((F_{\text{can}})^b(c)) = \nu(a) - \nu(b) + 1$. Hence this lemma follows from [17, Lemma 4.6].

2.4. Kolyvagin systems of rank 0. In this subsection, we recall the definition of Kolyvagin system of rank 0 in our previous paper [19]. Fix an isomorphism

$$H^1_{f_{\text{ur}}}(G_{\mathbb{Q}}, T) \cong R$$

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

$$v_\ell: H^1(G_{\mathbb{Q}}, T) \longrightarrow H^1_{f_{\text{ur}}}(G_{\mathbb{Q}}, T) \cong R,$$

$$\varphi_\ell^b: H^1(G_{\mathbb{Q}}, T) \longrightarrow H^1_{f_{\text{ur}}}(G_{\mathbb{Q}}, T) \otimes_{\mathbb{Z}} G_{\ell} \cong R \otimes_{\mathbb{Z}} G_{\ell}.$$

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

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

$$(\kappa_{d,\ell})_{(d, \ell) \in M_{m,n}} \in \prod_{(d, \ell) \in M_{m,n}} H^1_{F_{\text{cl}}(d)}(G_{\mathbb{Q}}, T) \otimes_{\mathbb{Z}} G_n$$

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

$$v_\ell(\kappa_{d,q}) = \varphi_\ell^b(\kappa_{d,q}),$$

$$v_\ell(\kappa_{q,\ell}) = v_q(\kappa_{q,\ell}),$$

$$v_\ell(\kappa_{d,\ell q}) = -\varphi_\ell^b(\kappa_{d,\ell q}).$$

We denote by $\text{KS}_0(T, F_{\text{cl}})$ the module of Kolyvagin systems of rank 0. For any Kolyvagin system $\kappa \in \text{KS}_0(T, F_{\text{cl}})$ and any element $(d, \ell) \in M_{\text{ur}}$, we put

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

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

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

Note that $F_{\text{cl}} = F_{\text{cl}}^*.$

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

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

$$0 \rightarrow H^1_{(\mathcal{F},\lambda)}(G_{\mathbb{Q}}, T) \rightarrow H^1_{(\mathcal{F},\lambda)}(G_{\mathbb{Q}}, T) \rightarrow H^1_{f}(G_{\mathbb{Q}}, T) \rightarrow 0.$$ 

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

When $p > 3$, the following theorem is proved in [19, Proposition 5.6, Theorem 5.8]. When $p = 3$, it is proved in Appendix A.

**Theorem 2.20.**

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

$$\text{KS}_0(T, \mathcal{F}_{\text{cl}}) \rightarrow H^1_{(\mathcal{F},\lambda)}(G_{\mathbb{Q}}, T) \otimes_{\mathbb{Z}} G_d$$

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

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

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

**Remark 2.21.** For any Selmer structure $\mathcal{F}$ on $E[p]$ with $\chi(\mathcal{F}) \geq 0$, there are infinitely many integers $d \in N_{m,n}$ satisfying $H^1_{(\mathcal{F},\lambda)}(G_{\mathbb{Q}}, E[p]) = 0$ (see [7, Corollary 4.1.9]).

**Corollary 2.22.** The homomorphism $\delta$ is injective.

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

2.5. Map from Kolyvagin systems of rank 1 to Kolyvagin systems of rank 0. Fix an isomorphism

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

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

$$\begin{array}{ccc}
\text{KS}_1(T, \mathcal{F}_{\text{can}}) & \xrightarrow{\varphi} & \text{KS}_0(T, \mathcal{F}_{\text{cl}}) \\
\downarrow{\delta} & & \\
\prod_{d \in N_{m,n}} R \otimes_{\mathbb{Z}} G_d & & \\
\end{array}$$

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

For any $R$-module $M$, we put

$$M^* := \text{Hom}_R(M, R) \quad \text{and} \quad \bigcap^r_R M := \left(\bigwedge^r_R M^* \right)^*$$

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

$$\phi: \bigcap^r_R M \rightarrow F \otimes_R \bigcap^r_R \ker(\phi).$$
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

$$W_d := \bigoplus_{\ell | d} H^1_{\text{ur}}(G_{\mathbb{Q},\ell}, T)^*,$$

$$X_d^r(T, \mathcal{F}) := \bigcap_{\ell | d} H^1_{\text{ur}}(G_{\mathbb{Q},\ell}, T) \otimes_R \text{det}(W_d).$$

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

$$0 \rightarrow H^1_{\text{ur}}(G_{\mathbb{Q},T}) \rightarrow H^1_{\text{ur}}(G_{\mathbb{Q},T}) \rightarrow \bigoplus_{\ell | d} H^1_{\text{ur}}(G_{\mathbb{Q},\ell}, T)$$

induces a natural homomorphism

$$\Phi_{d,e} : X_d^r(T, \mathcal{F}) \rightarrow X_d^r(T, \mathcal{F})$$

(see [17, Definition 2.3]). If $f | e | d$, then we have $\Phi_{d,f} = \Phi_{e,f} \circ \Phi_{d,e}$ (see [17, Proposition 2.4]), and we obtain the module of Stark systems of rank $r$

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

Since we have the isomorphisms

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

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

$$0 \rightarrow H^1_{\mathcal{F}_{\text{can},(d)}}(G_{\mathbb{Q},T}) \rightarrow H^1_{\mathcal{F}_{\text{can},(d)}}(G_{\mathbb{Q},T}) \rightarrow \bigoplus_{\ell | d} H^1_{\text{tr}}(G_{\mathbb{Q},\ell}, T)$$

induces a natural homomorphism

$$\Pi_d : X_d^1(T, \mathcal{F}_{\text{can}}) \rightarrow \bigcap_{\ell | d} H^1_{\mathcal{F}_{\text{can},(d)}}(G_{\mathbb{Q},T}) \otimes_{\mathbb{Z}} G_{d} = H^1_{\mathcal{F}_{\text{can},(d)}}(G_{\mathbb{Q},T}) \otimes_{\mathbb{Z}} G_{d},$$

and we obtain

$$\text{Reg}_1 : \text{SS}_1(T, \mathcal{F}_{\text{can}}) \rightarrow \text{KS}_1(T, \mathcal{F}_{\text{can}}); \quad ((\epsilon_d)_{d \in \mathcal{N}_{m,n}}) \mapsto ((-1)^{e(d)} \Pi_d(\epsilon_d))_{d \in \mathcal{N}_{m,n}}$$

(see [2, Proposition 4.3] or [8, Proposition 12.3]). The following important proposition is proved by Mazur and Rubin in [8, Proposition 12.4] when $p > 3$ (see also [1, Theorem 5.2(i)] and [18, Theorem 3.17]). When $p = 3$, this proposition is proved in Appendix A.

Proposition 2.24. The map

$$\text{Reg}_1 : \text{SS}_1(T, \mathcal{F}_{\text{can}}) \rightarrow \text{KS}_1(T, \mathcal{F}_{\text{can}})$$

is an isomorphism.

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

$$0 \rightarrow H^1_{\mathcal{F}_{\text{can},(d)}}(G_{\mathbb{Q},T}) \rightarrow H^1_{\mathcal{F}_{\text{can},(d)}}(G_{\mathbb{Q},T}) \rightarrow \bigoplus_{\ell | d} H^1_{\text{tr}}(G_{\mathbb{Q},\ell}, T)$$

induces a natural homomorphism

$$\Pi'_d : X_d^0(T, \mathcal{F}_{\text{el}}) \rightarrow \bigcap_{\ell | d} H^1_{\mathcal{F}_{\text{can},(d)}}(G_{\mathbb{Q},T}) \otimes_{\mathbb{Z}} G_{d} = R \otimes_{\mathbb{Z}} G_{d}.$$

Hence we obtain a homomorphism

$$\psi : \text{SS}_0(T, \mathcal{F}_{\text{el}}) \rightarrow \prod_{d \in \mathcal{N}_{m,n}} R \otimes_{\mathbb{Z}} G_{d}; \quad (\epsilon_d)_{d \in \mathcal{N}_{m,n}} \mapsto ((\Pi'_d(\epsilon_d))_{d \in \mathcal{N}_{m,n}}.$$

In [19, §5.2], we construct the canonical homomorphism

$$\text{Reg}_0 : \text{SS}_0(T, \mathcal{F}_{\text{el}}) \rightarrow \text{KS}_0(T, \mathcal{F}_{\text{el}})$$

such that the diagram
\[
\begin{array}{ccc}
\SS_0(T, \mathcal{F}_{\text{cl}}) & \xrightarrow{\Reg} & \KS_0(T, \mathcal{F}_{\text{cl}}) \\
\psi & & \downarrow \phi \\
\prod_{d \in N_{m,n}} R \otimes \mathbb{Z} G_d & & 
\end{array}
\]
(3)
commutes.

For any integer \(d \in N_{m,n}\), we have an exact sequence
\[
0 \longrightarrow H^1_{J_{cl}}(G_\mathbb{Q}, T) \longrightarrow H^1_{F_{\text{can}}}(G_\mathbb{Q}, T) \xrightarrow{\varphi} R.
\]
This exact sequence induces a homomorphism \(X^1_{J}(T, \mathcal{F}_{\text{can}}) \longrightarrow X^0_{\delta}(T, \mathcal{F}_{\text{cl}})\), and we obtain a homomorphism \(\SS_1(T, \mathcal{F}_{\text{can}}) \longrightarrow \SS_0(T, \mathcal{F}_{\text{cl}})\). By construction, the diagram
\[
\begin{array}{ccc}
\SS_1(T, \mathcal{F}_{\text{can}}) & \longrightarrow & \SS_0(T, \mathcal{F}_{\text{cl}}) \\
\Reg_1 \downarrow & & \downarrow \psi \\
\KS_1(T, \mathcal{F}_{\text{can}}) & \xrightarrow{\phi} & \prod_{d \in N_{m,n}} R \otimes \mathbb{Z} G_d 
\end{array}
\]
(4)
commutes. Since \(\Reg_1\) is an isomorphism, by using the commutative diagrams (3) and (4), we obtain the homomorphism \(\KS_1(T, \mathcal{F}_{\text{can}}) \longrightarrow \KS_0(T, \mathcal{F}_{\text{cl}})\) 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
\[
R_K := \mathbb{Z}_p[\Gal(K/\mathbb{Q})] \quad \text{and} \quad T_K := \Ind_{G_\mathbb{Q}}^{G_K}(T_p(E)).
\]

