JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Ryotaro SAKAMOTO

The theory of Kolyvagin systems for $p = 3$

Tome 36, nº 3 (2024), p. 919-946.
https://doi.org/10.5802/jtnb.1300

e-ISSN : 2118-8572

Journal de Théorie des Nombres de Bordeaux **36** (2024), 919–946

The theory of Kolyvagin systems for $p = 3$

par Ryotaro SAKAMOTO

Résumé. Dans cet article, nous considérons la théorie des systèmes de Kolyvagin lorsque $p = 3$ et montrons que cette théorie fonctionne toujours dans un certain cadre qui a été exclu dans les études précédentes. Comme application de ce résultat, nous prouvons une conjecture de Kurihara concernant les symboles modulaires dans le cas $p = 3$.

Abstract. In this paper, we consider the theory of Kolyvagin systems when $p = 3$ and show that this theory still works in a certain setting that has been excluded in previous studies. As an application of this result, we prove a conjecture of Kurihara concerning modular symbols in the case $p = 3$.

1. Introduction

The theory of Kolyvagin systems was introduced by Mazur and Rubin ([17]) in order to better understand the theory of Euler systems. Under suitable hypotheses, Mazur and Rubin showed in [17, Corollary 4.5.2 and Theorem 4.5.9] that Kolyvagin systems has a rigid structure, namely, the module of Kolyvagin systems is free of rank 1, and that its basis controls the size and shape of the corresponding dual Selmer module. This result has many applications. For example, using the rigidity of Kolyvagin systems, Mazur and Rubin proved in [19] the refined class number formula conjectured by Darmon. Büyükboduk proved results similar to those of Mazur–Rubin in the Iwasawa theoretic setting (see [5]), and he (and Lei) obtained many arithmetic consequences (see [3, 4, 6, 7, 8, 9, 10] for example). The author also generalized Mazur–Rubin's result to the case where the coefficient ring of a Galois representation is Gorenstein ([22]).

Let T be a Galois representation of a number field K over a local artinian ring R with finite cardinality. We write p for the residue characteristic of R. We denote by G_K the absolute Galois group of the number field K. Then for any Selmer structure $\mathcal{F}$ on T, we can define Kolyvagin systems associated with the pair $(T, \mathcal{F})$ (see Definition 4.1). One of the standard hypotheses of Kolyvagin systems says that $p \geq 5$ or $\mathrm{Hom}_{\mathbb{Z}_p[G_K]}(\overline{T}, \overline{T}^{\vee}(1)) = 0$ (see the hypothesis (H.4) in [17, p. 27]). Here $\overline{T}$ is the residual representation of

Manuscrit reçu le 27 mars 2023, révisé le 13 février 2024, accepté le 8 novembre 2024.
2020 *Mathematics Subject Classification.* 11R23, 11G05, 11R34, 11S25.
Mots-clefs. Kolyvagin systems, modular symbols, Kurihara conjecture.
The author is supported by JSPS KAKENHI Grant Number 24K16886.

T and $\overline{T}^{\vee}(1) := \mathrm{Hom}(\overline{T}, \mathbb{Q}_p/\mathbb{Z}_p)(1)$. Therefore, the case that $p = 3$ and $\mathrm{Hom}_{\mathbb{Z}_p[G_K]}(\overline{T}, \overline{T}^{\vee}(1)) \neq 0$ is excluded in the theory of Kolyvagin systems. This hypothesis, as mentioned by Mazur and Rubin at the beginning of [17, §3.6], is used only to guarantee that there exist infinitely many useful primes (see [17, Proposition 3.6.1]).

In the present paper, we consider the case $p = 3$ and the Galois representation T is residually self-dual. In this scenario, we prove the existence of useful primes (Lemma 5.2 and Corollary 5.5), although in a slightly weaker one than the Mazur–Rubin's result [17, Proposition 3.6.1]. Further assuming that the Selmer structure $\mathcal{F}$ is residually coisotropic (see Definition 3.8), we show the connectedness of the graph $\mathcal{X}^0$ defined in [17, Definition 4.3.6] from Lemma 5.2 and Corollary 5.5. The connectedness of the graph $\mathcal{X}^0$ is one of the important property in the theory of Kolyvagin systems, and this shows that the theory of Kolyvagin systems also works in our case. Roughly speaking, the main result of the present paper is the following:

Theorem 1.1 (Theorem 4.4)**.** *Suppose that*

- $p = 3$,
- *T is residually self-dual, that is, $\overline{T} \cong \overline{T}^{\vee}(1)$ as G_K-representations, and*
- *$\mathcal{F}$ is residually coisotropic.*

Then the module of Kolyvagin systems are free of rank 1 *and its basis controls the initial Fitting ideal of the dual Selmer module associated with $\mathcal{F}$.*

The proof of this theorem is given in Section 7. Furthermore, in Section 8, we explain that the theory of Kolyvagin system of rank 0 introduced by the author in [24] also works in the case that $p = 3$ and that T and $\mathcal{F}$ are residually self-dual (see Theorem 8.5). In Section 9, we give applications of Theorems 4.4 and 8.5 for a 3-adic Galois representation associated with an elliptic curve over $\mathbb{Q}$. In particular, we prove a conjecture of Kurihara ([14, Conjecture 2]) when $p = 3$ (see Theorem 9.11).

2. Setting

In this section, we introduce the notations and hypotheses used throughout this paper.

Let K be a number field and we write $\mathcal{O}_K$ for the ring of integers in K. Let $\mathcal{H}$ denote the Hilbert class field of K. We take a positive integer α and put

$$\mathcal{H}_\alpha := \mathcal{H}(\mu_{3^\alpha}, (\mathcal{O}_K^\times)^{3^{-\alpha}}).$$

Here for any positive integer m, we denote by μ_m the group of m-th roots of unity. For any field L, we write $\overline{L}$ for a (fixed) separable closure of L and set

$$G_L := \mathrm{Gal}(\overline{L}/L).$$

Let R be a zero-dimensional Gorenstein local ring with finite residue field $\mathbb{F}$ such that $3^\alpha R = 0$ and $\mathrm{char}(\mathbb{F}) = 3$. We denote by $\mathfrak{m}_R$ the maximal ideal of R. For any R-module M and ideal $I \subset R$, we write $M[I]$ for the R-submodule of M consisting of elements annihilated by I;

$$M[I] := \{m \in M \mid Im = 0\}.$$

Let T be a free R-module of finite rank with a continuous action of G_K, unramified at almost all primes of K. We denote by $S_{\mathrm{ram}}(T)$ the set of places of K at which T is ramified. For notational simplicity, we put

$$\overline{T} := T \otimes_R \mathbb{F}.$$

We also put $(-)^\vee := \mathrm{Hom}(-, \mathbb{Q}_3/\mathbb{Z}_3)$. In the present paper, we always assume the following conditions, which are (part of) standard hypotheses in the theory of Kolyvagin systems (see [17, §3.5]):

(H.1) The $\mathbb{F}[G_K]$-module $\overline{T}$ is irreducible.

(H.2) There is an element $\tau \in G_{\mathcal{H}_\alpha}$ such that $T/(\tau - 1)T \cong R$ as R-modules.

(H.3) The module $H^1(\mathcal{H}_\alpha(T)/K, \overline{T})$ vanishes, where $\mathcal{H}_\alpha(T)$ is the field corresponds to the kernel of the homomorphism $G_{\mathcal{H}_\alpha} \longrightarrow \mathrm{Aut}(T)$.

In addition, we also assume that

(H.SD) the Galois representation T is residually self-dual, i.e., there is an isomorphism $\overline{T} \cong \overline{T}^\vee(1)$ as $\mathbb{F}[G_K]$-modules.

Let $\mathcal{F}$ be a Selmer structure on T, namely, $\mathcal{F}$ is a collection of the following data:

- a finite set $S(\mathcal{F})$ of places of K containing the set $S_{\mathrm{ram}}(T) \cup \{\mathfrak{q} \mid 3\infty\}$,
- a choice of R-submodule $H^1_{\mathcal{F}}(K_\mathfrak{q}, T) \subset H^1(K_\mathfrak{q}, T)$ for each prime $\mathfrak{q} \in S(\mathcal{F})$.

We write $\overline{\mathcal{F}}$ for the Selmer structure on $\overline{T}$ induced by $\mathcal{F}$, that is, $S(\overline{\mathcal{F}}) := S(\mathcal{F})$ and $H^1_{\overline{\mathcal{F}}}(K_\mathfrak{q}, \overline{T}) := \mathrm{im}\left(H^1_{\mathcal{F}}(K_\mathfrak{q}, T) \longrightarrow H^1(K_\mathfrak{q}, \overline{T})\right)$.

We define a set $\mathcal{P}$ of primes of K by

$$\mathcal{P} := \left\{ \mathfrak{q} \notin S(\mathcal{F}) \;\middle|\; \begin{array}{l} \mathfrak{q} \text{ is unramified in } \mathcal{H}_\alpha(T)/K, \\ \mathrm{Fr}_\mathfrak{q} \text{ is conjugate to } \tau \text{ in } \mathrm{Gal}(\mathcal{H}_\alpha(T)/K) \end{array} \right\}.$$

We write $\mathcal{N}$ for the set of square-free products of primes in $\mathcal{P}$. Note that the trivial ideal 1 belongs to $\mathcal{N}$.

3. Selmer structures

3.1. Selmer module. For each prime $\mathfrak{q} \notin S(\mathcal{F})$ of K, we set

$$H^1_{\mathcal{F}}(K_\mathfrak{q}, T) := H^1_{\mathrm{ur}}(K_\mathfrak{q}, T) := \ker\left(H^1(K_\mathfrak{q}, T) \longrightarrow H^1(K_\mathfrak{q}^{\mathrm{ur}}, T)\right),$$

where $K_{\mathfrak{q}}^{\mathrm{ur}}$ is the maximal unramified extension of $K_{\mathfrak{q}}$. We then define the Selmer module $H^1_{\mathcal{F}}(K,T)$ by

$$H^1_{\mathcal{F}}(K,T) := \ker\left(H^1(K,T) \longrightarrow \bigoplus_{\mathfrak{q}} H^1(K_{\mathfrak{q}},T)/H^1_{\mathcal{F}}(K_{\mathfrak{q}},T)\right).$$

Here $\mathfrak{q}$ runs over the set of all the primes of K. For each prime $\mathfrak{q}$ of K, we define

$$H^1_{\mathcal{F}^*}(K_{\mathfrak{q}},T^\vee(1)) \subset H^1(K_{\mathfrak{q}},T^\vee(1))$$

to be the orthogonal complement of $H^1_{\mathcal{F}}(K_{\mathfrak{q}},T)$ with respect to the local Tate pairing, and we get the dual Selmer structure $\mathcal{F}^*$ on $T^\vee(1)$.

Theorem 3.1 ([17, Theorem 2.3.4])**.** *Let $T' \in \{T, \overline{T}\}$. Let $\mathcal{F}_1$ and $\mathcal{F}_2$ be Selmer structures on T' satisfying*

$$H^1_{\mathcal{F}_1}(K_{\mathfrak{q}},T') \subset H^1_{\mathcal{F}_2}(K_{\mathfrak{q}},T')$$

for any prime $\mathfrak{q}$ of K. Then we have an exact sequence of R-modules

$$\begin{aligned}0 \longrightarrow H^1_{\mathcal{F}_1}(K,T') \longrightarrow H^1_{\mathcal{F}_2}(K,T') \longrightarrow \bigoplus_{\mathfrak{q}} H^1_{\mathcal{F}_2}(K_{\mathfrak{q}},T')/H^1_{\mathcal{F}_1}(K_{\mathfrak{q}},T')\\ \longrightarrow H^1_{\mathcal{F}_1^*}(K,(T')^\vee(1))^\vee \longrightarrow H^1_{\mathcal{F}_2^*}(K,(T')^\vee(1))^\vee \longrightarrow 0,\end{aligned}$$

where $\mathfrak{q}$ runs over the set $S(\mathcal{F}_1) \cup S(\mathcal{F}_2)$.

Following Mazur and Rubin, we define a transversal local condition $H^1_{\mathrm{tr}}(K_{\mathfrak{q}},T)$ and a Selmer structure $\mathcal{F}^{\mathfrak{a}}_{\mathfrak{b}}(\mathfrak{c})$ on T.

Definition 3.2 ([17, Definition 1.1.6], [18, Definition 1.2])**.** Let $\mathfrak{q}$ be a prime of K. We write $K(\mathfrak{q})$ for the maximal 3-power extension of K in the ray class field modulo $\mathfrak{q}$. Define

$$H^1_{\mathrm{tr}}(K_{\mathfrak{q}},T) := \ker\left(H^1(K_{\mathfrak{q}},T) \longrightarrow H^1(K(\mathfrak{q})_{\tilde{\mathfrak{q}}},T)\right).$$

Here $\widetilde{\mathfrak{q}}$ is a (fixed) prime of $K(\mathfrak{q})$ above $\mathfrak{q}$.

Definition 3.3 ([18, Definition 2.3])**.** For any (square-free) ideals $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ which are pairwise relatively prime, the Selmer structure $\mathcal{F}^{\mathfrak{a}}_{\mathfrak{b}}(\mathfrak{c})$ on T is defined to be the following data:

- $S(\mathcal{F}^{\mathfrak{a}}_{\mathfrak{b}}(\mathfrak{c})) := S(\mathcal{F}) \cup \{\mathfrak{q} \mid \mathfrak{abc}\}$,
- $H^1_{\mathcal{F}^{\mathfrak{a}}_{\mathfrak{b}}(\mathfrak{c})}(K_{\mathfrak{q}},T) := \begin{cases} H^1(K_{\mathfrak{q}},T) & \text{if } \mathfrak{q} \mid \mathfrak{a}, \\ 0 & \text{if } \mathfrak{q} \mid \mathfrak{b}, \\ H^1_{\mathrm{tr}}(K_{\mathfrak{q}},T) & \text{if } \mathfrak{q} \mid \mathfrak{c}, \\ H^1_{\mathcal{F}}(K_{\mathfrak{q}},T) & \text{otherwise.} \end{cases}$

Note that $(\mathcal{F}^{\mathfrak{a}}_{\mathfrak{b}}(\mathfrak{c}))^* = (\mathcal{F}^*)^{\mathfrak{b}}_{\mathfrak{a}}(\mathfrak{c})$. If any of $\mathfrak{a}$, $\mathfrak{b}$, or $\mathfrak{c}$ are 1, they shall be excluded from the notation, e.g., $\mathcal{F}^{\mathfrak{a}} = \mathcal{F}^{\mathfrak{a}}_1(1)$.

Lemma 3.4 ([17, Lemma 3.5.3]). *For any square-free ideals $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ in $\mathcal{N}$ which are pairwise relatively prime, the inclusion map*

$$\overline{T}^{\vee}(1) = T^{\vee}(1)[\mathfrak{m}_R] \hookrightarrow T^{\vee}(1)$$

induces an R-isomorphism

$$H^1_{(\overline{\mathcal{F}}^*)^{\mathfrak{b}}_{\mathfrak{a}}(\mathfrak{c})}(K, \overline{T}^{\vee}(1)) \xrightarrow{\sim} H^1_{(\mathcal{F}^*)^{\mathfrak{b}}_{\mathfrak{a}}(\mathfrak{c})}(K, T^{\vee}(1))[\mathfrak{m}_R].$$

3.1.1. *Cartesian condition.* Fix an injective R-homomorphism $\mathbb{F} \hookrightarrow R$. This homomorphism induces an injective $R[G_K]$-homomorphism

$$\overline{T} \hookrightarrow T.$$

Since R is a zero dimensional Gorenstein local ring, we have $\dim_{\mathbb{F}}(R[\mathfrak{m}_R]) = \dim_{\mathbb{F}}(\mathrm{Hom}_R(\mathbb{F}, R)) = 1$ see [16, Theorem 18.1] and hence, injection $\mathbb{F} \hookrightarrow R$ is unique up to the multiplication by a unit in R.

For notational simplicity, we set

$$H^1_{/?}(K_{\mathfrak{q}}, T) := H^1(K_{\mathfrak{q}}, T)/H^1_?(K_{\mathfrak{q}}, T)$$

for each $? \in \{\mathrm{ur}, \mathrm{tr}, \mathcal{F}, \mathcal{F}^*\}$.

Definition 3.5. We say that $\mathcal{F}$ is cartesian if for any prime $\mathfrak{q} \in S(\mathcal{F})$, the R-homomorphism

$$H^1_{/\overline{\mathcal{F}}}(K_{\mathfrak{q}}, \overline{T}) \longrightarrow H^1_{/\mathcal{F}}(K_{\mathfrak{q}}, T)$$

induced by $\overline{T} \hookrightarrow T$ is injective. Note that the definition of the cartesian property in the present paper is slightly weaker than that of Mazur and Rubin in [17, Definition 1.1.4].

For any square-free ideal $\mathfrak{d} \in \mathcal{N}$, we define

$$\begin{aligned}
\nu(\mathfrak{d}) &:= \text{the number of distinct primes dividing } \mathfrak{d},\\
\lambda(\mathfrak{d}) &:= \dim_{\mathbb{F}}(H^1_{\overline{\mathcal{F}}(\mathfrak{d})}(K, \overline{T})),\\
\lambda^*(\mathfrak{d}) &:= \dim_{\mathbb{F}}(H^1_{\overline{\mathcal{F}}^*(\mathfrak{d})}(K, \overline{T}^{\vee}(1))).
\end{aligned}$$

Definition 3.6. We define the core rank $\chi(\mathcal{F})$ of $\mathcal{F}$ by

$$\chi(\mathcal{F}) := \lambda(1) - \lambda^*(1).$$

Lemma 3.7. *Let $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ be ideals in $\mathcal{N}$ which are pairwise relatively prime. Suppose that $\mathcal{F}$ is cartesian. Then the following claims are valid.*

(1) *The Selmer structure $\mathcal{F}^{\mathfrak{a}}_{\mathfrak{b}}(\mathfrak{c})$ is cartesian and $\chi(\mathcal{F}^{\mathfrak{a}}_{\mathfrak{b}}(\mathfrak{c})) = \chi(\mathcal{F}) + \nu(\mathfrak{a}) - \nu(\mathfrak{b})$. In particular, $\chi(\mathcal{F}) = \chi(\mathcal{F}(\mathfrak{c}))$.*

(2) *If $H^1_{(\mathcal{F}^*)^{\mathfrak{b}}_{\mathfrak{a}}(\mathfrak{c})}(K, T^{\vee}(1))$ vanishes, then $H^1_{\mathcal{F}^{\mathfrak{a}}_{\mathfrak{b}}(\mathfrak{c})}(K, T)$ is a free R-module of rank $\chi(\mathcal{F}^{\mathfrak{a}}_{\mathfrak{b}}(\mathfrak{c}))$.*

(3) *The fixed injection $\overline{T} \hookrightarrow T$ induces an R-isomorphism*

$$H^1_{\overline{\mathcal{F}}^{\mathfrak{a}}_{\mathfrak{b}}(\mathfrak{c})}(K, \overline{T}) \xrightarrow{\sim} H^1_{\mathcal{F}^{\mathfrak{a}}_{\mathfrak{b}}(\mathfrak{c})}(K, T)[\mathfrak{m}_R].$$

Proof. Claim (1) follows from [22, Corollary 3.21]. Note that the formula $\chi(\mathcal{F}^{\mathfrak{a}}_{\mathfrak{b}}(\mathfrak{c})) = \chi(\mathcal{F}) + \nu(\mathfrak{a}) - \nu(\mathfrak{b})$ easily follows from Theorem 3.1 (see [17, Lemma 4.1.6]). Let us show Claim (2). The Selmer structure $\mathcal{F}^{\mathfrak{a}}_{\mathfrak{b}}(\mathfrak{c})$ is cartesian by [22, Corollary 3.18]. Moreover, since the module $H^1_{(\mathcal{F}^*)^{\mathfrak{b}}_{\mathfrak{a}}(\mathfrak{c})}(K, T^\vee(1))$ vanishes, the trivial ideal 1 is a core vertex for $\mathcal{F}^{\mathfrak{a}}_{\mathfrak{b}}(\mathfrak{c})$ in the sense of [22, Definition 4.3]. Hence, applying [22, Lemma 4.6] with $\mathcal{F}^{\mathfrak{a}}_{\mathfrak{b}}(\mathfrak{c})$ and $\mathfrak{n} = 1$, we conclude that $H^1_{\mathcal{F}^{\mathfrak{a}}_{\mathfrak{b}}(\mathfrak{c})}(K, T)$ is a free R-module of rank $\chi(\mathcal{F}^{\mathfrak{a}}_{\mathfrak{b}}(\mathfrak{c}))$. Claim (3) follows from [22, Corollaries 3.13 and 3.18]. □

3.1.2. ***Coisotropic Selmer structure.*** Recall that $\overline{T} \cong \overline{T}^\vee(1)$ as $\mathbb{F}[G_K]$-modules thanks to the hypothesis (H.SD) in Section 2. Throughout this paper, by using this $\mathbb{F}[G_K]$-isomorphism, we regard $\overline{\mathcal{F}}^*$ as a Selmer structure on $\overline{T}$, and hence $\overline{\mathcal{F}}$ and $\overline{\mathcal{F}}^*$ can be compared.