3.1. Modular symbols. We recall the definition of the Mazur–Tate elements.
For any integer \(d \geq 1\), we define the modular element \(\tilde{\theta}_{Q(\mu_d)}\) by
\[
\tilde{\theta}_{Q(\mu_d)} := \sum_{\substack{a \in \mathbb{Z}_p^\times \\cap \langle a, d \rangle \neq 1}} \frac{\text{Re}([a/d])}{\Omega_k^a} \sigma_a \in \mathbb{Q}[\Gal(\mathbb{Q}(\mu_d)/\mathbb{Q})].
\]
Here \(\sigma_a \in \Gal(\mathbb{Q}(\mu_d)/\mathbb{Q})\) is the element satisfying \(\sigma_a(\zeta) = \zeta^a\) for any \(\zeta \in \mu_d\). For any integer \(e \mid d\), we put
\[
\nu_{d,e} : R_{Q(\mu_d)} \longrightarrow R_{Q(\mu_d)}; \quad x \mapsto \sum_{\sigma \in \Gal(\mathbb{Q}(\mu_d)/\mathbb{Q}(\mu_{e}))} \sigma x.
\]
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 \(G_\mathbb{Q} \longrightarrow \text{GL}(E[p])\) is surjective, for any integers \(d \in \mathcal{N}\) and \(n \geq 1\), we have
\[
\tilde{\theta}_{Q(\mu_{dp^n})} \in R_{Q(\mu_{dp^n})}
\]
(see [21]). Let \(\alpha \in \mathbb{Z}_p^\times\) be the unit root of \(x^2 - a_p x + p = 0\). We set
\[
\theta_{Q(\mu_{dp^n})} := \alpha^{-n}(\tilde{\theta}_{Q(\mu_{dp^n})} - \alpha^{-1} \nu_{d,p^n,dp^n-1}(\tilde{\theta}_{Q(\mu_{dp^n-1})})) \in R_{Q(\mu_{dp^n})}.
\]
Then the set \(\{\vartheta_{Q(\mu_{dp^n})}\}_{n \geq 1}\) is a projective system and we get an element
\[
\vartheta_{Q(\mu_{dp^n})} := \lim_{\longrightarrow n} \vartheta_{Q(\mu_{dp^n})} \in \lim_{\longrightarrow n} R_{Q(\mu_{dp^n})} =: \Lambda_{Q(\mu_{dp^n})}.
\]
Remark 3.1. Note that for any positive integer $d \nmid p$, we have
\[ \vartheta_{\mathbb{Q}(\mu_d)} = (1 - \alpha^{-1} \sigma_p) (1 - \alpha^{-1} \sigma_p^{-1}) \vartheta_{\mathbb{Q}(\mu_d)}. \]
The assumption (c) shows that $\alpha \not\equiv 1 \pmod{p}$, and $(1 - \alpha^{-1} \sigma_p) (1 - \alpha^{-1} \sigma_p^{-1})$ is a unit in $R_{\mathbb{Q}(\mu_d)}$.

For any prime $\ell$ with $\ell \nmid d$, let $\pi_{\ell,d,d}$: $\Lambda_{\mathbb{Q}(\mu_{d\ell})} \rightarrow \Lambda_{\mathbb{Q}(\mu_{d\ell})}$ denote the natural projection map, and we have
\[ \pi_{\ell,d,d}(\vartheta_{\mathbb{Q}(\mu_{d\ell})}) = (a_\ell - \sigma_\ell - \sigma_\ell^{-1}) \vartheta_{\mathbb{Q}(\mu_{d\ell})}. \]
Here $a_\ell := \ell + 1 - \#E(\mathbb{F}_\ell)$. Following Kurihara in [6, page 324], for any positive divisor $e$ of $d$, we put
\[ \alpha_{d,e} := \left( \prod_{\ell \mid d} (-\sigma_\ell^{-1}) \right) \vartheta_{\mathbb{Q}(\mu_{d\ell})} \in \Lambda_{\mathbb{Q}(\mu_{d\ell})}, \]
\[ \xi_{\mathbb{Q}(\mu_{d\ell})} := \sum_{e \mid d} \alpha_{d,e}(\alpha_{d,e}) \in \Lambda_{\mathbb{Q}(\mu_{d\ell})}. \]
Here $e$ runs over the set of positive divisors of $d$. We also put
\[ \tilde{\xi}_{\mathbb{Q}(\mu_{d\ell})} := \left( \prod_{\ell \mid d} (-\ell \sigma_\ell^{-1}) \right) \xi_{\mathbb{Q}(\mu_{d\ell})}. \]

Definition 3.2. For any prime $\ell \in \mathcal{P}$, we define the Frobenius polynomial at $\ell$ by
\[ P_\ell(t) := \det(1 - t \sigma_\ell^{-1} \mid T) = t^2 - t^{-1} a_\ell + \ell^{-1}. \]

Proposition 3.3. For any integer $d \in \mathbb{N}$ and any prime $\ell \in \mathcal{P}$ with $\ell \nmid d$, we have
\[ \pi_{\ell,d,d}(\tilde{\xi}_{\mathbb{Q}(\mu_{d\ell})}) = P_\ell(\sigma_\ell^{-1}) \tilde{\xi}_{\mathbb{Q}(\mu_{d\ell})}. \]

Proof. Kurihara showed in [6, page 325, (7)] that
\[ \pi_{\ell,d,d}(\xi_{\mathbb{Q}(\mu_{d\ell})}) = (-\sigma_\ell + a_\ell - \ell \sigma_\ell^{-1}) \xi_{\mathbb{Q}(\mu_{d\ell})} = (-\ell \sigma_\ell) P_\ell(\sigma_\ell^{-1}) \xi_{\mathbb{Q}(\mu_{d\ell})}, \]
which implies $\pi_{\ell,d,d}(\tilde{\xi}_{\mathbb{Q}(\mu_{d\ell})}) = P_\ell(\sigma_\ell^{-1}) \tilde{\xi}_{\mathbb{Q}(\mu_{d\ell})}$.

3.2. Coleman maps. Let $K/\mathbb{Q}$ be a $p$-abelian extension at which $p$ is unramified, and we denote by $K_\infty/K$ the cyclotomic $\mathbb{Z}_p$-extension. Put
\[ \Lambda_{K_\infty} := \mathbb{Z}_p[[\text{Gal}(K_\infty/\mathbb{Q})]] \quad \text{and} \quad \mathbb{T}_{K_\infty} := \lim_{\longleftarrow} T_{K_n}, \]
where $K_n$ denotes the $n$-th layer of the cyclotomic $\mathbb{Z}_p$-extension $K_\infty/K$. We note that the $\Lambda_{K_{\infty}}$-module $H^1_{\text{I}}(G_\mathbb{Q}, T_{K_{\infty}})$ is free of rank 1 by Corollary 2.14.

The following theorem follows from the works of Perrin-Riou in [16] and Kato in [4]

Theorem 3.4 ([4, Theorem 16.4, Theorem 16.6, and Proposition 17.11]). There exists an isomorphism
\[ \mathcal{L}_{K_\infty} : H^1_{\text{I}}(G_\mathbb{Q}, T_{K_{\infty}}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \overset{\sim}{\rightarrow} \Lambda_{K_\infty} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \]
such that
Remark 3.5. Note that the integrality of the element $z_{K,\infty}$ follows from the assumption (b) (see [3, Theorem 6.1]).

### 3.3. Euler systems

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

**Definition 3.6.**

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

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

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

Here $\text{Cor}_{K_2/K_1} : H^1(G_Q, \mathbb{T}_{K_2,\infty}) \to H^1(G_Q, \mathbb{T}_{K_1,\infty})$ denotes the homomorphism induced by $\mathbb{T}_{K_2,\infty} \to \mathbb{T}_{K_1,\infty}$. Let $\text{ES}_1(T)$ 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 $\Omega$, we have

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

Here $\pi_{K_2,K_1} : \Lambda_{K_2,\infty} \to \Lambda_{K_1,\infty}$ denotes the canonical projection map. Let $\text{ES}_0(T)$ denote the set of Euler systems of rank 0.

For any abelian field $K$ of conductor $d$, we denote by $\xi_{K,\infty}$ the image of $\xi_{Q,(\mu_d)_{\infty}}$ in $\Lambda_{K,\infty}$. Then Proposition 3.3 implies the following proposition.

**Proposition 3.7.** We have $(\xi_{K,\infty})_{K \in \Omega} \in \text{ES}_0(T)$.

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

$$0 \to \text{Sel}(K_n, E[p^m]) \to H^1_{\text{an}}(G_Q, T_{K_n/p^m}) \to H^1_{f}(G_Q, T_{K_n/p^m}) \to \text{Sel}(K_n, E[p^m])^\vee.$$

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

$$H^1_{\text{an}}(G_Q, T_{K_n/p^m}) := \ker \left( H^1(G_Q, T_{K_n/p^m}) \to \bigoplus_{\ell \neq p} H^1_{\text{ur}}(G_Q, T_{K_n/p^m}) \right).$$
We set
\[ H^1_f(G_{Q}, T_{K_{\infty}}) \ := \ \lim_{m,n} H^1_f(G_{Q}, T_{K_{\infty}}/p^m), \]
\[ \text{Sel}(K_{\infty}, E[p^\infty]) \ := \ \lim_{m,n} \text{Sel}(K_n, E[p^m]). \]
Since \( \text{Sel}(K_{\infty}, E[p^\infty]) \) is a finitely generated torsion \( \Lambda_{K_{\infty}} \)-module, we have
\[ \lim_{m,n} \text{Sel}(K_n, E[p^m]) = 0. \]
Moreover, [12, Proposition B.3.4] implies
\[ H^1(G_{Q}, T_{K_{\infty}}) = \lim_{m,n} H^1_{\text{can}}(G_{Q}, T_{K_{n}}/p^m). \]
Hence we get an exact sequence of \( \Lambda_{K_{\infty}} \)-modules
\[ 0 \to H^1(K_{Q}, T_{K_{\infty}}) \to H^1_f(K_{Q}, T_{K_{\infty}}) \to \text{Sel}(K_{\infty}, E[p^\infty]) \to 0. \]
For each field \( K \in \Omega \), we put
\[ M_{K_{\infty}} := (\text{loc}_p^{(j)})^{-1}(H^1(K_{Q}, T_{K_{\infty}}) \cap \mathfrak{L}_{K_{\infty}}^{-1}(\Lambda_{K_{\infty}})), \]
and we obtain an injection
\[ \mathfrak{L}: \text{ES}_1(T) \cap \prod_{K \in \Omega} M_{K_{\infty}} \hookrightarrow \text{ES}_0(T); (c_K)_{K \in \Omega} \mapsto (\text{loc}_p^{(j)}(\mathfrak{L}_{K_{\infty}}(c_K)))_{K \in \Omega}. \]
Then Theorem 3.4 and the injectivity of \( \text{loc}_p^{(j)} \circ \mathfrak{L}_{K_{\infty}} \) imply the following proposition.