Definition 3.8. We say that $\mathcal{F}$ is residually coisotropic if $\overline{\mathcal{F}}^* < \overline{\mathcal{F}}$, that is,

$$H^1_{\overline{\mathcal{F}}^*}(K_{\mathfrak{q}}, \overline{T}) \subset H^1_{\overline{\mathcal{F}}}(K_{\mathfrak{q}}, \overline{T})$$

for any prime $\mathfrak{q} \in S(\mathcal{F})$.

Definition 3.9. We define a set $E(\mathcal{F})$ of primes of K by

$$E(\mathcal{F}) := \{\mathfrak{q} \in S(\mathcal{F}) \mid H^1_{\overline{\mathcal{F}}}(K_{\mathfrak{q}}, \overline{T}) \neq H^1_{\overline{\mathcal{F}}^*}(K_{\mathfrak{q}}, \overline{T})\}.$$

Remark 3.10. In Theorem 4.4 we make the assumption that $\mathcal{F}$ is cartesian with $\chi(\mathcal{F}) = 1$ and residually coisotropic. To prove Theorem 4.4, we need to compare Selmer structures $\mathcal{F}^*(\mathfrak{d})$ and $\mathcal{F}(\mathfrak{d})$ for any square-free ideal $\mathfrak{d} \in \mathcal{N}$. Hence we use Theorem 3.1 with $\mathcal{F}_1 = \mathcal{F}^*(\mathfrak{d})$ and $\mathcal{F}_2 = \mathcal{F}(\mathfrak{d})$, and the set $E(\mathcal{F})$ plays an important role.

Lemma 3.11. *Suppose that $\mathcal{F}$ is cartesian with $\chi(\mathcal{F}) = 1$ and residually coisotropic. For any square-free ideal $\mathfrak{d} \in \mathcal{N}$, any element $c \in H^1_{\overline{\mathcal{F}}(\mathfrak{d})}(K, \overline{T}) \setminus H^1_{\overline{\mathcal{F}}^*(\mathfrak{d})}(K, \overline{T})$, and any prime $\mathfrak{q} \in E(\mathcal{F})$, we have*

$$\mathrm{loc}_{\mathfrak{q}}(c) \notin H^1_{\overline{\mathcal{F}}^*(\mathfrak{d})}(K_{\mathfrak{q}}, \overline{T}).$$

Here $\mathrm{loc}_{\mathfrak{q}}$ *is the localization map at* $\mathfrak{q}$.

Proof. For notational simplicity, we put

$$X_{\mathfrak{q}} := H^1_{\overline{\mathcal{F}}(\mathfrak{d})}(K_{\mathfrak{q}}, \overline{T}) / H^1_{\overline{\mathcal{F}}^*(\mathfrak{d})}(K_{\mathfrak{q}}, \overline{T}),$$
$$X := \bigoplus_{\mathfrak{q} \in E(\mathcal{F})} X_{\mathfrak{q}}.$$

Applying Theorem 3.1 with $\mathcal{F}_1 = \overline{\mathcal{F}}^*(\mathfrak{d})$ and $\mathcal{F}_2 = \overline{\mathcal{F}}(\mathfrak{d})$, we obtain an exact sequence of $\mathbb{F}$-modules

$$0 \to H^1_{\overline{\mathcal{F}}^*(\mathfrak{d})}(K, \overline{T}) \to H^1_{\overline{\mathcal{F}}(\mathfrak{d})}(K, \overline{T}) \xrightarrow{\bigoplus_{\mathfrak{q} \in E(\mathcal{F})} \mathrm{loc}_{\mathfrak{q}}} X \to H^1_{\overline{\mathcal{F}}(\mathfrak{d})}(K, \overline{T})^\vee. \tag{3.1}$$

Put

$$Y := \operatorname{im}\left(H^1_{\overline{\mathcal{F}}(\mathfrak{d})}(K,\overline{T}) \xrightarrow{\bigoplus_{\mathfrak{q}\in E(\mathcal{F})}\mathrm{loc}_{\mathfrak{q}}} X\right).$$

The local Tate pairing and the fixed isomorphism $\overline{T} \cong \overline{T}^{\vee}(1)$ induce a pairing $(-,-)_{\mathfrak{q}} \colon X_{\mathfrak{q}} \times X_{\mathfrak{q}} \longrightarrow R$ for each prime $\mathfrak{q} \in E(\mathcal{F})$. Moreover, the orthogonal complement $Y^{\perp}$ with respect to the sum $\sum_{\mathfrak{q}\in E(\mathcal{F})}(-,-)_{\mathfrak{q}}$ of pairings coincides with Y (see [17, Theorem 2.3.4]). If $\mathrm{loc}_{\mathfrak{q}}(H^1_{\overline{\mathcal{F}}(\mathfrak{d})}(K,\overline{T})) = 0$ for some prime $\mathfrak{q} \in E(\mathcal{F})$, then we have $X_{\mathfrak{q}} \cap Y = \{0\}$ and $0 \neq X_{\mathfrak{q}} \subset Y^{\perp}$, which contradicts the fact that $Y = Y^{\perp}$. Hence

$$\mathrm{loc}_{\mathfrak{q}}(H^1_{\overline{\mathcal{F}}(\mathfrak{d})}(K,\overline{T})) \neq 0$$

for each prime $\mathfrak{q} \in E(\mathcal{F})$, which completes the proof of the lemma since $\lambda(\mathfrak{d}) - \lambda^*(\mathfrak{d}) = \chi(\mathcal{F}) = 1$ by Lemma 3.7(1). □

4. Kolyvagin systems of rank 1

In this section, we recall the definition of Kolyvagin systems (of rank 1) introduced by Mazur and Rubin in [17] and state our main result (Theorem 4.4).

For any prime $\mathfrak{q} \in \mathcal{P}$, the hypothesis (H.2) and the definition of $\mathcal{P}$ show that

$$H^1_{\mathrm{ur}}(K_{\mathfrak{q}},T) \cong T/(\mathrm{Fr}_{\mathfrak{q}}-1)T \cong R$$

as R-modules. Moreover, Mazur and Rubin proved in [17, Definition 1.2.2, and Lemmas 1.2.3 and 1.2.4] that we have a functorial splitting

$$H^1(K_{\mathfrak{q}},T) = H^1_{\mathrm{ur}}(K_{\mathfrak{q}},T) \oplus H^1_{\mathrm{tr}}(K_{\mathfrak{q}},T)$$

and a natural R-isomorphism (called the finite-singular comparison isomorphism)

$$\phi^{\mathrm{fs}}_{\mathfrak{q}} \colon H^1_{\mathrm{ur}}(K_{\mathfrak{q}},T) \xrightarrow{\sim} H^1_{/\mathrm{ur}}(K_{\mathfrak{q}},T) \otimes_{\mathbb{Z}} G_{\mathfrak{q}}.$$

For each square-free ideal $\mathfrak{d} \in \mathcal{N}$, we put

$$G_{\mathfrak{d}} := \bigotimes_{\mathfrak{q}\mid\mathfrak{d}} \mathrm{Gal}(K(\mathfrak{q})_{\tilde{\mathfrak{q}}}/K_{\mathfrak{q}}).$$

Note that for any R-module M, we have $M \cong M \otimes_{\mathbb{Z}} G_{\mathfrak{d}}$ as R-modules by the definition of $\mathcal{P}$ and the fact that $3^{\alpha}R = 0$.

For any prime $\mathfrak{q} \in \mathcal{P}$, we have two R-homomorphisms

$$v_{\mathfrak{q}} \colon H^1(K,T) \xrightarrow{\mathrm{loc}_{\mathfrak{q}}} H^1(K_{\mathfrak{q}},T) \longrightarrow H^1_{/\mathrm{ur}}(K_{\mathfrak{q}},T),$$

$$\varphi^{\mathrm{fs}}_{\mathfrak{q}} \colon H^1(K,T) \xrightarrow{\mathrm{loc}_{\mathfrak{q}}} H^1(K_{\mathfrak{q}},T) \xrightarrow{\mathrm{pr}_{\mathrm{ur}}} H^1_{\mathrm{ur}}(K_{\mathfrak{q}},T) \xrightarrow[\cong]{\phi^{\mathrm{fs}}_{\mathfrak{q}}} H^1_{/\mathrm{ur}}(K_{\mathfrak{q}},T) \otimes_{\mathbb{Z}} G_{\mathfrak{q}}.$$

Here $\mathrm{pr}_{\mathrm{ur}} \colon H^1(K_{\mathfrak{q}},T) \longrightarrow H^1_{\mathrm{ur}}(K_{\mathfrak{q}},T)$ is the projection map with respect to the decomposition $H^1(K_{\mathfrak{q}},T) = H^1_{\mathrm{ur}}(K_{\mathfrak{q}},T) \oplus H^1_{\mathrm{tr}}(K_{\mathfrak{q}},T)$.

Definition 4.1. We define the R-module $\mathrm{KS}_1(T, \mathcal{F})$ of Kolyvagin systems of rank 1 to be the set of elements

$$(\kappa_{\mathfrak{d}})_{\mathfrak{d} \in \mathcal{N}} \in \prod_{\mathfrak{d} \in \mathcal{N}} H^1_{\mathcal{F}(\mathfrak{d})}(K, T) \otimes_{\mathbb{Z}} G_{\mathfrak{d}}$$

satisfying the finite-singular relation

$$v_{\mathfrak{q}}(\kappa_{\mathfrak{d}\mathfrak{q}}) = \varphi^{\mathrm{fs}}_{\mathfrak{q}}(\kappa_{\mathfrak{d}})$$

for any ideal $\mathfrak{d} \in \mathcal{N}$ and any prime $\mathfrak{q} \in \mathcal{P}$ with $\mathfrak{q} \nmid \mathfrak{d}$.

Definition 4.2. Let S be a ring and M a finitely generated S-module. For any element $m \in M$, we define an ideal $I_S(m)$ of S by

$$I_S(m) := \{f(m) \mid f \in \mathrm{Hom}_S(M, S)\}.$$

Remark 4.3. Let S be a ring and M a finitely generated S-module. When the ring S is a zero-dimensional Gorenstein local ring, for any element $m \in M$, the natural homomorphism $\mathrm{Hom}_S(M, S) \longrightarrow \mathrm{Hom}_S(Sm, S)$ is surjective since S is an injective S-module. Hence in this case, the ideal $I_S(m)$ is independent of what the module M the element m is in, namely, for any R-submodule $N \subset M$ with $m \in N$, we have

$$I_S(m) = \{f(m) \mid f \in \mathrm{Hom}_S(M, S)\} = \{f(m) \mid f \in \mathrm{Hom}_S(N, S)\}.$$

The following is the main result of this paper, derived from Propositions 7.6 and 7.7.

Theorem 4.4. *Suppose that*

- T *satisfies the hypotheses* (H.1), (H.2), (H.3), *and* (H.SD) *in Section 2,*
- $\mathcal{F}$ *is cartesian with* $\chi(\mathcal{F}) = 1$ *and residually coisotropic.*

Then the following claims are valid.