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

### 3.4. Construction of \( \kappa_{d,m,n} \)

Fix integers \( m \geq 1 \) and \( n \geq 0 \). First, we introduce the Kolyvagin derivative homomorphism (defined by Mazur and Rubin in [7])
\[ \mathcal{D}^{1}_{m,n}: \text{ES}_1(T) \to \text{KS}_1(T_{Q_n}/p^m, \mathcal{F}_{\text{can}}). \]
Recall that \( Q(d) \) is the maximal \( p \)-subextension of \( Q(\mu_d) \), and note that \( Q_n = Q(p^{n+1}) \). We fix a generator \( g_\ell \) of \( G_{\ell} = \text{Gal}(Q(\ell)/Q) \) for each prime \( \ell \in \mathcal{P}_{1,0} \) and denote by \( D_\ell \in Z[G_{\ell}] \) 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_{d|d} D_\ell \in Z[\text{Gal}(Q(d)/Q) \]}. Let \( c \in \text{ES}_1(T) \) be an Euler system. For any integer \( d \in \mathcal{N}_{m,n} \), we denote by \( c_{d p^{n+1}} \in H^1(G_{Q}, T_{Q(p^{n+1})}) \) the image of \( c_{Q(d)} \in H^1(G_{Q}, T_{Q(d)}) \). Then it is well-known that Euler system relations imply
\[ \kappa(c)_{d,m,n} := D_d c_{d p^{n+1}} \mod p^m \in H^1(G_{Q}, T_{Q(p^{n+1})/p^m})^{\text{Gal}(Q(d)/Q)}. \]
(see, for example, [12, Lemma 4.4.2]). Since we have an isomorphism
\[ H^1(G_{Q}, T_{Q_n}/p^m) \cong H^1(G_{Q}, T_{Q(p^{n+1})/p^m})^{\text{Gal}(Q(d)/Q)}, \]
we can regard \( \kappa(c)_{d,m,n} \) as an element of \( H^1(G_{Q}, T_{Q_n}/p^m) \). The following theorem is proved by Mazur and Rubin in [7, Appendix A].

**Theorem 3.9.** For any Euler system \( c \in \text{ES}_1(T) \), we have
\[ \mathcal{D}^{1}_{m,n}(c) := (\kappa(c)_{d,m,n})_{d \in \mathcal{N}_{m,n}} \in \text{KS}_1(T_{Q_n}/p^m, \mathcal{F}_{\text{can}}). \]
Hence we obtain the Kolyvagin derivative homomorphism
\[ \mathcal{D}^{1}_{m,n}: \text{ES}_1(T) \to \text{KS}_1(T_{Q_n}/p^m, \mathcal{F}_{\text{can}}). \]
Remark 3.10. For any $\ell \in P_{m,n}$, we have

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

Hence $\kappa(c)_{d,m,n}$ coincides with $\kappa'_d$ defined in [7, page 80, (33)].

Next let us construct a homomorphism

$$D^\ell_{m,n} : ES_0(T) \rightarrow \prod_{d \in N_{m,n}} R_{Q_d}/p^m \otimes \mathbb{Z} G_d.$$  

Let $c \in ES_0(T)$ be an Euler system and take an integer $d \in N_{m,n}$. We denote by $c_{dp^{n+1}} \in R_{Q_d(p^{n+1})}$ the image of $c_{Q_d} \in \Lambda_{Q_d}$.

**Lemma 3.11.** For any integer $d \in N_{m,n}$, we have

$$\delta(c)_{d,m,n} := D_d c_{dp^{n+1}} \pmod{p^m} \in (R_{Q_d(p^{n+1})}/p^m)^{\text{Gal}(Q_d/Q)} \rightarrow R_{Q_d}/p^m.$$  

Moreover, if we write $c_{dp^{n+1}} \pmod{p^m} = \sum_{\sigma \in \text{Gal}(Q_d/Q)} a_{\sigma} \sigma$, where $a_{\sigma} \in R_{Q_d}/p^m$, then we have

$$\delta(c)_{d,m,n} = (-1)^{\nu(d)} \sum_{\sigma \in \text{Gal}(Q_d/Q)} a_{\sigma} \prod_{\ell \mid d} \log_{g_{\ell}}(\sigma).$$  

Here

$$\log_{g_{\ell}} : G_{\ell} \hookrightarrow \mathbb{Z}/(\ell - 1) \rightarrow \mathbb{Z}/p^m : g_{\ell}^a \mapsto a \pmod{p^m}$$

is the surjection induced by the discrete logarithm to the base $g_{\ell}$.

**Proof.** The assertion that

$$D_d c_{dp^{n+1}} \pmod{p^m} \in (R_{Q_d(p^{n+1})}/p^m)^{\text{Gal}(Q_d/Q)}$$

is well-known (see, for example, [12, Lemma 4.4.2]). Let us show the latter assertion. We write $d = \ell_1 \cdots \ell_t$. We put

$$N_{\ell_i} := \sum_{\sigma \in \text{Gal}(Q_{(\ell_i)})} \sigma$$

and $X_{\ell_i} := g_{\ell_i} - 1$.

Note that $D_{\ell_i} X_{\ell_i} = -N_{\ell_i}$ and $D_{\ell_i} X_{\ell_i}^2 = 0$. Hence we have

$$D_d \sum_{\sigma \in \text{Gal}(Q_d/Q)} a_{\sigma} \sigma = \sum_{i_1 = 1}^{G_{\ell_1} - 1} \cdots \sum_{i_t = 1}^{G_{\ell_t} - 1} a_{g_{\ell_1} \cdots g_{\ell_t}} D_d (1 + X_{\ell_1})^{i_1} \cdots (1 + X_{\ell_t})^{i_t}$$

$$= \sum_{i_1 = 1}^{G_{\ell_1} - 1} \cdots \sum_{i_t = 1}^{G_{\ell_t} - 1} a_{g_{\ell_1} \cdots g_{\ell_t}} (1 - i_1 N_{\ell_1}) \cdots (1 - i_t N_{\ell_t})$$

$$= \sum_{i = 1}^{G_d - 1} \sum_{j_i \in \{0, 1\}} b_{j_1 \cdots j_t} N_{\ell_1} \cdots N_{\ell_t}.$$  

Since

$$b_{1 \cdots 1} = (-1)^{\nu(d)} \sum_{\sigma \in \text{Gal}(Q_d/Q)} a_{\sigma} \prod_{\ell \mid d} \log_{g_{\ell}}(\sigma),$$

it suffices to show that $b_{j_1 \cdots j_t}$ is 0 for any $(j_1, \ldots, j_t) \neq (1, \ldots, 1)$. This follows from the facts that $X_{\ell_i} D_d c_{dp^{n+1}} \pmod{p^m} = 0$ and $X_{\ell_i} N_{\ell_i} = 0$ for any $1 \leq i \leq t$.

In fact, since

$$0 = X_{\ell_1} \cdots X_{\ell_t} D_d c_{dp^{n+1}} \pmod{p^m} = b_{0 \cdots 0} X_{\ell_1} \cdots X_{\ell_t},$$

we have $b_{0 \cdots 0} = 0$. Moreover, since

$$0 = X_{\ell_2} \cdots X_{\ell_t} D_d c_{dp^{n+1}} \pmod{p^m} = (b_{0 \cdots 0} + b_{1,0 \cdots 0}) X_{\ell_2} \cdots X_{\ell_t},$$

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

Definition 3.12. We define the homomorphism
\[ D^0_{m,n} : E_S(T) \rightarrow \prod_{d \in \mathcal{N}_{m,n}} R_{Q_n}/p^m \otimes \mathbb{G}_d \]
by \( D^0_{m,n}(c) := (\delta(c)_{d,m,n})_{d \in \mathcal{N}_{m,n}} \).

Recall that we have the isomorphism \( \mathcal{L}_{Q_{\infty}} : H^1_f(G_{Q_p}, T_{Q_{\infty}}) \sim \Lambda_{Q_{\infty}} \) by Theorem 3.4(ii). Since
\[ H^1_f(G_{Q_p}, T_{Q_{\infty}}) \otimes_{\Lambda_{Q_{\infty}}} R_{Q_n}/p^m \sim H^1_f(G_{Q_p}, T_{Q_n}/p^m), \]
the isomorphism \( \mathcal{L}_{Q_{\infty}} \) induces an isomorphism
\[ \mathcal{L}_{Q_{n,m}} : H^1_f(G_{Q_p}, T_{Q_n}/p^m) \sim R_{Q_n}/p^m, \]
and hence we obtain a homomorphism
\[ \mathcal{L}_{Q_{n,m}} : K_S(T_{Q_n}/p^m, F_{\text{can}}) \rightarrow \prod_{d \in \mathcal{N}_{m,n}} R_{Q_n}/p^m \otimes \mathbb{G}_d. \]
By construction, we have the following proposition.

Proposition 3.13. The diagram
\[
\begin{array}{c}
ES_1(T) \cap \prod_{K \in \Omega} M_{K_{\infty}} \\
\downarrow D^0_{m,n} \quad \downarrow \Phi \quad \downarrow D^0_{m,n} \\
K_S(T_{Q_n}/p^m, F_{\text{can}}) \longrightarrow \prod_{d \in \mathcal{N}_{m,n}} R_{Q_n}/p^m \otimes \mathbb{G}_d
\end{array}
\]
commutes.

Theorem 3.14. There is a Kolyvagin system \( \kappa_{\xi,m,n} \in K_S(T_{Q_n}/p^m, F_{\text{can}}) \) satisfying \( \delta(\kappa_{\xi,m,n}) = D^0_{m,n}((\xi_{K_{\infty}})_{K \in \Omega}) \).

Proof. Let \( z_\xi \in ES_1(T) \) be the Euler system defined in Proposition 3.8. Note that \( \mathcal{L}(e_\xi) = (\xi_{K_{\infty}})_{K \in \Omega} \). We define
\[ \kappa_{\xi,m,n} := \Phi \circ D^1_{m,n}(z_\xi). \]
Here \( \Phi : K_S(T, F_{\text{can}}) \rightarrow K_S(T, F_{\text{can}}) \) is the homomorphism associated with the isomorphism \( \mathcal{L}_{Q_{n,m}} : H^1_f(G_{Q_p}, T_{Q_n}/p^m) \sim R_{Q_n}/p^m \) (see §2.5). The commutative diagram (2) shows that \( \delta \circ \Phi = \mathcal{L}_{Q_{n,m}}. \) Hence Proposition 3.13 implies
\[
\delta(\kappa_{\xi,m,n}) = \delta \circ \Phi \circ D^1_{m,n}(z_\xi) = \mathcal{L}_{Q_{n,m}} \circ D^1_{m,n}(z_\xi) = D^0_{m,n}(z_\xi) = D^0_{m,n}((\xi_{K_{\infty}})_{K \in \Omega}).
\]

Remark 3.15. The Kolyvagin system \( \kappa_{\xi,m,n} \) constructed in Theorem 3.14 is a natural extension of a family of cohomology classes constructed by Kurihara in [6] (see also [5]). 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 \( \delta. \) 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

$$\tilde{\zeta}_{\infty} \Lambda_{\infty} = \text{char}_{\Lambda_{\infty}}(\text{Sel}(\mathbb{Q}_{\infty}, E[p^{\infty}]))^\vee.$$  