(1) *The R-module* $\mathrm{KS}_1(T, \mathcal{F})$ *is free of rank* 1. *More precisely, for any square-free ideal* $\mathfrak{d} \in \mathcal{N}$ *with* $\lambda^*(\mathfrak{d}) = 0$, *the projection map*

$$\mathrm{KS}_1(T, \mathcal{F}) \longrightarrow H^1_{\mathcal{F}(\mathfrak{d})}(K, T) \otimes_{\mathbb{Z}} G_{\mathfrak{d}}$$

is an isomorphism.

(2) *For any square-free ideal* $\mathfrak{d} \in \mathcal{N}$ *and basis* $(\kappa_{\mathfrak{e}})_{\mathfrak{e} \in \mathcal{N}} \in \mathrm{KS}_1(T, \mathcal{F})$, *we have*

$$I_R(\kappa_{\mathfrak{d}}) = \mathrm{Fitt}^0_R(H^1_{\mathcal{F}(\mathfrak{d})}(K, T^\vee(1))^\vee).$$

Remark 4.5. In this remark, we consider the case that the assumptions (H.1), (H.2), (H.3) hold true and that

$$\mathrm{char}(\mathbb{F}) := p \geq 5 \quad \text{or} \quad \mathrm{Hom}_{\mathbb{F}_p[G_K]}(\overline{T}, \overline{T}^\vee(1)) = 0$$

instead of the assumption (H.SD). In particular, the assumption (H.SD) does not hold if $p = 3$.

When the maximal ideal $\mathfrak{m}_R$ of R is principal, the assertions in Theorem 4.4 is proved by Mazur, Rubin, and Howard in [17, Corollary 4.5.2]. When R is a complete regular local ring or certain Gorenstein local ring, the assertions in Theorem 4.4 is proven by Büyükboduk in [5, 8]. When R is a general complete Gorenstein local ring, the assertions in Theorem 4.4 is proven by Burns, the author, and Sano in [1, Theorem 5.2].

5. Application of the Chebotarev density theorem

As mentioned by Mazur and Rubin in the beginning of [17, §3.6], in the theory of Kolyvagin systems, the assumption that $\mathrm{char}(\mathbb{F}) = p > 3$ or $\mathrm{Hom}_{\mathbb{F}_p[G_K]}(\overline{T}, \overline{T}^\vee(1)) = 0$ is only used for choosing useful primes in $\mathcal{P}$ ([17, Proposition 3.6.1]). In this section, by using the coisotropy of $\overline{\mathcal{F}}$, we prove a result similar to [17, Proposition 3.6.1] in our case, i.e., when $\mathrm{char}(\mathbb{F}) = 3$ and $\overline{T} \cong \overline{T}^\vee(1)$ (see Lemma 5.2 and Corollary 5.5).

Lemma 5.1. *Let a be a positive integer and G a group. Take non-zero group homomorphisms $\varphi_1, \varphi_2, \varphi_3, \varphi_4 \in \mathrm{Hom}(G, \mathbb{F}_3^a)$. 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 $\varphi_{i,j} := \mathrm{pr}_j \circ \varphi_i \colon G \longrightarrow \mathbb{F}_3$, where $\mathrm{pr}_j \colon \mathbb{F}_3^a \longrightarrow \mathbb{F}_3$ is the j-th projection. Since $g_i \ker(\varphi_i) = \bigcap_{j=1}^{a} g_i \ker(\varphi_{i,j})$, we have

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

Hence it suffices to show that

$$\bigcup_{i=1}^{4} g_i \ker(\varphi_{i,j_i}) \neq G$$

for some tuple $(j_1, j_2, j_3, j_4) \in \{1, \ldots, a\}^4$. Therefore we may assume without loss of generality that $a = 1$.

First, we suppose that $\dim_{\mathbb{F}_3}(\mathbb{F}_3\varphi_1 + \mathbb{F}_3\varphi_2 + \mathbb{F}_3\varphi_3 + \mathbb{F}_3\varphi_4) = 4$. Then the group homomorphism

$$G \longrightarrow \mathbb{F}_3^4;\ g \mapsto (\varphi_1(g), \varphi_2(g), \varphi_3(g), \varphi_4(g))$$

is surjective. Moreover, its kernel is contained in $\ker(\varphi_i)$ for each $i \in \{1,2,3,4\}$, and hence we may assume that $G = \mathbb{F}_3^4$ and $\varphi_i = \mathrm{pr}_i$ for any $i \in \{1,2,3,4\}$. In this case, an explicit calculation shows that

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

Next, we 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 $\varphi_4 \in \mathbb{F}_3\varphi_1 + \mathbb{F}_3\varphi_2 + \mathbb{F}_3\varphi_3$. In this case, the group homomorphism

$$G \longrightarrow \mathbb{F}_3^3;\ g \mapsto (\varphi_1(g), \varphi_2(g), \varphi_3(g))$$

is surjective. Since $\varphi_4 \in \mathbb{F}_3\varphi_1 + \mathbb{F}_3\varphi_2 + \mathbb{F}_3\varphi_3$, the kernel of this surjection is contained in $\ker(\varphi_i)$ for any $i \in \{1,2,3,4\}$, and hence we may assume that $G = \mathbb{F}_3^3$ and $\varphi_i = \mathrm{pr}_i$ for each $i \in \{1,2,3\}$. Since $G = \mathbb{F}_3^3$, we write the group operation additively. We then have

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

It is easy to see that the set

$$-g_4 + \{(h_1,h_2,h_3) \in \mathbb{F}_3^3 \mid \mathrm{pr}_i(g_i) \neq h_i \text{ for any } 1 \leq i \leq 3\}$$

contains a $\mathbb{F}_3$-basis of $\mathbb{F}_3^3$. Since $\varphi_4 \neq 0$, this fact shows that

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

which completes the proof. □

Lemma 5.2. *Let $c_1, c_2, c_3, c_4 \in H^1(K, \overline{T})$ be non-zero elements. Suppose that*

$$\dim_{\mathbb{F}_3}(\mathbb{F}_3 c_1 + \mathbb{F}_3 c_2 + \mathbb{F}_3 c_3 + \mathbb{F}_3 c_4) \geq 3.$$

Then there are infinitely many primes $\mathfrak{q} \in \mathcal{P}$ such that $\mathrm{loc}_{\mathfrak{q}}(c_i) \neq 0$ for any $1 \leq i \leq 4$.

Remark 5.3. When $\mathbb{F} = \mathbb{F}_3$ and $\dim_{\mathbb{F}_3}(\mathbb{F}_3 c_1 + \mathbb{F}_3 c_2 + \mathbb{F}_3 c_3 + \mathbb{F}_3 c_4) = 2$, the conclusion of Lemma 5.2 is not valid. In fact, if we have $c_3 = c_1 + c_2$ and $c_4 = c_1 - c_2$, then at least one of the elements among the set $\{\mathrm{loc}_{\mathfrak{q}}(c_1), \mathrm{loc}_{\mathfrak{q}}(c_2), \mathrm{loc}_{\mathfrak{q}}(c_3), \mathrm{loc}_{\mathfrak{q}}(c_4)\}$ is zero for all but finitely many primes $\mathfrak{q} \in \mathcal{P}$, since $H^1_{\mathrm{ur}}(K_{\mathfrak{q}}, \overline{T}) \cong \overline{T}/(\mathrm{Fr}_{\mathfrak{q}} - 1)\overline{T} \cong \mathbb{F} = \mathbb{F}_3$.

Remark 5.4. Lemma 5.2 is only used to prove Corollary 5.5 and Lemma 6.4.

Proof. The proof of this lemma is almost identical to the proof of [17, Proposition 3.6.1]. Since our setting is different from that of [17], we record its proof here.

Recall that $\tau \in G_{\mathcal{H}_\alpha}$ is an element satisfying $T/(\tau - 1)T \cong R$. Put $F := \mathcal{H}_\alpha(T)$. Since we assume that

$$H^1(F/K, \overline{T}) = 0,$$

the restriction map induces an injection

$$H^1(K, \overline{T}) \hookrightarrow H^1(F, \overline{T})^{G_K} = \mathrm{Hom}(G_F, \overline{T})^{G_K}.$$

Since $\overline{T}$ is an irreducible G_K-module, the map

$$\mathrm{Hom}(G_F, \overline{T})^{G_K} \hookrightarrow \mathrm{Hom}(G_F, \overline{T}/(\tau - 1)\overline{T}) \tag{5.1}$$

is injective. Let $\bar{c}_i \in \mathrm{Hom}(G_F, \overline{T}/(\tau - 1)\overline{T})$ denote the image of c_i under the injection (5.1). We also put

$$H_i := \{g \in G_F \mid c_i(\tau g) = 0 \text{ in } \overline{T}/(\tau - 1)\overline{T}\}.$$

As mentioned in the proof of [17, Proposition 3.6.1], the value $c_i(\tau g)$ mod $(\tau - 1)\overline{T}$ is well-defined since $g \in G_F$ acts trivially on $\overline{T}$. Note that any representative $\widetilde{c}_i$ of c_i satisfies the cocycle condition, that is, $\widetilde{c}_i(g_1 g_2) = g_1 \widetilde{c}(g_2) + \widetilde{c}(g_1)$. Hence we see that there is an element $g_i \in G_F$ such that $H_i \subset g_i \ker(\bar{c}_i)$.

Since the map (5.1) is injective, we have

$$\dim_{\mathbb{F}_3} (\mathbb{F}_3\bar{c}_1 + \mathbb{F}_3\bar{c}_2 + \mathbb{F}_3\bar{c}_3 + \mathbb{F}_3\bar{c}_4) \geq 3$$

by assumption. Hence Lemma 5.1 shows that there is an element

$$g \in G_F \setminus (g_1 \ker(\bar{c}_1) \cup g_2 \ker(\bar{c}_2) \cup g_3 \ker(\bar{c}_3) \cup g_4 \ker(\bar{c}_4)).$$

For each integer $1 \leq i \leq 4$, we put $F_i := \overline{F}^{\ker(c_i)}$. Note that F/K is a Galois extension since $c_i \in \mathrm{Hom}(G_F, \overline{T})^{G_K}$. Let S be the set of primes of K whose Frobenius conjugacy class in $\mathrm{Gal}(F_1F_2F_3F_4/K)$ is the class of τg. Note that for any prime $\mathfrak{q} \in S$, we have

$$H^1_{\mathrm{ur}}(K_{\mathfrak{q}}, \overline{T}) \cong \overline{T}/(\mathrm{Fr}_{\mathfrak{q}} - 1)\overline{T} = \overline{T}/(\tau - 1)\overline{T} \cong \mathbb{F}.$$

Hence S is an infinite set and $\mathrm{loc}_{\mathfrak{q}}(c_i) \neq 0$ for any $1 \leq i \leq 4$ and $\mathfrak{q} \in S$. Since the image of τg in $\mathrm{Gal}(\mathcal{H}_\alpha/K)$ is trivial, we have $(S \setminus S(\mathcal{F})) \subset \mathcal{P}$. □

Corollary 5.5. *Let $c_1, c_2, c_3 \in H^1(K, \overline{T})$ be non-zero elements. Then there are infinitely many primes $\mathfrak{q} \in \mathcal{P}$ satisfying $\mathrm{loc}_{\mathfrak{q}}(c_i) \neq 0$ for any $1 \leq i \leq 3$.*

Proof. First, we note that $\dim_{\mathbb{F}_3}(H^1(K, \overline{T})) = \infty$. Hence, when

$$\dim_{\mathbb{F}_3} (\mathbb{F}_3 c_1 + \mathbb{F}_3 c_2 + \mathbb{F}_3 c_3) \geq 2,$$

there exists an element $c \in H^1(K, \overline{T})$ satisfying

$$\dim_{\mathbb{F}_3} (\mathbb{F}_3 c_1 + \mathbb{F}_3 c_2 + \mathbb{F}_3 c_3 + \mathbb{F}_3 c) \geq 3.$$

When $\dim_{\mathbb{F}_3}(\mathbb{F}_3c_1 + \mathbb{F}_3c_2 + \mathbb{F}_3c_3) = 1$, we may assume, without loss, that $c_1 = c_2 = c_3$. One can take elements $c, c' \in H^1(K, \overline{T})$ such that

$$\dim_{\mathbb{F}_3}(\mathbb{F}_3c_1 + \mathbb{F}_3c + \mathbb{F}_3c') = 3.$$

The corollary follows from Lemma 5.2. □

6. Connectedness of the graph $\mathcal{X}^0$

Throughout this section, suppose that

- $\mathcal{F}$ is cartesian with $\chi(\mathcal{F}) = 1$ and residually coisotropic.

Following [17, Definition 4.3.6], we define the graph $\mathcal{X}^0 := \mathcal{X}^0(\mathcal{F})$ as follows:

- the vertices of $\mathcal{X}^0$ are square-free ideals $\mathfrak{d} \in \mathcal{N}$ with $\lambda^*(\mathfrak{d}) = 0$,
- for any vertices $\mathfrak{d}, \mathfrak{d}\mathfrak{q} \in \mathcal{X}^0$ with $\mathfrak{q} \in \mathcal{P}$, we join $\mathfrak{d}$ and $\mathfrak{d}\mathfrak{q}$ by an edge in $\mathcal{X}^0$ if and only if $H^1_{\overline{\mathcal{F}}(\mathfrak{d})}(K, \overline{T}) \neq H^1_{\overline{\mathcal{F}}_{\mathfrak{q}}(\mathfrak{d})}(K, \overline{T})$.

In this section, we prove the connectedness of the graph $\mathcal{X}^0$ which is one of the most important facts in the theory of Kolyvagin systems. In the case that $\mathrm{char}(\mathbb{F}) = p \geq 5$ or $\mathrm{Hom}_{\mathbb{F}_p[G_K]}(\overline{T}, \overline{T}^\vee(1)) = 0$, this fact is proved by Mazur and Rubin in [17, Theorem 4.3.12].

The following lemma follows easily from Theorem 3.1.

Lemma 6.1. *Let $\mathfrak{d} \in \mathcal{N}$ be a square-free ideal and $\mathfrak{q} \in \mathcal{P}$ a prime with $\mathfrak{q} \nmid \mathfrak{d}$. Then the following claims are valid.*

(1) $|\lambda(\mathfrak{d}) - \lambda(\mathfrak{d}\mathfrak{q})| \leq 1$.
(2) $|\lambda^*(\mathfrak{d}) - \lambda^*(\mathfrak{d}\mathfrak{q})| \leq 1$. *In particular* $\nu(\mathfrak{d}) \geq \lambda^*(1)$ *if* $\lambda^*(\mathfrak{d}) = 0$.
(3) *If* $H^1_{\overline{\mathcal{F}}(\mathfrak{d})}(K, \overline{T}) \neq H^1_{\overline{\mathcal{F}}_{\mathfrak{q}}(\mathfrak{d})}(K, \overline{T})$, *then* $\lambda^*(\mathfrak{d}\mathfrak{q}) \leq \lambda^*(\mathfrak{d})$.
(4) *If* $H^1_{\overline{\mathcal{F}}^*(\mathfrak{d})}(K, \overline{T}) \neq H^1_{(\overline{\mathcal{F}}^*)_{\mathfrak{q}}(\mathfrak{d})}(K, \overline{T})$, *then* $\lambda(\mathfrak{d}\mathfrak{q}) = \lambda(\mathfrak{d}) - 1$ *and* $\lambda^*(\mathfrak{d}\mathfrak{q}) = \lambda^*(\mathfrak{d}) - 1$.

Proof. Claims (1) and (2) follow from [17, Lemma 4.1.7 (i)].

Suppose that $H^1_{\overline{\mathcal{F}}(\mathfrak{d})}(K, \overline{T}) \neq H^1_{\overline{\mathcal{F}}_{\mathfrak{q}}(\mathfrak{d})}(K, \overline{T})$. Since $H^1_{\mathrm{ur}}(K_{\mathfrak{q}}, \overline{T}) \cong \mathbb{F}$, applying Theorem 3.1 with $\mathcal{F}_1 = \overline{\mathcal{F}}_{\mathfrak{q}}(\mathfrak{d})$ and $\mathcal{F}_2 = \overline{\mathcal{F}}(\mathfrak{d})$, we see that

$$H^1_{\overline{\mathcal{F}}^*(\mathfrak{d})}(K, \overline{T}) = H^1_{(\overline{\mathcal{F}}^*)^{\mathfrak{q}}(\mathfrak{d})}(K, \overline{T}) \supset H^1_{\overline{\mathcal{F}}^*(\mathfrak{d}\mathfrak{q})}(K, \overline{T}),$$

which implies claim (3).

Since $\mathcal{F}$ is residually coisotropic, the assumption that $H^1_{\overline{\mathcal{F}}^*(\mathfrak{d})}(K, \overline{T}) \neq H^1_{(\overline{\mathcal{F}}^*)_{\mathfrak{q}}(\mathfrak{d})}(K, \overline{T})$ proves that $H^1_{\overline{\mathcal{F}}(\mathfrak{d})}(K, \overline{T}) \neq H^1_{\overline{\mathcal{F}}_{\mathfrak{q}}(\mathfrak{d})}(K, \overline{T})$. Hence claim (4) follows from [17, Lemma 4.1.7 (iv)]. □

The following two lemmas follow from exactly the same arguments as in [17, Lemma 4.3.9] and [17, Proposition 4.3.10], respectively. In the proofs of these propositions, [17, Proposition 3.6.1] is used, which does not hold true in our case. However, the arguments are still valid if we use Corollary 5.5 instead of [17, Proposition 3.6.1].

Lemma 6.2 ([17, Lemma 4.3.9])**.** *For any vertices $\mathfrak{d}, \mathfrak{d}\mathfrak{q} \in \mathcal{X}^0$ with $\mathfrak{q} \in \mathcal{P}$, there is a path in $\mathcal{X}^0$ from $\mathfrak{d}$ to $\mathfrak{d}\mathfrak{q}$.*

Lemma 6.3 ([17, Proposition 4.3.10])**.** *For any vertex $\mathfrak{d} \in \mathcal{X}^0$ with $\nu(\mathfrak{d}) > \lambda^*(1)$, there is a vertex $\mathfrak{e} \in \mathcal{X}^0$ with $\nu(\mathfrak{e}) < \nu(\mathfrak{d})$ such that there is a path in $\mathcal{X}^0$ from $\mathfrak{d}$ to $\mathfrak{e}$.*

Lemma 6.4. *For each integer $i \in \{1, 2\}$, we take a vertex $\mathfrak{d}_i \in \mathcal{X}^0$ and a prime $\mathfrak{q}_i \in \mathcal{P}$ satisfying $\mathfrak{q}_i \mid \mathfrak{d}_i$. Suppose that $\nu(\mathfrak{d}_1) = \nu(\mathfrak{d}_2) = \lambda^*(1)$ and $\mathfrak{q}_1 \neq \mathfrak{q}_2$.*

Then there are infinitely many primes $\mathfrak{q} \in \mathcal{P}$ with $\mathfrak{q} \nmid \mathfrak{d}_1\mathfrak{d}_2$ such that there is a path in $\mathcal{X}^0$ from $\mathfrak{d}_i$ to $\mathfrak{d}_i\mathfrak{q}/\mathfrak{q}_i$ for each integer $1 \leq i \leq 2$.

Remark 6.5. In the case that $\mathrm{char}(\mathbb{F}) = p \geq 5$ or $\mathrm{Hom}_{\mathbb{F}_p[G_K]}(\overline{T}, \overline{T}^\vee(1)) = 0$, this lemma is proved by Mazur and Rubin (see the proof of [17, Proposition 4.3.11]). However, in their proof, they takes advantage of the existence of a localization map that simultaneously maps any four non-zero cohomology classes to non-zero elements ([17, Proposition 3.6.1]). As explained in Remark 5.3, this fact does not hold true in our case.