**Proposition 3.16.** The following are equivalent.

1. The Kolyvagin system $\kappa_{\xi,m,n} \in KS_0(T_{Q_n}/p^m, F_{cl})$ is a basis for some $m \geq 1$ and $n \geq 0$.

2. The Kolyvagin system $\kappa_{\xi,m,n} \in KS_0(T_{Q_n}/p^m, F_{cl})$ 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

$$KS_0(T_{Q_{\infty}}, F_{cl}) := \lim_{\longrightarrow \quad m,n} KS_0(T_{Q_n}/p^m, F_{cl}).$$

Then Theorem 2.20 and [17, Lemma 3.25] (see [19, Theorem 6.3]) show that the canonical map $KS_0(T_{Q_{\infty}}, F_{cl}) \rightarrow KS_0(T_{Q_n}/p^m, F_{cl})$ is surjective and the $\Lambda_{\infty}$-module $KS_0(T_{Q_{\infty}}, F_{cl})$ is free of rank 1. By construction,

$$\kappa_{\xi} := (\kappa_{\xi,m,n})_{m \geq 1, n \geq 0} \in KS_0(T_{Q_{\infty}}, F_{cl}).$$

Since $\delta: KS_0(E[p], F_{cl}) \rightarrow \prod_{d \in \mathcal{N}_{1,0}} \mathbb{F}_p \otimes \mathbb{Z} G_d$ 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 $\kappa_{\xi}$ is a basis. We have the canonical homomorphism

$$\delta_1: KS_0(T_{Q_{\infty}}, F_{cl}) \rightarrow \Lambda_{\infty}; (\kappa_{m,n})_{m \geq 1, n \geq 0} \mapsto \lim_{\longrightarrow \quad m,n} \delta(\kappa_{m,n}).$$

By Theorem 3.14, we have

$$\delta_1(\kappa_{\xi}) = \lim_{\longrightarrow \quad m,n} \delta((\tilde{\zeta}_{K_{\infty}})_{K \in \Omega})_{1,m,n} = \lim_{\longrightarrow \quad m,n} \tilde{\zeta}_{p^{m+1}} \mod p^m = \tilde{\zeta}_{\infty}.$$  

Let $\kappa \in KS_0(T_{Q_{\infty}}, F_{cl})$ be a basis and write $\kappa_{\xi} = a\kappa$ for some $a \in \Lambda_{\infty}$. Then, by Theorem 2.20 (see [19, Theorem 6.4]), we have

$$\tilde{\zeta}_{\infty} \Lambda_{\infty} = a\delta_1(\kappa) = a \cdot \text{char}_{\Lambda_{\infty}}(\text{Sel}(\mathbb{Q}_{\infty}, E[p^{\infty}]))^\vee.$$  

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

4. Main results

4.1. **Proof of Theorem 1.2.** First, let us discuss the relation between $\delta(\kappa_{\xi,1,0})d$ and $\tilde{\delta}_d$. As in §1, for each prime $\ell \in \mathcal{P}_{1,0}$, we fix a generator $h_{\ell} \in \text{Gal}(\mathbb{Q}(\mu_\ell)/\mathbb{Q})$, and it naturally induces the surjection

$$\overline{\log}_{h_{\ell}}: \text{Gal}(\mathbb{Q}(\mu_\ell)/\mathbb{Q}) \xrightarrow{\sim} \mathbb{Z}/(\ell - 1) \rightarrow \mathbb{F}_p; h_{\ell}^a \mapsto a \mod p.$$  

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

$$\tilde{\delta}_d := \sum_{\substack{a = 1 \\atop (a,d) = 1}}^{d} \frac{\text{Re}(a/d)}{\Omega_E} \cdot \prod_{\ell \mid d} \overline{\log}_{h_{\ell}}(\sigma_a).$$

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

$$e_d^{\nu(d)} \delta_0 = \sum_{\substack{a = 1 \\atop (a,d) = 1}}^{d} \frac{\text{Re}(a/d)}{\Omega_E} \cdot \prod_{\ell \mid d} \overline{\log}_{h_{\ell}}(\sigma_a^{e_d}) = 0.$$
Let \( \tilde{\theta}_d = \sum_{\sigma \in \text{Gal}(Q(d)/Q)} a_{\sigma} \sigma \) denote the image of \( \tilde{\theta}_{Q(d)} \) in \( Z_p[\text{Gal}(Q(d)/Q)] \) (see §3.1 for the definition of \( \tilde{\theta}_{Q(d)} \)). Assume for simplicity that the image of \( h_{\ell}^{(d)} \) is the fixed generator \( g_{\ell} \in \text{Gal}(Q(\ell)/Q) \). Recall that we have the surjection
\[
\sum_{\ell | d} \log g_{\ell} : \text{Gal}(Q(d)/Q) \xrightarrow{\sim} \mathbb{Z}/(\ell - 1) \longrightarrow \mathbb{F}_p.
\]
Since \( \sigma_a = \sigma_b \in \text{Gal}(Q(d)/Q) \) if \( \sigma_a^{(d)} = \sigma_b^{(d)} \), we see that
\[
e_{d}^{(d)} \delta_d = \sum_{\sigma \in \text{Gal}(Q(d)/Q)} \alpha_{\sigma} \prod_{\ell | d} \log g_{\ell}(\sigma).
\]
Since we have
\[
D_{d} \tilde{\theta}_d \mod p = (-1)^{\nu(d)} \left( \sum_{\sigma \in \text{Gal}(Q(d)/Q)} \alpha_{\sigma} \prod_{\ell | d} \log g_{\ell}(\sigma) \right) N_d
\]
by Lemma 3.11, we obtain the following lemma.

**Lemma 4.1.** For any integer \( d \in N_{1,0} \), the following are equivalent.

1. \( \tilde{\delta}_d \neq 0 \).
2. \( D_{d} \tilde{\theta}_d \mod p \neq 0 \).

**Lemma 4.2.** For any integer \( d \in N_{1,0} \), the following are equivalent.

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

**Proof.** Since any prime \( \ell \in \mathcal{P}_{1,0} \) is congruent to 1 modulo \( p \), the relation \( \delta(\kappa_{\xi,1,0}) = D_{1,0}^{(d)}(\xi_{\kappa_{\xi,1}})_{\kappa \in Q} \) in Theorem 3.14 shows that \( \delta(\kappa_{\xi,1,0}) \neq 0 \) if and only if \( D_{d} \tilde{\theta}_d \mod p \neq 0 \). 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 \( d \in N_{1,0} \) satisfying \( \tilde{\delta}_d \neq 0 \) if and only if the Iwasawa main conjecture for \( E/Q \) holds true.

**Proof.** This corollary follows from Proposition 3.16 and Lemma 4.2. \( \square \)

4.2. **Proof of Theorem 1.5.** In this subsection, we give a proof of Theorem 1.5. Recall that an integer \( d \in N_{1,0} \) is \( \delta \)-minimal if \( \tilde{\delta}_d \neq 0 \) and \( \tilde{\delta}_e = 0 \) for any positive proper divisor \( e \) of \( d \). Note that the existence of a \( \delta \)-minimal integer implies that the Kolyvagin system \( \kappa_{\xi,1,0} \) is a basis of \( \text{KS}_0(E[p], F_d) \) by Proposition 3.16 and Corollary 4.3.

**Lemma 4.4.** Let \( d \in N_{1,0} \) be an integer. Then the following are equivalent.

1. \( \tilde{\delta}_d \neq 0 \).
2. \( H_{F_0(\ell)}^{1}(G_Q, E[p]) = 0 \).

**Proof.** By Theorem 2.20, we have
\[
\mathbb{F}_p \cdot \delta(\kappa_{\xi,1,0})_{d} = \text{Fitt}^{(d)}_{\mathbb{F}_p}(H_{F_0(\ell)}^{1}(G_Q, E[p])).
\]
Hence this lemma follows from Lemma 4.2. \( \square \)

**Remark 4.5.** The injectivity of the homomorphism (1) (proved by Kurihara) follows immediately from Lemma 4.4. In fact, we have
\[
\ker \left( \text{Sel}(Q, E[p]) \xrightarrow{(1)} \bigoplus_{\ell | d} \mathcal{E}(Q_{\ell}) \otimes \mathbb{F}_p \right) = H_{F_0(\ell)}^{1}(G_Q, E[p]) \subset H_{F_0(\ell)}^{1}(G_Q, E[p]).
\]
For any integer \( d \in N_{1,0} \), we set
\[
\lambda(d) := \dim_{\mathbb{F}_p}(H_{F_0(\ell)}^{1}(G_Q, E[p]))
\]
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 \(H^1_{(\mathcal{F}_d)}(G_Q, E[p]) \neq H^1_{(\mathcal{F}_{d \ell})}(G_Q, E[p])\), then \(\lambda(d) = \lambda(d) - 1\).
2. If \(H^1_{(\mathcal{F}_d)}(G_Q, E[p]) = H^1_{(\mathcal{F}_{d \ell})}(G_Q, E[p])\), then \(\lambda(d) \leq \lambda(d)\).

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

Proof. If \(H^1_{(\mathcal{F}_d)}(G_Q, E[p]) \neq H^1_{(\mathcal{F}_{d \ell})}(G_Q, E[p])\), then the localization map

\[ H^1_{(\mathcal{F}_d)}(G_Q, E[p]) \to H^1_{(\mathcal{F}_{d \ell})}(G_Q, E[p]) \]

is non-zero. Since \(\mathcal{F}_d(d)^* = \mathcal{F}_d(d)\), claim (1) follows from [7, Lemma 4.1.7 (iv)]. Claim (2) is trivial since

\[ H^1_{(\mathcal{F}_d)}(G_Q, E[p]) = H^1_{(\mathcal{F}_{d \ell})}(G_Q, E[p]) \supset H^1_{(\mathcal{F}_{d \ell})}(G_Q, E[p]). \]

\(\square\)

Proposition 4.7. Let \(d \in \mathcal{N}_{1,0}\) be an integer satisfying \(H^1_{(\mathcal{F}_d)}(G_Q, E[p]) = 0\). 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 \(d = 1\). Hence we may assume that \(\lambda(1) > 0\). If \(H^1_{(\mathcal{F}_d)}(G_Q, E[p]) = H^1_{(\mathcal{F}_{d \ell})}(G_Q, E[p])\) for any prime \(\ell \mid d\), then

\[ H^1_{(\mathcal{F}_d)}(G_Q, E[p]) = \bigcap_{\ell \mid d} H^1_{(\mathcal{F}_{d \ell})}(G_Q, E[p]) \]

\[ = H^1_{(\mathcal{F}_{d \ell})}(G_Q, E[p]) \]

\[ < H^1_{(\mathcal{F}_{d \ell})}(G_Q, E[p]) \]

\[ = 0. \]

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

\[ H^1_{(\mathcal{F}_d)}(G_Q, E[p]) \neq H^1_{(\mathcal{F}_{d \ell_1})}(G_Q, E[p]). \]

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

\[ H^1_{(\mathcal{F}_{d / \ell_1})}(G_Q, E[p]) \subset H^1_{(\mathcal{F}_{d \ell_1})}(G_Q, E[p]) = 0, \]

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

\[ H^1_{(\mathcal{F}_{d / \ell_2})}(G_Q, E[p]) \neq H^1_{(\mathcal{F}_{d / \ell_1})}(G_Q, E[p]). \]

Then \(\lambda(\ell_1 \ell_2) = \lambda(1) - 1\) by Lemma 4.6. By repeating this argument, we obtain a sequence \(\ell_1, \ldots, \ell_{M(1)}\) of prime divisors of \(d\) such that \(\lambda(\ell_i) = \lambda(1) - 1\) 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 \(d\). \(\square\)

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

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

Proof. Let \(d \in \mathcal{N}_{1,0}\) be a \(\delta\)-minimal integer. Then \(H^1_{(\mathcal{F}_d)}(G_Q, E[p]) = 0\) 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 4.2 implies \(\delta_e \neq 0\), and we have \(d = e\) by the definition of the \(\delta\)-minimality. Therefore, we obtain \(\nu(d) = \nu(e) = \lambda(1)\). \(\square\)

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 ([6, 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 $\mathcal{F}_{cl}$ is self-dual, and hence one can say that the self-duality of the Selmer structure $\mathcal{F}_{cl}$ is one of the most important ingredients in order to prove Theorem 1.5.

Let $\kappa_{\xi,1,0} = (\kappa_{d,t}, t_{d,0})$ be the Kolyvagin system constructed in Theorem 3.14. By using the fixed generator $g_{t_i} \in G_t$, we regard $G_t$ as $\mathbb{Z}/\#G_t$, and hence one can regard $\kappa_{d,t} \in H^1_{\mathcal{F}_{cl}(d)}(G_{\mathbb{Q}}, E[p])$. As discussed by Kurihara in [6, Theorem 3(2)], by using Theorem 4.8, one can construct a basis of the $p$-Selmer group $\text{Sel}(\mathbb{Q}, E[p])$ from the Kolyvagin system $\kappa_{\xi,1,0}$.

**Corollary 4.10.** For any $\delta$-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 $\text{Sel}(\mathbb{Q}, E[p])$.

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

$$0 \longrightarrow H^1_{\mathcal{F}_{cl}(d)}(G_{\mathbb{Q}}, E[p]) \longrightarrow \text{Sel}(\mathbb{Q}, E[p]) \longrightarrow \bigoplus_{\ell_i \mid d} H^1_{ur}(G_{\mathbb{Q}}, E[p])$$

$$\longrightarrow H^1_{\mathcal{F}_{cl}(d)}(G_{\mathbb{Q}}, E[p])^\vee \longrightarrow \text{Sel}(\mathbb{Q}, E[p])^\vee \longrightarrow 0.$$

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

$$\bigoplus_{\ell_i \mid d} \phi_{\ell_i} : \text{Sel}(\mathbb{Q}, E[p]) \xrightarrow{\sim} \bigoplus_{\ell_i \mid d} H^1_{ur}(G_{\mathbb{Q}}, E[p]) \xrightarrow{\sim} \mathbb{F}_p^t.$$ 

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

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

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

**Appendix A. Remarks on $p = 3$**

The assumption that $p > 3$ is one of the standard hypotheses of the theory of Kolyvagin systems (see the hypothesis (H.4) in the page 27 of [7]). In this appendix, we explain that Theorem 2.20 and Proposition 2.24 are valid even when $p = 3$. We note that, in the theory of Stark systems, the assumption that $p > 3$ is not needed (see [17, Hypothesis 3.12]). Hence one can use all results in [17] even if $p = 3$.

In this appendix, we consider the following situation.

- $R$ is a zero-dimensional Gorenstein local ring with finite residue field $\mathbb{F}$ such that $p^nR = 0$ and $\text{char}(\mathbb{F}) = 3$.
- $T$ is a free $R$-module of finite rank with a continuous $G_{\mathbb{Q}}$-action satisfying the following:
  - $T \otimes_R \mathbb{F}$ is an irreducible $G_{\mathbb{Q}}$-module.
  - There is a rational prime $\ell \notin S_{\text{ram}}(T) \cup \{3\}$ such that $T/(\mathbb{F}_\ell - 1)T \cong R$ and $\ell \equiv 1 \mod 3^m$.
  - $H^1(\text{Gal}(\mathbb{Q}(\mu_{3^n}, T)/\mathbb{Q}), T \otimes_R \mathbb{F}) = 0$. Here $\mathbb{Q}(\mu_{3^n}, T)$ is the field corresponding to the kernel of $G_{\mathbb{Q}(\mu_{3^n})} \longrightarrow \text{Aut}(T)$.
  - $T$ is residually self-dual, i.e., there is a $G_{\mathbb{Q}}$-isomorphism $T \otimes_R \mathbb{F} \cong (T \otimes_R \mathbb{F})^\vee(1)$.

We put

$\overline{T} := T \otimes_R \mathbb{F}$,
\( \mathcal{P} := \{ \ell \notin S_{\text{ram}}(T) \cup \{ 3 \} \mid T/(F_{1\ell} - 1)T \cong R, \ell \equiv 1 \mod 3^n \} \),

- \( \mathcal{N} \) denotes the set of square-free products in \( \mathcal{P} \).

A.1. **Application of the Chebotarev density theorem.** As mentioned in the beginning of [7, §3.6], in the theory of Kolyvagin systems, the assumption that \( p > 3 \) is only used for choosing useful primes. In this subsection, we prove a slightly weaker result than [7, Proposition 3.6.1] when \( p = 3 \).

**Lemma A.1.** Let \( a > 0 \) be an integer. Let \( G \) be a group and \( \varphi_1, \varphi_2, \varphi_3, \varphi_4 \in \text{Hom}(G, \mathbb{F}_3^a) \setminus \{0\} \). Suppose that

\[
\dim_{\mathbb{F}_3} (\mathbb{F}_3\varphi_1 + \mathbb{F}_3\varphi_2 + \mathbb{F}_3\varphi_3 + \mathbb{F}_3\varphi_4) \geq 3.
\]

Then, for any \( g_1, g_2, g_3, g_4 \in G \), we have

\[
\bigcup_{i=1}^{4} g_i \ker(\varphi_i) \neq G.
\]

**Proof.** Put \( \varphi_{i,j} := \text{pr}_j \circ \varphi_i : G \twoheadrightarrow \mathbb{F}_3 \). Then

\[
\bigcup_{i=1}^{4} g_i \ker(\varphi_i) = \bigcup_{i=1}^{4} \bigcap_{(j_1, j_2, j_3, j_4) \in \{1,\ldots,a\}^4} g_i \ker(\varphi_{i,j_i})
\]

\[
\subseteq \bigcap_{(j_1, j_2, j_3, j_4) \in \{1,\ldots,a\}^4} \bigcup_{i=1}^{4} g_i \ker(\varphi_{i,j_i}).
\]

Hence we may assume that \( a = 1 \).

Suppose that \( \dim_{\mathbb{F}_3} (\mathbb{F}_3\varphi_1 + \mathbb{F}_3\varphi_2 + \mathbb{F}_3\varphi_3 + \mathbb{F}_3\varphi_4) = 4 \). Since the kernel of the surjection

\[
G \twoheadrightarrow \mathbb{F}_3^4; \; g \mapsto (\varphi_1(g), \varphi_2(g), \varphi_3(g), \varphi_4(g))
\]

is contained in \( \ker(\varphi_i) \) for any \( 1 \leq i \leq 4 \), we may assume that \( G = \mathbb{F}_3^4 \) and \( \varphi_i = \text{pr}_i \) for each \( 1 \leq i \leq 4 \). In this case, an explicit calculation shows that

\[
G \setminus (g_1 \ker(\varphi_1) \cup g_2 \ker(\varphi_2) \cup g_3 \ker(\varphi_3) \cup g_4 \ker(\varphi_4)) = \{(h_1, h_2, h_3, h_4) \in \mathbb{F}_3^4 \mid \text{pr}_i(g_i) \neq h_i \text{ for any } 1 \leq i \leq 4 \} \neq \emptyset.
\]

Suppose that \( \dim_{\mathbb{F}_3} (\mathbb{F}_3\varphi_1 + \mathbb{F}_3\varphi_2 + \mathbb{F}_3\varphi_3 + \mathbb{F}_3\varphi_4) = 3 \). We may then assume that \( \varphi_4 \in \mathbb{F}_3\varphi_1 + \mathbb{F}_3\varphi_2 + \mathbb{F}_3\varphi_3 \). Moreover, since the kernel of the surjection

\[
G \twoheadrightarrow \mathbb{F}_3^3; \; g \mapsto (\varphi_1(g), \varphi_2(g), \varphi_3(g))
\]

is contained in \( \ker(\varphi_i) \) for any \( 1 \leq i \leq 4 \), we may also assume that \( G = \mathbb{F}_3^3 \) and \( \varphi_1 = \varphi_2 = \varphi_3 = \text{pr}_i \) for each \( 1 \leq i \leq 3 \). Then we have

\[
G \setminus (g_1 \ker(\varphi_1) \cup g_2 \ker(\varphi_2) \cup g_3 \ker(\varphi_3)) = \{(h_1, h_2, h_3) \in \mathbb{F}_3^3 \mid \text{pr}_i(g_i) \neq h_i \text{ for any } 1 \leq i \leq 3 \}.
\]

Since the set \( -g_4 + \{(h_1, h_2, h_3) \in \mathbb{F}_3^3 \mid \text{pr}_i(g_i) \neq h_i \text{ for any } 1 \leq i \leq 3 \} \) contains a basis of \( \mathbb{F}_3^3 \) and \( \varphi_4 = 0 \), we have

\[
\{(h_1, h_2, h_3) \in \mathbb{F}_3^3 \mid \text{pr}_i(g_i) \neq h_i \text{ for any } 1 \leq i \leq 3 \} \not\subseteq g_4 \ker(\varphi_4),
\]

which completes the proof. \( \square \)

The following is the result which corresponds to [7, Proposition 3.6.1].

**Lemma A.2.** Let \( c_1, c_2, c_3, c_4 \in H^1(G_{\mathbb{Q}}, T) \) be non-zero elements. Suppose that

\[
\dim_{\mathbb{F}_3} (\mathbb{F}_3c_1 + \mathbb{F}_3c_2 + \mathbb{F}_3c_3 + \mathbb{F}_3c_4) \geq 3.
\]

Then there are infinitely many primes \( \ell \in \mathcal{P} \) satisfying \( \text{loc}_\ell(c_i) \neq 0 \) for any \( 1 \leq i \leq 4 \). Here, \( \text{loc}_\ell : H^1(G_{\mathbb{Q}}, T) \twoheadrightarrow H^1(G_{\mathbb{Q}}, T) \) denotes the localization map at \( \ell \).
Corollary A.5. The image of \( \text{loc}(c_1), \text{loc}(c_2), \text{loc}(c_3), \) and \( \text{loc}(c_4) \) are zero for all but finitely many primes \( \ell \in \mathcal{P} \) since \( H^1_{\text{ur}}(G_{\mathbb{Q}}, \mathcal{T}) \cong \mathbb{F}_3. \)

Remark A.4. Lemma A.2 is only used for proving Lemma A.10.