Proof. Take an integer $i \in \{1, 2\}$ and put $\mathfrak{e}_i = \mathfrak{d}_i/\mathfrak{q}_i$. Since $\nu(\mathfrak{e}_i) = \nu(\mathfrak{d}_i) - 1 = \lambda^*(1) - 1$ and $\lambda^*(\mathfrak{d}_i) = 0$, Lemma 6.1 (2) and the fact that $\lambda(\mathfrak{e}_i) - \lambda^*(\mathfrak{e}_i) = 1$ show that

$$\lambda(\mathfrak{e}_i) = 2 \quad \text{and} \quad \lambda^*(\mathfrak{e}_i) = 1.$$

By the coisotropy $\overline{\mathcal{F}}^* \subset \overline{\mathcal{F}}$, we have

$$H^1_{\overline{\mathcal{F}}^*(\mathfrak{e}_i)}(K, \overline{T}) \subset H^1_{\overline{\mathcal{F}}(\mathfrak{e}_i)}(K, \overline{T}).$$

By [17, Lemma 4.1.6 (iii)], we have

$$\dim_{\mathbb{F}}\Big(H^1_{\overline{\mathcal{F}}^{\mathfrak{q}_i}(\mathfrak{e}_i)}(K, \overline{T})/H^1_{\overline{\mathcal{F}}(\mathfrak{e}_i)}(K, \overline{T})\Big) + \dim_{\mathbb{F}}\Big(H^1_{\overline{\mathcal{F}}^*(\mathfrak{e}_i)}(K, \overline{T})/H^1_{\overline{\mathcal{F}}^*_{\mathfrak{q}_i}(\mathfrak{e}_i)}(K, \overline{T})\Big) = 1.$$

The facts that $\lambda^*(\mathfrak{e}_i) = 1$ and $\lambda^*(\mathfrak{d}_i) = 0$ imply that $H^1_{\overline{\mathcal{F}}^{\mathfrak{q}_i}(\mathfrak{e}_i)}(K, \overline{T}) = H^1_{\overline{\mathcal{F}}(\mathfrak{e}_i)}(K, \overline{T})$. In particular,

$$H^1_{\overline{\mathcal{F}}(\mathfrak{d}_i)}(K, \overline{T}) \subset H^1_{\overline{\mathcal{F}}(\mathfrak{e}_i)}(K, \overline{T}).$$

Since $\lambda^*(\mathfrak{d}_i) = 0$, we have

$$H^1_{\overline{\mathcal{F}}^*(\mathfrak{e}_i)}(K, \overline{T}) \cap H^1_{\overline{\mathcal{F}}(\mathfrak{d}_i)}(K, \overline{T}) \subset H^1_{\overline{\mathcal{F}}^*(\mathfrak{d}_i)}(K, \overline{T}) = 0.$$

Hence the facts that $\lambda(\mathfrak{e}_i) = 2$ and $\lambda(\mathfrak{d}_i) = \lambda^*(\mathfrak{e}_i) = 1$ show that

$$H^1_{\overline{\mathcal{F}}(\mathfrak{e}_i)}(K, \overline{T}) = H^1_{\overline{\mathcal{F}}(\mathfrak{d}_i)}(K, \overline{T}) \oplus H^1_{\overline{\mathcal{F}}^*(\mathfrak{e}_i)}(K, \overline{T}).$$

Take non-zero elements $c_1^{(i)} \in H^1_{\overline{\mathcal{F}}(\mathfrak{d}_i)}(K, \overline{T})$ and $c_2^{(i)} \in H^1_{\overline{\mathcal{F}}^*(\mathfrak{e}_i)}(K, \overline{T})$. Let us show that there are infinitely many primes $\mathfrak{q} \in \mathcal{P}$ such that $\mathrm{loc}_{\mathfrak{q}}(c_j^{(i)}) \neq 0$ for any $i, j \in \{1, 2\}$. If $c_2^{(2)} \notin H^1_{\overline{\mathcal{F}}(\mathfrak{e}_1)}(K, \overline{T})$, then the existence of such primes $\mathfrak{q} \in \mathcal{P}$ follows from Lemma 5.2 since

$$\dim_{\mathbb{F}_3}\left(\mathbb{F}_3 c_1^{(1)} + \mathbb{F}_3 c_2^{(1)} + \mathbb{F}_3 c_1^{(2)} + \mathbb{F}_3 c_2^{(2)}\right) \geq 3.$$

Suppose that $c_2^{(2)} \in H^1_{\mathcal{F}(\mathfrak{e}_1)}(K, \overline{T})$, that is, $c_2^{(2)} = ac_1^{(1)} + bc_2^{(1)}$ for some $a, b \in \mathbb{F}$. Take a prime $\mathfrak{r} \in E(\mathcal{F})$. Then by the choice of $c_2^{(1)}$ and $c_2^{(2)}$, we have

$$\mathrm{loc}_{\mathfrak{r}}(c_2^{(1)}) = 0 = \mathrm{loc}_{\mathfrak{r}}(c_2^{(2)}).$$

In particular, $0 = \mathrm{loc}_{\mathfrak{r}}(c_2^{(1)}) = \mathrm{loc}_{\mathfrak{r}}(ac_1^{(1)} + bc_2^{(1)}) = \mathrm{loc}_{\mathfrak{r}}(ac_1^{(1)})$. Moreover, Lemma 3.11 shows that $\mathrm{loc}_{\mathfrak{r}}(c_1^{(1)}) \neq 0$ and hence

$$a = 0.$$

Therefore, we may assume that $c_2^{(1)} = c_2^{(2)}$. Then by Corollary 5.5, there are infinitely many primes $\mathfrak{q} \in \mathcal{P}$ such that $\mathrm{loc}_{\mathfrak{q}}(c_j^{(i)}) \neq 0$ for any $i, j \in \{1, 2\}$.

Let us prove that the primes $\mathfrak{q}$ are the desired ones. Lemma 6.1 (3) and the fact that $\mathrm{loc}_{\mathfrak{q}}(c_1^{(i)}) \neq 0$ imply $0 \leq \lambda^*(\mathfrak{d}_i\mathfrak{q}) \leq \lambda^*(\mathfrak{d}_i) = 0$, that is, $\mathfrak{d}_i\mathfrak{q} \in \mathcal{X}^0$. Since $\mathrm{loc}_{\mathfrak{q}}(c_2^{(i)}) \neq 0$, we have

$$H^1_{\overline{\mathcal{F}}^*_{\mathfrak{q}}(\mathfrak{e}_i)}(K, \overline{T}) \neq H^1_{\overline{\mathcal{F}}^*(\mathfrak{e}_i)}(K, \overline{T}).$$

Hence Lemma 6.1 (4) shows that $\lambda^*(\mathfrak{e}_i\mathfrak{q}) = \lambda^*(\mathfrak{e}_i) - 1 = 0$, that is, $\mathfrak{e}_i\mathfrak{q} \in \mathcal{X}^0$. Since $\mathfrak{d}_i, \mathfrak{d}_i\mathfrak{q}, \mathfrak{e}_i\mathfrak{q} \in \mathcal{X}^0$, Lemma 6.2 shows that there is a path in $\mathcal{X}^0$ from $\mathfrak{d}_i$ to $\mathfrak{e}_i\mathfrak{q}$. □

Corollary 6.6. *For any vertices $\mathfrak{d}_1, \mathfrak{d}_2 \in \mathcal{X}^0$ satisfying $\nu(\mathfrak{d}_1) = \nu(\mathfrak{d}_2) = \lambda^*(1)$, there is a path in $\mathcal{X}^0$ from $\mathfrak{d}_1$ to $\mathfrak{d}_2$.*

Proof. Using Lemma 6.4, this proposition can be proved by exactly the same induction argument with respect to $\lambda^*(1) - \nu(\gcd(\mathfrak{d}_1, \mathfrak{d}_2))$ as in the proof of [17, Proposition 4.3.11]. □

Since $\lambda^*(1) \leq \nu(\mathfrak{d})$ for any vertex $\mathfrak{d} \in \mathcal{X}^0$, Lemma 6.3 and Corollary 6.6 imply the connectedness of the graph $\mathcal{X}^0$:

Theorem 6.7. *The graph $\mathcal{X}^0$ is connected.*

7. Proof of main theorem

As in the previous section, we assume that $\mathcal{F}$ is cartesian with $\chi(\mathcal{F}) = 1$ and residually coisotropic.

7.1. Stark systems. In this subsection, using Stark systems, we prove the surjectivity of the R-homomorphism

$$\mathrm{KS}_1(T, \mathcal{F}) \longrightarrow H^1_{\mathcal{F}(\mathfrak{d})}(K, T) \otimes_{\mathbb{Z}} G_{\mathfrak{d}}$$

for any square-free ideal $\mathfrak{d} \in \mathcal{N}$ with $\lambda^*(\mathfrak{d}) = 0$ (which is part of Theorem 4.4(1)).

For any R-module M and integer $r \geq 0$, we define

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

Since R is an injective R-module, the R-dual functor $M \mapsto M^*$ is exact. Hence, an R-homomorphism $\phi\colon M \longrightarrow F$, where F is a free R-module of rank $s \leq r$, induces a natural R-homomorphism

$$\phi^{(r)}\colon \bigcap\nolimits^r_R M \longrightarrow \det(F) \otimes_R \bigcap\nolimits^{r-s}_R \ker(\phi).$$

Namely, $\phi^{(r)}$ is the R-dual of the R-homomorphism

$$\det(F^*) \otimes_R \bigwedge\nolimits^r_R \ker(\phi)^* \longrightarrow \bigwedge\nolimits^{r+1}_R M^*$$

defined by $f^* \otimes (x_1^* \wedge \cdots \wedge x_r^*) \mapsto f^* \wedge \widetilde{x}_1^* \wedge \cdots \wedge \widetilde{x}_r^*$, where $\widetilde{x}_r^*$ is a lift of x_r with respect to the surjection $M^* \longrightarrow \ker(\phi)^*$.

Definition 7.1. For any square-free ideal $\mathfrak{d} \in \mathcal{N}$ and $r \geq 0$, we set

$$W_{\mathfrak{d}} := \bigoplus_{\mathfrak{q} \mid \mathfrak{d}} H^1_{/\mathrm{ur}}(K_{\mathfrak{q}}, T)^*,$$

$$X^r_{\mathfrak{d}}(T, \mathcal{F}) := \bigcap\nolimits^{r+\nu(\mathfrak{d})}_R H^1_{\mathcal{F}^{\mathfrak{d}}}(K, T) \otimes_R \det(W_{\mathfrak{d}}).$$

For any divisor $\mathfrak{e}$ of $\mathfrak{d}$, the exact sequence of R-modules

$$0 \longrightarrow H^1_{\mathcal{F}^{\mathfrak{e}}}(K, T) \longrightarrow H^1_{\mathcal{F}^{\mathfrak{d}}}(K, T) \longrightarrow \bigoplus_{\mathfrak{q} \mid \frac{\mathfrak{d}}{\mathfrak{e}}} H^1_{/\mathrm{ur}}(K_{\mathfrak{q}}, T)$$

induces a natural R-homomorphism

$$\bigcap\nolimits^{r+\nu(\mathfrak{d})}_R H^1_{\mathcal{F}^{\mathfrak{d}}}(K, T) \longrightarrow \bigcap\nolimits^{r+\nu(\mathfrak{e})}_R H^1_{\mathcal{F}^{\mathfrak{e}}}(K, T) \otimes_R \det(W^*_{\mathfrak{d}/\mathfrak{e}})$$

as described earlier. Hence we obtain an R-homomorphism

$$\Phi_{\mathfrak{d},\mathfrak{e}}\colon X^r_{\mathfrak{d}}(T, \mathcal{F}) \longrightarrow X^r_{\mathfrak{e}}(T, \mathcal{F})$$

(see [22, Definition 2.3]). If $\mathfrak{f} \mid \mathfrak{e} \mid \mathfrak{d}$, then we see that $\Phi_{\mathfrak{d},\mathfrak{f}} = \Phi_{\mathfrak{e},\mathfrak{f}} \circ \Phi_{\mathfrak{d},\mathfrak{e}}$ (see [22, Proposition 2.4]), and we can define the module of Stark systems of rank r to be

$$\mathrm{SS}_r(T,\mathcal{F}) := \varprojlim_{\mathfrak{d}\in\mathcal{N}} X^r_{\mathfrak{d}}(T,\mathcal{F}).$$

Theorem 7.2. *For any square-free ideal* $\mathfrak{d} \in \mathcal{N}$ *with* $H^1_{(\mathcal{F}^*)_{\mathfrak{d}}}(K,T) = 0$, *the projection map*

$$\mathrm{SS}_1(T,\mathcal{F}) \longrightarrow X^1_{\mathfrak{d}}(T,\mathcal{F})$$

is an isomorphism. In particular, the R*-module* $\mathrm{SS}_1(T,\mathcal{F})$ *is free of rank* 1.