Proof. The proof of this lemma is based on that of [7, Proposition 3.6.1]. Fix an element \( \tau \in G_{\mathbb{Q}(\mu_{p^n})} \) such that \( T/(\tau - 1)T \cong R. \) Put \( F := \mathbb{Q}(\mu_{p^n}, T). \) Since we assume that
\[
H^1(\text{Gal}(F/\mathbb{Q}), \mathcal{T}) = 0,
\]
the restriction map induces an injection
\[
H^1(G_{\mathbb{Q}}, \mathcal{T}) \hookrightarrow H^1(G_F, \mathcal{T})^{G_0} = \text{Hom}(G_F, \mathcal{T})^{G_0}.
\]
Since \( \mathcal{T} \) is an irreducible \( G_{\mathbb{Q}} \)-module, the map
\[
\text{Hom}(G_F, \mathcal{T})^{G_0} \hookrightarrow \text{Hom}(G_F, \mathcal{T}/(\tau - 1)\mathcal{T})
\]
is injective. Let \( \tau_i \in \text{Hom}(G_F, \mathcal{T}/(\tau - 1)\mathcal{T}) \) denote the image of \( c_i \) under the injection (6). We also put
\[
H_i := \{ g \in G_F \mid c_i(\tau g) = 0 \text{ in } \mathcal{T}/(\tau - 1)\mathcal{T} \}.
\]
As mentioned in the proof of [7, Proposition 3.6.1], the value \( c_i(\tau g) \mod (\tau - 1)\mathcal{T} \) is well-defined since \( g \in G_F \) acts trivially on \( \mathcal{T} \). Note that \( \tau_i \) is surjective since \( \tau_i \neq 0 \).

Hence we see that there is an element \( g_i \in G_F \) such that \( H_i = g_i \ker(\tau_i). \) Since the map (6) is injective, we have \( \dim_{G_0}(F_3\mathcal{T}_1 + F_3\mathcal{T}_2 + F_3\mathcal{T}_3 + F_3\mathcal{T}_4) \geq 3 \) by assumption. Hence Lemma A.1 shows that there is an element \( g \in G_F \setminus (H_1 \cup H_2 \cup H_3 \cup H_4). \)

For each \( 1 \leq i \leq 4 \), we put \( F_i := F_\ell^{\ker(c_i)}. \) Note that \( F/\mathbb{Q} \) is a Galois extension since \( c_i \in \text{Hom}(G_F, \mathcal{T})^{G_0}. \) Let \( S \) be the set of rational primes whose Frobenius conjugacy class in \( \text{Gal}(F_1F_2F_3F_4/\mathbb{Q}) \) is the class of \( \tau g. \) Note that for any prime \( \ell \in S, \) we have
\[
H^1_{\text{ur}}(G_{\mathbb{Q}_\ell}, \mathcal{T}) \cong \mathcal{T}/(\ell \ell - 1)\mathcal{T} = \mathcal{T}/(\tau - 1)\mathcal{T} \cong F.
\]

Hence \( S \) is an infinite set and \( \text{loc}(c_i) \neq 0 \) for any \( 1 \leq i \leq 4 \) and \( \ell \in S. \) Since the image of \( \tau g \) in \( \text{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q}) \) is trivial, we have \( \ell \equiv 1 \mod p^n, \) and so \( S \subset \mathcal{P}. \)

Corollary A.5. Let \( c_1, c_2, c_3 \in H^1(G_{\mathbb{Q}}, \mathcal{T}) \) be non-zero elements. Then there are infinitely many primes \( \ell \in \mathcal{P} \) satisfying \( \text{loc}(c_i) \neq 0 \) for any \( 1 \leq i \leq 3. \)

Proof. Note that \( \dim_{G_0}(H^1(G_{\mathbb{Q}}, \mathcal{T})) = \infty. \) When \( \dim_{G_0}(F_3\mathcal{T}_1 + F_3\mathcal{T}_2 + F_3\mathcal{T}_3) \geq 2, \) there exists an element \( c \in H^1(G_{\mathbb{Q}}, \mathcal{T}) \) satisfying
\[
\dim_{G_0}(F_3c_1 + F_3c_2 + F_3c_3 + F_3c_4) \geq 3.
\]

Hence this corollary follows from Lemma A.2. When \( \dim_{G_0}(F_3c_1 + F_3c_2 + F_3c_3) = 1, \) we may assume that \( c_1 = c_2 = c_3. \) Then the same argument shows that there are infinitely many primes \( \ell \in \mathcal{P} \) satisfying \( \text{loc}(c_i) \neq 0 \) for any \( 1 \leq i \leq 3. \)

A.2. Connectedness of the graph \( \Delta^0. \) Let \( \mathcal{G} \) be a Selmer structure on \( T. \) We denote by \( \overline{\mathcal{G}} \) the Selmer structure on \( \mathcal{T} \) induced by \( \mathcal{G}, \) that is,
\[
H^1_{\text{ur}}(G_{\mathbb{Q}}, \mathcal{T}) := \text{im} \left( H^1(\mathcal{G}_{\mathbb{Q}}, T) \longrightarrow H^1(G_{\mathbb{Q}}, \mathcal{T}) \right)
\]
for any rational prime \( \ell. \) Since we assume that \( \mathcal{T} \) is self-dual, one can regard \( \overline{\mathcal{G}} \) as a Selmer structure on \( \mathcal{T} \). Suppose that

\- \( \mathcal{G} \) is cartesian and residually self-dual (i.e., \( \overline{\mathcal{G}} = \overline{\mathcal{G}}^* \)).

Note that residual self-duality implies that \( \chi(\mathcal{G}) = 0. \) In this subsection, we fix a rational prime \( r \) such that
\[ \dim_{\mathbb{F}}(H^1(G_{\mathbb{Q}}, T)/H^1_{\mathbb{Q}}(G_{\mathbb{Q}}, T)) = 1, \]
\[ H^1(G_{\mathbb{Q}}, T) \to H^1(G_{\mathbb{Q}}, F) \text{ is surjective.} \]

We put \( F := G^r \).

**Remark A.6.** When \( T = \text{Ind}_{G_{\mathbb{Q},0}}^G(E[p^n]) \), \( G = F_{\text{cl}} \) and \( r = 3 \), all assumptions in this appendix are satisfied and we have \( F = F_{\text{can}} \).

We set \( \mathcal{P}(\mathcal{G}, r) = \mathcal{P} \setminus (\mathcal{S}(\mathcal{G}) \cup \{r\}) \) and \( \mathcal{N}(\mathcal{G}, r) \) denotes the set of square products in \( \mathcal{P}(\mathcal{G}, r) \). For notational simplicity, we also write \( F \) for the Selmer structure on \( T \) induced by \( F \). For any square-free integer \( d \), we define
\[
\lambda(d) := \dim_{\mathbb{F}}(H^1_{\mathcal{F}(d)}(G_{\mathbb{Q}}, T)),
\]
\[
\lambda^*(d) := \dim_{\mathbb{F}}(H^1_{\mathcal{F}^*(d)}(G_{\mathbb{Q}}, T)).
\]

Following [7, Definition 4.3.6], we define the graph \( X^0 := X^0(F) \) as follows.

- The vertices of \( X^0 \) are integers \( d \in \mathcal{N}(\mathcal{G}, r) \) with \( \lambda^*(d) = 0 \).
- For any vertices \( d, d\ell \in X^0 \) with \( \ell \in \mathcal{P}(\mathcal{G}, r) \), we join \( d \) and \( d\ell \) by an edge in \( X^0 \) if and only if \( H^1_{\mathcal{F}(d)}(G_{\mathbb{Q}}, T) \neq H^1_{\mathcal{F}(d\ell)}(G_{\mathbb{Q}}, T) \).

In this subsection, we prove the connectedness of the graph \( X^0 \) which is one of the most important facts in the theory of Kolyvagin systems.

**Lemma A.7.** The Selmer structure \( F \) is cartesian and \( \chi(F) = 1 \).

**Proof.** Since \( H^1(G_{\mathbb{Q}}, T) \to H^1(G_{\mathbb{Q}}, F) \) is surjective and \( G \) is cartesian, we see that \( F = G^r \) is cartesian. Applying Theorem 2.1 with \( \mathcal{F}_1 = \mathcal{G} \) and \( \mathcal{F}_2 = F \), we obtain
\[
\chi(F) = \chi(G) + \dim_{\mathbb{F}}(H^1(G_{\mathbb{Q}}, T)/H^1_{\mathbb{Q}}(G_{\mathbb{Q}}, T)) = 1.
\]
\( \square \)

The following lemma is an applications of Theorem 2.1.

**Lemma A.8.** Let \( d \in \mathcal{N}(\mathcal{G}, r) \) be an integer. Then the following claims are valid.

1. \( \lambda(d) = \lambda^*(d) + 1 \).
2. \( |\lambda(d) - \lambda(d\ell)| \leq 1 \) for any prime \( \ell \in \mathcal{P}(\mathcal{G}, r) \) with \( \ell \not| d \).
3. \( |\lambda^*(d) - \lambda^*(d\ell)| \leq 1 \) for any prime \( \ell \in \mathcal{P}(\mathcal{G}, r) \) with \( \ell \not| d \).
4. If \( H^1_{\mathcal{F}(d)}(G_{\mathbb{Q}}, T) \neq H^1_{\mathcal{F}(d\ell)}(G_{\mathbb{Q}}, T) \), then \( \lambda^*(d\ell) \leq \lambda^*(d) \).
5. If \( H^1_{\mathcal{F}^*(d)}(G_{\mathbb{Q}}, T) \neq H^1_{\mathcal{F}^*(d\ell)}(G_{\mathbb{Q}}, T) \), then \( \lambda(d\ell) = \lambda(d) - 1 \) and \( \lambda^*(d\ell) = \lambda^*(d) - 1 \).

In particular, \( \nu(d) \geq \lambda^*(1) \) for any integer \( d \in \mathcal{N}(\mathcal{G}, r) \) with \( \lambda^*(d) = 0 \).

**Proof.** Claim (1) follows from [7, Proposition 4.1.4] and the fact that \( \lambda(1) - \lambda^*(1) = \chi(F) = 1 \). Claims (2) and (3) follow from [7, Lemma 4.1.7(i)].

Suppose that \( H^1_{\mathcal{F}(d)}(G_{\mathbb{Q}}, T) \neq H^1_{\mathcal{F}(d\ell)}(G_{\mathbb{Q}}, T) \). Since \( H^1_{\mathcal{F}^*(d)}(G_{\mathbb{Q}}, T) \cong \mathbb{F} \), applying Theorem 2.1 with \( \mathcal{F}_1 = \mathcal{G}(d) \) and \( \mathcal{F}_2 = F(d) \), we see that \( H^1_{\mathcal{F}^*(d)}(G_{\mathbb{Q}}, T) = H^1_{\mathcal{F}^*(d\ell)}(G_{\mathbb{Q}}, T) \), which implies claim (4).