Proof. Since we assume that $\mathcal{F}$ is cartesian with $\chi(\mathcal{F}) = 1$, the first assertion follows from [22, Theorem 4.7]. As $\chi(\mathcal{F}) = 1$, the R-module $H^1_{\mathcal{F}^{\mathfrak{d}}}(K,T)$ is free of rank $1+\nu(\mathfrak{d})$ by Lemma 3.7 (2) and the R-module $X^1_{\mathfrak{d}}(T,\mathcal{F})$ is free of rank 1. The latter assertion follows from this fact. □

Since we have two R-isomorphisms

$$\phi^{\mathrm{fs}}_{\mathfrak{q}} \colon H^1_{\mathrm{ur}}(K_{\mathfrak{q}},T) \xrightarrow{\sim} H^1_{/\mathrm{ur}}(K_{\mathfrak{q}},T) \otimes_{\mathbb{Z}} G_{\mathfrak{q}} \quad \text{and} \quad H^1_{\mathrm{ur}}(K_{\mathfrak{q}},T) \xrightarrow{\sim} H^1_{/\mathrm{tr}}(K_{\mathfrak{q}},T)$$

for each prime $\mathfrak{q} \mid \mathfrak{d}$, we obtain the exact sequence of R-modules

$$0 \longrightarrow H^1_{\mathcal{F}(\mathfrak{d})}(K,T) \longrightarrow H^1_{\mathcal{F}^{\mathfrak{d}}}(K,T) \longrightarrow \bigoplus_{\mathfrak{q}\mid\mathfrak{d}} H^1_{/\mathrm{tr}}(K_{\mathfrak{q}},T) \cong \bigoplus_{\mathfrak{q}\mid\mathfrak{d}} H^1_{/\mathrm{ur}}(K_{\mathfrak{q}},T) \otimes_{\mathbb{Z}} G_{\mathfrak{q}},$$

and this exact sequence induces a natural R-homomorphism

$$\Pi_{\mathfrak{d}} \colon X^1_{\mathfrak{d}}(T,\mathcal{F}) \longrightarrow {\textstyle\bigcap}^1_R H^1_{\mathcal{F}(\mathfrak{d})}(K,T) \otimes_{\mathbb{Z}} G_{\mathfrak{d}} = H^1_{\mathcal{F}(\mathfrak{d})}(K,T) \otimes_{\mathbb{Z}} G_{\mathfrak{d}}.$$

Moreover, Burns and Sano showed in [2, Proposition 4.3] (see also [18, Proposition 12.3]) that for any Stark system $(\epsilon_{\mathfrak{d}})_{\mathfrak{d}\in\mathcal{N}} \in \mathrm{SS}_1(T,\mathcal{F})$, we have

$$\mathrm{Reg}_1((\epsilon_{\mathfrak{d}})_{\mathfrak{d}\in\mathcal{N}}) := ((-1)^{\nu(\mathfrak{d})}\Pi_{\mathfrak{d}}(\epsilon_{\mathfrak{d}}))_{\mathfrak{d}\in\mathcal{N}} \in \mathrm{KS}_1(T,\mathcal{F}).$$

Proposition 7.3.

(1) *The* R*-homomorphism* Reg_1 *is injective*

(2) *For any square-free ideal* $\mathfrak{d} \in \mathcal{N}$ *with* $\lambda^*(\mathfrak{d}) = 0$, *the* R*-homomorphism* $\mathrm{KS}_1(T,\mathcal{F}) \longrightarrow H^1_{\mathcal{F}(\mathfrak{d})}(K,T) \otimes_{\mathbb{Z}} G_{\mathfrak{d}}$ *is surjective.*

Proof. Note that by the definition of the R-homomorphism Reg_1, for any square-free ideal $\mathfrak{d} \in \mathcal{N}$, we have the commutative diagram

$$\begin{array}{ccc} \mathrm{SS}_1(T,\mathcal{F}) & \longrightarrow & X^1_{\mathfrak{d}}(T,\mathcal{F}) \\ \downarrow{\scriptstyle \mathrm{Reg}_1} & & \downarrow{\scriptstyle (-1)^{\nu(\mathfrak{d})}\Pi_{\mathfrak{d}}(\epsilon_{\mathfrak{d}})} \\ \mathrm{KS}_1(T,\mathcal{F}) & \longrightarrow & H^1_{\mathcal{F}(\mathfrak{d})}(K,T) \otimes_{\mathbb{Z}} G_{\mathfrak{d}}. \end{array} \tag{7.1}$$

If $\lambda^*(\mathfrak{d}) = 0$, then $H^1_{\mathcal{F}^*(\mathfrak{d})}(K, T^\vee(1)) = 0$ by Lemma 3.4. Hence applying Theorem 3.1 with $\mathcal{F}_1 = \mathcal{F}(\mathfrak{d})$ and $\mathcal{F}_2 = \mathcal{F}^{\mathfrak{d}}$, we obtain an exact sequence of R-modules

$$0 \longrightarrow H^1_{\mathcal{F}(\mathfrak{d})}(K,T) \longrightarrow H^1_{\mathcal{F}^{\mathfrak{d}}}(K,T) \longrightarrow \bigoplus_{\mathfrak{q}\mid\mathfrak{d}} H^1_{/\,\mathrm{tr}}(K_{\mathfrak{q}},T) \longrightarrow 0.$$

Moreover, Lemma 3.7 shows the R-modules $H^1_{\mathcal{F}^{\mathfrak{d}}}(K,T)$ and $H^1_{\mathcal{F}(\mathfrak{d})}(K,T)$ are free of rank $1+\nu(\mathfrak{d})$ and 1, respectively. Hence in this case, $\Pi_{\mathfrak{d}}$ is an isomorphism. Therefore, Theorem 7.2 together with the commutative diagram (7.1) shows that Reg_1 is injective and the projection map $\mathrm{KS}_1(T,\mathcal{F}) \longrightarrow H^1_{\mathcal{F}(\mathfrak{d})}(K,T) \otimes_{\mathbb{Z}} G_{\mathfrak{d}}$ is surjective. □

7.2. Proof of Theorem 4.4.

Lemma 7.4. *For any prime $\mathfrak{q} \in \mathcal{P}$, the fixed injection $\overline{T} \hookrightarrow T$ induces an R-isomorphism $H^1_{/\mathrm{ur}}(K_{\mathfrak{q}}, \overline{T}) \xrightarrow{\sim} H^1_{/\mathrm{ur}}(K_{\mathfrak{q}}, T)[\mathfrak{m}_R]$.*

Proof. By the definition of $\mathcal{P}$, we have natural R-isomorphisms

$$H^1_{\mathrm{ur}}(K_{\mathfrak{q}}, \overline{T}) \cong \overline{T}/(\mathrm{Fr}_{\mathfrak{q}} - 1)\overline{T} \cong \mathbb{F} \quad \text{and} \quad H^1_{\mathrm{ur}}(K_{\mathfrak{q}}, T) \cong T/(\mathrm{Fr}_{\mathfrak{q}} - 1)T \cong R.$$

Hence the fixed injection $\overline{T} \hookrightarrow T$ induces an R-isomorphism

$$H^1_{\mathrm{ur}}(K_{\mathfrak{q}}, \overline{T}) \xrightarrow{\sim} H^1_{\mathrm{ur}}(K_{\mathfrak{q}}, T)[\mathfrak{m}_R].$$

This lemma follows from the fact that we have the finite-singlular isomorphisms (see [17, Lemma 1.2.3], and the definition of $\mathcal{P}$ and (H.2))

$$H^1_{\mathrm{ur}}(K_{\mathfrak{q}}, T) \xrightarrow{\sim} H^1_{/\mathrm{ur}}(K_{\mathfrak{q}}, T) \otimes_{\mathbb{Z}} G_{\mathfrak{q}}$$
$$\text{and} \quad H^1_{\mathrm{ur}}(K_{\mathfrak{q}}, \overline{T}) \xrightarrow{\sim} H^1_{/\mathrm{ur}}(K_{\mathfrak{q}}, \overline{T}) \otimes_{\mathbb{Z}} G_{\mathfrak{q}}. \qquad \square$$

Lemma 7.5. *The fixed injection $\overline{T} \hookrightarrow T$ induces an R-isomorphism*

$$\mathrm{KS}_1(\overline{T}, \overline{\mathcal{F}}) \xrightarrow{\sim} \mathrm{KS}_1(T, \mathcal{F})[\mathfrak{m}_R].$$

Proof. This lemma follows from Lemmas 3.7 and 7.4. □

Proposition 7.6 (Theorem 4.4 (1))**.** *Suppose that*

- *T satisfies the hypotheses* (H.1), (H.2), (H.3), *and* (H.SD) *in Section 2,*
- *$\mathcal{F}$ is cartesian with $\chi(\mathcal{F}) = 1$ and residually coisotropic.*

For any square-free ideal $\mathfrak{d} \in \mathcal{N}$ with $\lambda^*(\mathfrak{d}) = 0$, the canonical projection

$$\mathrm{KS}_1(T,\mathcal{F}) \longrightarrow H^1_{\mathcal{F}(\mathfrak{d})}(K,T) \otimes_{\mathbb{Z}} G_{\mathfrak{d}}$$

is an isomorphism. Moreover, the R-homomorphism $\mathrm{Reg}_1 \colon \mathrm{SS}_1(T,\mathcal{F}) \longrightarrow \mathrm{KS}_1(T,\mathcal{F})$ is also an isomorphism.