Since \( \mathcal{F}^* \subset \mathcal{F} \) by definition, if \( H^1_{\mathcal{F}^*(d)}(G_{\mathbb{Q}}, T) \neq H^1_{\mathcal{F}^*(d\ell)}(G_{\mathbb{Q}}, T) \), then we have \( H^1_{\mathcal{F}(d)}(G_{\mathbb{Q}}, T) \neq H^1_{\mathcal{F}(d\ell)}(G_{\mathbb{Q}}, T) \). Hence claim (5) follows from [7, Lemma 4.1.7(iv)].
\( \square \)

**Lemma A.9.** For any vertices \( d, d\ell \in X^0 \) with \( \ell \in \mathcal{P}(\mathcal{G}, r) \), there is a path in \( X^0 \) from \( d \) to \( d\ell \).
Proof. This lemma is proved by Mazur and Rubin in [7, Lemma 4.3.9]. Note that [7, Proposition 3.6.1] is used in the proof of [7, Lemma 4.3.9]. However, exactly the same argument as in [7, Lemma 4.3.9] works even if we use Corollary A.5 instead of [7, Proposition 3.6.1]. □

Lemma A.10. For each integer 1 ≤ i ≤ 2, let d_i ∈ X^0 and e_i ∈ P(G, r) with e_i | r, d_i. Suppose that ν(d_1) = ν(d_2) = λ^*(1) and e_1 ≠ e_2. Then there exists a prime q ∈ P(G, r) with q | d_1d_2 such that there is a path in X^0 from d_1 to d_1q/ℓ_i for each integer 1 ≤ i ≤ 2.

Proof. Let 1 ≤ i ≤ 2 and put e_i = d_i/ℓ_i. Since ν(e_i) = λ^*(1) − 1, we have λ(e_i) = 2 and λ^*(e_i) = 1 by Lemma A.8. By definition, we have

H_{F(e_i)}^1(G_Q, T) = H_{F(e_i)}^1(G_Q, T).$$

Moreover, since λ^*(d_i) = 0, we also have

H_{F(e_i)}^1(G_Q, T) ∩ H_{F(d_i)}^1(G_Q, T) ⊂ H_{F(e_i)}^1(G_Q, T) = 0.

Since λ(e_i) = 2 and λ(d_i) = λ^*(e_i) = 1, we obtain a decomposition

H_{F(e_i)}^1(G_Q, T) = H_{F(d_i)}^1(G_Q, T) ⊕ H_{F(e_i)}^1(G_Q, T).

Take non-zero elements c_1^{(i)} ∈ H_{F(e_i)}^1(G_Q, T) and c_2^{(i)} ∈ H_{F(d_i)}^1(G_Q, T). By definition, we have H_{F(e_i)}^1(G_Q, T) ∩ ker(loc_r) = H_{F(e_i)}^1(G_Q, T). Hence we see that loc_r(c_1^{(i)}) ≠ 0 ≠ loc_r(c_2^{(i)}) and loc_r(c_2^{(i)}) = 0 = loc_r(c_2^{(2)}).

Let us show that there is a prime q ∈ P(G, r) such that loc_q(c_2^{(1)}) ≠ 0 for any i, j ∈ {1, 2}. If c_2^{(1)} ∉ H_{F(d_i)}^1(G_Q, T), then this claim follows from Lemma A.2. Suppose that c_2^{(1)} ∈ H_{F(d_i)}^1(G_Q, T), that is, c_2^{(1)} = ac_1^{(1)} + bc_2^{(1)} for some a, b ∈ F. Then

0 = loc_q(c_2^{(1)}) = loc_q(ac_1^{(1)}) + loc_q(bc_2^{(1)}) = loc_q(ac_1^{(1)}).

Since loc_q(c_1^{(1)}) ≠ 0, we may assume that c_2^{(1)} = c_2^{(2)}. Then Corollary A.5 shows that there is a prime q ∈ P(G, r) such that loc_q(c_2^{(1)}) ≠ 0 for any i, j ∈ {1, 2}.

Let us prove that q is a desired prime. Lemma A.8 and the fact that loc_q(c_2^{(1)}) ≠ 0 imply λ^*(d_1q) ≤ λ^*(d_1) = 0, that is, d_1q ∈ X^0. Since loc_q(c_2^{(1)}) ≠ 0, we have

H_{F(e_i)}^1(G_Q, T) ≠ H_{F(e_i)}^1(G_Q, T).

Hence Lemma A.8 shows that λ^*(e_iq) = λ^*(e_i) − 1 = 0, that is, e_iq ∈ X^0. Since loc_q(c_2^{(1)}) ≠ 0, we have

H_{F(e_i)}^1(G_Q, T) ≠ H_{F(e_i)}^1(G_Q, T).

Hence Lemma A.8 shows that λ^*(e_iq) = λ^*(e_i) − 1 = 0, that is, e_iq ∈ X^0. Since loc_q(c_2^{(1)}) ≠ 0, we have

ν(d_1) = ν(d_2) = λ^*(1), there is a path in X^0 from d_1 to d_2.

□

Corollary A.11 ([7, Proposition 4.3.11]). For any vertices d_1, d_2 ∈ X^0 satisfying ν(d_1) = ν(d_2) = λ^*(1), there is a path in X^0 from d_1 to d_2.

Proof. Put d := gcd(d_1, d_2). Let us show this corollary by induction on λ^*(1) − ν(d).

When ν(d) = λ^*(1), then d_1 = d_2, and there is nothing to prove. When ν(d) < λ^*(1), there are primes ℓ_1, ℓ_2 ∈ P(G, r) with ℓ_1 | d_1/d and ℓ_2 | d_2/d. Then by Lemma A.10, we have a prime q ∈ P(G, r) with q | d_1d_2 such that d_1q/ℓ_1, d_2q/ℓ_2 ∈ X^0 and that there is a path in X^0 from d_1 to d_1q/ℓ_1 for any 1 ≤ i ≤ 2. Since ν(d) < ν(gcd(d_1q/ℓ_1, d_2q/ℓ_2)), the induction hypothesis shows that there is a path in X^0 from d_1q/ℓ_1 to d_2q/ℓ_2, and hence we obtain a path in X^0 from d_1 to d_2. □

Lemma A.12. For any vertex d ∈ X^0 with ν(d) > λ^*(1), there is a vertex e ∈ X^0 with ν(e) < ν(d) such that there is a path in X^0 from d to e.
By construction, the following diagram commutes:

\[ \begin{array}{ccc}
\text{Reg}_1 : SS_1(T,F) & \longrightarrow & X_d(T,F) \\
\downarrow & & \downarrow (-1)^{(e\ell)}\Pi_d \\
KS_1(T,F) & \longrightarrow & H^1_{\mathcal{F}(d)}(G_{\mathbb{Q}}, T) \otimes \mathbb{Z}G_d
\end{array} \]

Since \( \lambda^*(1) \leq \nu(d) \) for any vertex \( d \in X^0 \), Corollary A.11 and Lemma A.12 imply the following

**Theorem A.13** ([7, Theorem 4.3.12]). The graph \( \mathcal{X}^0 \) is connected.

### 3.13 Kolyvagin systems

We use the same notations as in the previous subsection. In this subsection, we prove Theorem 2.20 and Proposition 2.24 when \( p = 3 \).

**Definition A.14.** Let \( KS_1(T,F) \) denote the module of Kolyvagin systems of rank 1 (for \( F \)), that is, the set of elements in \( \prod_{d \in \mathcal{N}(G,r)} H^1_{\mathcal{F}(d)}(G_{\mathbb{Q}}, T) \otimes \mathbb{Z}G_d \) satisfying the finite-singular relations.

**Proposition A.15.** For any integer \( d \in \mathcal{N}(G,r) \) with \( \lambda^*(d) = 0 \), the canonical projection

\[ KS_1(T,F) \longrightarrow H^1_{\mathcal{F}(d)}(G_{\mathbb{Q}}, T) \otimes \mathbb{Z}G_d \]

is injective.

**Proof.** Let \( \mathfrak{m}_R \) denote the maximal ideal of \( R \). Since \( F \) is cartesian, so is \( F(d) \) for any integer \( d \in \mathcal{N}(G,r) \) (see [17, Corollary 3.18]). Hence, by [17, Lemma 3.13], the canonical injection \( T \mapsto R \) induces an isomorphism \( H^1_{\mathcal{F}(d)}(G_{\mathbb{Q}}, T) \cong H^1_{\mathcal{F}(d)}(G_{\mathbb{Q}}, T)[\mathfrak{m}_R] \) for any integer \( d \in \mathcal{N}(G,r) \). Therefore, we may assume that \( R = \mathbb{F} \) and \( T = T \) since \( KS_1(T,F) \Rightarrow KS_1(T,F)[\mathfrak{m}_R] \).

Take an integer \( d \in \mathcal{N}(G,r) \) with \( \lambda^*(d) = 0 \). Let \( (\kappa_e)_{e \in \mathcal{N}(G,r)} \in KS_1(T,F) \) be a Kolyvagin system satisfying \( \kappa_d = 0 \). Let us show \( \kappa_e = 0 \) by induction on \( \lambda^*(e) \). When \( \lambda^*(e) = 0 \), there is a path in \( X^0 \) from \( d \) to \( e \) by Theorem A.13. Hence the finite-singular relation and [7, Lemma 4.3.8] imply \( \kappa_e = 0 \). Suppose that \( \lambda^*(e) > 0 \), and take a non-zero element \( e \in H^1_{\mathcal{F}(e)}(G_{\mathbb{Q}}, E[p]) \). If \( \kappa_e \neq 0 \), then by Corollary A.5, there is a prime \( \ell \in \mathcal{P}(G,r) \) with \( \ell \nmid e \) such that \( \text{loc}_{\ell}(\kappa_e) \neq 0 \) and \( \text{loc}_{\ell}(e) \neq 0 \). Since \( \text{loc}_{\ell}(e) \neq 0 \), we have \( \lambda^*(e\ell) = \lambda^*(e) - 1 \) by Lemma A.8. Hence the induction hypothesis and the finite-singular relation imply

\[ 0 \neq \varphi_{\ell}^e(\kappa_e) = v_{\ell}(\kappa_{e\ell}) = 0. \]

Therefore, we conclude that \( \kappa_e = 0 \).

As explained in §2.5, for any integer \( d \in \mathcal{N}(G,r) \), the exact sequence

\[ 0 \longrightarrow H^1_{\mathcal{F}(d)}(G_{\mathbb{Q}}, T) \longrightarrow H^1_{\mathcal{F}d}(G_{\mathbb{Q}}, T) \longrightarrow \bigoplus_{\ell \mid d} H^1_{\mathcal{F}\ell}(G_{\mathbb{Q}}, T) \]

induces a natural homomorphism \( \Pi_d : X^1_d(T,F) \longrightarrow H^1_{\mathcal{F}(d)}(G_{\mathbb{Q}}, T) \otimes \mathbb{Z}G_d \), and we obtain

\[ \text{Reg}_1 : SS_1(T,F) \longrightarrow KS_1(T,F). \]

By construction, the following diagram commutes:

\[ \begin{array}{ccc}
SS_1(T,F) & \longrightarrow & X^1_d(T,F) \\
\downarrow & & \downarrow (-1)^{(e\ell)}\Pi_d \\
KS_1(T,F) & \longrightarrow & H^1_{\mathcal{F}(d)}(G_{\mathbb{Q}}, T) \otimes \mathbb{Z}G_d
\end{array} \]

**Theorem A.16.** Let \( G \) be a residually self-dual cartesian Selmer structure on \( T \) and let \( r \) be a rational prime satisfying

- \( \dim_{\mathbb{F}}(H^1(G_{\mathbb{Q}}, T)/H^1_{\mathcal{F}}(G_{\mathbb{Q}}, T)) = 1 \),
By the definition of Kolyvagin system of rank 0, we have a homomorphism
\[ X_0 \rightarrow \text{image} (8) \] is an isomorphism. Hence, it suffices to show that the map \( KS \) is an isomorphism. By \[17, \text{Lemma 4.6}, \] we have
\[ H^1_\mathcal{F}(G_q, T) \cong R \] and \[ H^1_\mathcal{F}(G_q, T) \cong R^{1+\nu(d)}. \]
Moreover, by 
\[ \text{Theorem 2.1}, \] we have a split exact sequence of free \( R \)-modules:
\[ 0 \rightarrow H^1_\mathcal{F}(G_q, T) \rightarrow H^1_\mathcal{F}(G_q, T) \rightarrow \bigoplus_{\ell \mid d} H^1_{\mathcal{F}_\ell}(G_q, T) \rightarrow 0. \]
These facts shows that \( \Pi_d \) is an isomorphism. By \[17, \text{Theorem 4.7}, \] the projection map
\[ SS_1(T, \mathcal{F}) \rightarrow X_0^1(T, \mathcal{F}) \]
is also an isomorphism. Hence this theorem follows from Proposition A.15 and the commutative diagram (7).

Next, we prove Theorem 2.20 when \( p = 3 \). First, let us show that the regulator map (constructed in \[19, \S 5.2\])
\[ \text{Reg}_0 : \text{SS}_0(T, \mathcal{G}) \rightarrow \text{KS}_0(T, \mathcal{G}) \]
is an isomorphism. Recall that we fix an isomorphism \( H^1_{\text{ur}}(G_q, T) \cong R \) for any prime \( \ell \in \mathcal{P} \) in order to define Kolyvagin systems of rank 0.
Suppose that \( r \in \mathcal{P} \setminus S(\mathcal{G}), \) we have
\[ \text{dim}_R(H^1(G_q, T)/H^1_{\mathcal{F}}(G_q, T)) = \text{dim}_R(H^1_{\text{ur}}(G_q, T)) = 1, \]
\[ H^1(G_q, T) \rightarrow H^1(G_q, T) \] is surjective.
The fixed isomorphism \( H^1_{\text{ur}}(G_q, T) \cong R \) induces an isomorphism \( W_d \cong W_{dr} \) for any integer \( d \in \mathcal{N}(\mathcal{G}, r) \) (see Definition 2.23). Hence we can obtain an isomorphism \( X_0^1(T, \mathcal{G}) \cong X_0^1(T, \mathcal{F}) \) for any integer \( d \in \mathcal{N}(\mathcal{G}, r) \), and it naturally induces an isomorphism
\[ \text{SS}_0(T, \mathcal{G}) \cong \text{SS}_1(T, \mathcal{F}). \]
By the definition of Kolyvagin system of rank 0, we have a homomorphism
\[ \text{KS}_0(T, \mathcal{G}) \rightarrow \text{KS}_1(T, \mathcal{F}); \ (\kappa_{d, r})_{(d, r) \in \mathcal{M}(\mathcal{G})} \rightarrow (\kappa_{d, r})_{d \in \mathcal{N}(\mathcal{G}, r)}. \]
Here \( \mathcal{M}(\mathcal{G}) := \bigcup_{q \in \mathcal{P} \setminus S(\mathcal{G})} \mathcal{N}(\mathcal{G}, q) \times \{q\}. \) By \[19, \text{Lemma 5.4}, \] we have the following commutative diagram:
\[ \begin{array}{ccc}
\text{SS}_0(T, \mathcal{G}) & \xrightarrow{\text{Reg}_0} & \text{SS}_1(T, \mathcal{F}) \\
\text{KS}_0(T, \mathcal{G}) & \xrightarrow{\text{Reg}_1} & \text{KS}_1(T, \mathcal{F}).
\end{array} \]

**Proposition A.18.** For any residually self-dual cartesian Selmer structure \( \mathcal{G} \) on \( T, \) the map \( \text{Reg}_0 \) is an isomorphism.

**Proof.** Theorem A.16 shows that the homomorphism \( \text{Reg}_1 \) in the commutative diagram (8) is an isomorphism. Hence, it suffices to show that the map \( \text{KS}_0(T, \mathcal{G}) \rightarrow \text{KS}_1(T, \mathcal{F}) \) is injective.

Let \( (\kappa_{d, r})_{(d, r) \in \mathcal{M}(\mathcal{G})} \in \text{KS}_0(T, \mathcal{G}) \) be a Kolyvagin system satisfying \( \kappa_{d, r} = 0 \) for any \( d \in \mathcal{N}(\mathcal{G}, r). \) Take a prime \( q \in \mathcal{P} \setminus S(\mathcal{G}) \) and an integer \( e \in \mathcal{N}(\mathcal{G}, q) \cap \mathcal{N}(\mathcal{G}, r) \)
with \( H^1_{\mu(G)}(G_{\mathbb{Q}}, T) = 0 \). Since \( T = T^\vee(1) \) and \( \overline{\gamma}(eq) = \overline{\gamma}^*(eq) \), by [17, Lemmas 3.13 and 3.14], we have isomorphisms
\[
H^1_{\mu(G)}(G_{\mathbb{Q}}, T)[m_\mathbb{R}] \cong H^1_{\mu(G)}(G_{\mathbb{Q}}, T) \cong H^1_{\mu(G)}(G_{\mathbb{Q}}, T^\vee(1))[m_\mathbb{R}].
\]
Hence \( H^1_{\mu(G)}(G_{\mathbb{Q}}, T) = H^1_{\mu(G)}(G_{\mathbb{Q}}, T^\vee(1)) = 0 \). Applying Theorem 2.1 with \( \mathcal{F}_1 = \mathcal{G}(e) \) and \( \mathcal{F}_2 = \mathcal{G}^t(e) \), we obtain an isomorphism
\[
\varphi_q^e : H^1_{\mu(G)}(G_{\mathbb{Q}}, T) \cong H^1_{\mu(G)}(G_{\mathbb{Q}}, T) \cong R \otimes_{\mathbb{Z}} G_q.
\]

The definition of Kolyvagin system of rank 0 implies that
\[
\varphi_q^e(\kappa, q) = -v_\nu(\kappa, q) = 0,
\]
and hence we have \( \kappa = 0 \). By proposition A.15, the map \( KS_1(T, \mathcal{G}) \longrightarrow H^1_{\mu(G)}(G_{\mathbb{Q}}, T) \) is injective. Therefore, \( 0 = (\kappa, q)_{d, \ell} \in KS_1(T, \mathcal{G}) \). Since \( q \) is an arbitrary prime and \( \mathcal{M}(\mathcal{G}) = \bigcup_{q \in \mathcal{P} \setminus S(\mathcal{G})} \mathcal{N}(\mathcal{G}, q) \times \{q\} \), we have \( 0 = (\kappa_{d, \ell}, q)_{d, \ell} \in KS_0(T, \mathcal{G}) \).

The same argument as in the proof of [19, Theorem 5.8] shows the following Theorem.

**Theorem A.19.** Let \( \mathcal{G} \) be a residually self-dual cartesian Selmer structure on the residually self-dual Galois representation \( T \).

1. For any element \( (d, \ell) \in \mathcal{M}(\mathcal{G}) \) with \( H^1_{\mu(G)}(G_{\mathbb{Q}}, T) = 0 \), the projection map
\[
KS_0(T, \mathcal{G}) \longrightarrow H^1_{\mu(G)}(G_{\mathbb{Q}}, T) \otimes_{\mathbb{Z}} G_d
\]
is an isomorphism. In particular, the \( R \)-module \( KS_0(T, \mathcal{G}) \) is free of rank 1.

2. For any basis \( \kappa \in KS_0(T, \mathcal{G}) \) and any integer \( d \in \bigcup_{q \in \mathcal{P} \setminus S(\mathcal{G})} \mathcal{N}(\mathcal{G}, q) \), we have
\[
R \cdot \delta(\kappa)_d = \text{Fit}^R_0(H^1_{\mu(G)}(G_{\mathbb{Q}}, T^\vee(1)), q).
\]

**References**

[1] Burns, David; Sakamoto, Ryotaro; Sano, Takamichi. On the theory of higher rank Euler, Kolyvagin and Stark systems, II, submitted for publication, arXiv: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 No. 295 (2004), ix, 117–290.
[5] Kurihara, Masato. Refined Iwasawa theory for p-adic representations and the structure of Selmer groups, Münster J. Math. 7 (2014), no. 1, 149–223.
[6] 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.
[7] Mazur, Barry; Rubin, Karl. Kolyvagin systems, Mem. Amer. Math. Soc. 799 (2004).
[8] Mazur, Barry; Rubin, Karl. Controlling Selmer groups in the higher core rank case, J. Th. Nombres Bordeaux 28 (2016) 145–183.
[9] Mazur, Barry; Tate, John. Refined conjectures of the "Birch and Swinnerton-Dyer type", Duke Math. J. 54 (1987), no. 2, 711–750.
[10] 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.
[11] Nekovář, Jan. Selmer complexes. Astérisque No. 310 (2006), viii+559 pp.
[12] Rubin, Karl. Euler systems, Annals of Math. Studies 147, Princeton Univ. Press, 2000.
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.

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

Kim, Chan-Ho. A refined Birch and Swinnerton-Dyer type conjecture for Selmer groups, preprint.

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

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

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, 141–159.

Sakamoto, Ryotaro. On the theory of Kolyvagin systems of rank 0, to appear in Journal de Théorie des Nombres.

Skinner, Christopher; Urban, Eric. The Iwasawa main conjectures for GL2. Invent. Math. 195 (2014), no. 1, 1–277.

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

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

RIKEN Center for Advanced Intelligence Project, Nihonbashi 1-chome Mitsui Building, 15th floor, 1-4-1 Nihonbashi, Chuo-ku, Tokyo 103-0027, Japan

Email address: ryotaro.sakamoto@riken.jp