Proof. Let $\mathfrak{d} \in \mathcal{N}$ be a square-free ideal with $\lambda^*(\mathfrak{d}) = 0$. By Proposition 7.3 and the commutative diagram (7.1), we only need to prove that $\mathrm{KS}_1(T, \mathcal{F}) \longrightarrow H^1_{\mathcal{F}(\mathfrak{d})}(K, T) \otimes_{\mathbb{Z}} G_{\mathfrak{d}}$ is injective. Moreover, by Lemma 7.5, we may assume that $R = \mathbb{F}$ and $T = \overline{T}$. In this case, the connectedness of the graph $\mathcal{X}^0$ implies the injectivity of the $\mathbb{F}$-homomorphism $\mathrm{KS}_1(T, \mathcal{F}) \longrightarrow H^1_{\mathcal{F}(\mathfrak{d})}(K, T) \otimes_{\mathbb{Z}} G_{\mathfrak{d}}$ (see the case 3 in the proof of [17, Theorem 4.4.1] or the proof of [23, Theorem 3.17]). □

Proposition 7.7 (Theorem 4.4 (2))**.** *Suppose that*

- T *satisfies the hypotheses* (H.1), (H.2), (H.3)*, and* (H.SD) *in Section 2,*
- $\mathcal{F}$ *is cartesian with* $\chi(\mathcal{F}) = 1$ *and residually coisotropic.*

For any square-free ideal $\mathfrak{d} \in \mathcal{N}$ *and basis* $(\kappa_{\mathfrak{e}})_{\mathfrak{e} \in \mathcal{N}} \in \mathrm{KS}_1(T, \mathcal{F})$*, we have*

$$I_R(\kappa_{\mathfrak{d}}) = \mathrm{Fitt}^0_R(H^1_{\mathcal{F}^*(\mathfrak{d})}(K, T^\vee(1))^\vee).$$

Proof. By Proposition 7.6, there is a Stark system $(\epsilon_{\mathfrak{e}})_{\mathfrak{e} \in \mathcal{N}} \in \mathrm{SS}_1(T, \mathcal{F})$ such that

$$\mathrm{Reg}_1((\epsilon_{\mathfrak{e}})_{\mathfrak{e} \in \mathcal{N}}) = (\kappa_{\mathfrak{e}})_{\mathfrak{e} \in \mathcal{N}}.$$

Note that, since $(\kappa_{\mathfrak{e}})_{\mathfrak{e} \in \mathcal{N}}$ is a basis of $\mathrm{KS}_1(T, \mathcal{F})$, the Stark system $(\epsilon_{\mathfrak{e}})_{\mathfrak{e} \in \mathcal{N}}$ is also a basis of $\mathrm{SS}_1(T, \mathcal{F})$. By Corollary 5.5, there is a squeare-free ideal $\mathfrak{f} \in \mathcal{N}$ satisfying $\mathfrak{d} \mid \mathfrak{f}$ and $H^1_{(\mathcal{F}^*)_{\mathfrak{f}}}(K, T^\vee(1)) = 0$. Applying Theorem 3.1 with $\mathcal{F}_1 = \mathcal{F}(\mathfrak{d})$ and $\mathcal{F}_2 = \mathcal{F}^{\mathfrak{f}}$, we obtain an exact sequence of R-modules

$$0 \longrightarrow H^1_{\mathcal{F}(\mathfrak{d})}(K, T) \longrightarrow H^1_{\mathcal{F}^{\mathfrak{f}}}(K, T) \longrightarrow U_{\mathfrak{f}/\mathfrak{d}} \oplus T_{\mathfrak{d}} \longrightarrow H^1_{\mathcal{F}^*(\mathfrak{d})}(K, T^\vee(1))^\vee \longrightarrow 0. \tag{7.2}$$

Here $U_{\mathfrak{f}/\mathfrak{d}} := \bigoplus_{\mathfrak{q} \mid \frac{\mathfrak{f}}{\mathfrak{d}}} H^1_{/\mathrm{ur}}(K_{\mathfrak{q}}, T)$ and $T_{\mathfrak{d}} := \bigoplus_{\mathfrak{q} \mid \mathfrak{d}} H^1_{/\mathrm{tr}}(K_{\mathfrak{q}}, T)$. Note that, by Lemma 3.7, the R-modules $H^1_{\mathcal{F}^{\mathfrak{f}}}(K, T)$ and $U_{\mathfrak{f}/\mathfrak{d}} \oplus T_{\mathfrak{d}}$ are free of rank $1 + \nu(\mathfrak{f})$ and $\nu(\mathfrak{f})$, respectively. The R-homomorphism

$$P_{\mathfrak{f},\mathfrak{d}} \colon X^1_{\mathfrak{f}}(T, \mathcal{F}) \longrightarrow H^1_{\mathcal{F}(\mathfrak{d})}(K, T) \otimes_{\mathbb{Z}} G_{\mathfrak{d}}$$

obtained by the exact sequence (7.2) combined with the finite-singular isomorphisms can be decomposed by $P_{\mathfrak{f},\mathfrak{d}} = \Pi_{\mathfrak{d}} \circ \Phi_{\mathfrak{f},\mathfrak{d}}$. Hence by the definition of Stark systems, we have $P_{\mathfrak{f},\mathfrak{d}}(\epsilon_{\mathfrak{f}}) = \Pi_{\mathfrak{d}} \circ \Phi_{\mathfrak{f},\mathfrak{d}}(\epsilon_{\mathfrak{f}}) = \Pi_{\mathfrak{d}}(\epsilon_{\mathfrak{d}}) = (-1)^{\nu(\mathfrak{d})}\kappa_{\mathfrak{d}}$. Since $\epsilon_{\mathfrak{f}}$ is a basis of $X^1_{\mathfrak{f}}(T, \mathcal{F})$ by Theorem 7.2, this proposition follows from [22, Lemma 4.8]. □

8. Kolyvagin systems of rank 0

The author of the present paper developed in the paper [24] the theory of Kolyvagin systems of rank 0 in the same setting that was considered by Mazur and Rubin in [17]. In this section, we briefly explain that the theory of Kolyvagin systems of rank 0 for a residually self-dual Selmer structure works also in our setting.

We first recall the definition of Kolyvagin systems of rank 0 ([24, §5]). In order to define rank 0 Kolyvagin systems, we fix an R-isomorphism

$$H^1_{/\mathrm{ur}}(K_{\mathfrak{q}}, T) \cong R$$

for each prime $\mathfrak{q} \in \mathcal{P}$ (see the isomorphism that appears at the beginning of Section 4). Then we obtain a pair of R-homomorphisms

$$v_{\mathfrak{q}} \colon H^1(K, T) \longrightarrow H^1_{/\mathrm{ur}}(K_{\mathfrak{q}}, T) \cong R,$$
$$\varphi^{\mathrm{fs}}_{\mathfrak{q}} \colon H^1(K, T) \longrightarrow H^1_{/\mathrm{ur}}(K_{\mathfrak{q}}, T) \otimes_{\mathbb{Z}} G_{\mathfrak{q}} \cong R \otimes_{\mathbb{Z}} G_{\mathfrak{q}}$$

(see the homomorphisms that appears just before Definition 4.1).

Definition 8.1 ([24, Definition 5.1])**.** We set

$$\mathcal{M} := \{(\mathfrak{d}, \mathfrak{q}) \in \mathcal{N} \times \mathcal{P} \mid \mathfrak{q} \nmid \mathfrak{d}\}.$$

A Kolyvagin system of rank 0 is an element

$$(\kappa_{\mathfrak{d},\mathfrak{q}})_{(\mathfrak{d},\mathfrak{q}) \in \mathcal{M}} \in \prod_{(\mathfrak{d},\mathfrak{q}) \in \mathcal{M}} H^1_{\mathcal{F}^{\mathfrak{q}}(\mathfrak{d})}(K, T) \otimes_{\mathbb{Z}} G_{\mathfrak{d}}$$

satisfying the following relations for any elements $(\mathfrak{d}, \mathfrak{q}), (\mathfrak{d}, \mathfrak{r}), (\mathfrak{d}\mathfrak{q}, \mathfrak{r}) \in \mathcal{M}$:

$$v_{\mathfrak{q}}(\kappa_{\mathfrak{d}\mathfrak{q},\mathfrak{r}}) = \varphi^{\mathrm{fs}}_{\mathfrak{q}}(\kappa_{\mathfrak{d},\mathfrak{r}}),$$
$$v_{\mathfrak{r}}(\kappa_{\mathfrak{d}\mathfrak{q},\mathfrak{r}}) = -\varphi^{\mathrm{fs}}_{\mathfrak{q}}(\kappa_{\mathfrak{d},\mathfrak{q}}),$$
$$v_{\mathfrak{q}}(\kappa_{1,\mathfrak{q}}) = v_{\mathfrak{r}}(\kappa_{1,\mathfrak{r}}).$$

We write $\mathrm{KS}_0(T, \mathcal{F})$ for the module of Kolyvagin systems of rank 0. For any Kolyvagin system $\kappa := (\kappa_{\mathfrak{d},\mathfrak{q}})_{(\mathfrak{d},\mathfrak{q}) \in \mathcal{M}} \in \mathrm{KS}_0(T, \mathcal{F})$ and square-free ideal $\mathfrak{d} \in \mathcal{N}$, we put

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

Note that $\delta(\kappa)_{\mathfrak{d}}$ does not depend on the choice of the prime $\mathfrak{q} \in \mathcal{P}$ with $\mathfrak{q} \nmid \mathfrak{d}$.

Definition 8.2. We say that the Selmer structure $\mathcal{F}$ is residually self-dual if $\overline{\mathcal{F}} = \overline{\mathcal{F}}^*$, that is, $H^1_{\mathcal{F}}(K_{\mathfrak{q}}, \overline{T}) = H^1_{\mathcal{F}^*}(K_{\mathfrak{q}}, \overline{T})$ for any prime $\mathfrak{q} \in S(\mathcal{F})$.

Remark 8.3. If $\mathcal{F}$ is residually self-dual, then $\chi(\mathcal{F}) = 0$ by definition.

Lemma 8.4. *For any prime $\mathfrak{q} \in \mathcal{P}$, the Selmer structure $\mathcal{F}^{\mathfrak{q}}$ is cartesian with $\chi(\mathcal{F}^{\mathfrak{q}}) = 1$ and residually coisotropic.*

Proof. Since $\overline{\mathcal{F}} = \overline{\mathcal{F}}^*$, we have $(\overline{\mathcal{F}}^{\mathfrak{q}})^* = (\overline{\mathcal{F}}^*)_{\mathfrak{q}} = \overline{\mathcal{F}}_{\mathfrak{q}} \subset \overline{\mathcal{F}}$. By Lemma 3.7 (1), the Selmer structure $\mathcal{F}^{\mathfrak{q}}$ is cartesian with $\chi(\mathcal{F}^{\mathfrak{q}}) = 1$. □

By Lemma 8.4, we can use Theorem 4.4 (or Propositions 7.6 and 7.7) for $\mathcal{F}^{\mathfrak{q}}$. Hence from the same arguments of the proofs of [24, Theorem 5.5, Proposition 5.6, and Theorem 5.8], we obtain the following result:

Theorem 8.5. *Suppose that $\mathcal{F}$ is cartesian and residually self-dual.*

(1) *The R-homomorphism* $\mathrm{Reg}_0\colon \mathrm{SS}_0(T,\mathcal{F}) \longrightarrow \mathrm{KS}_0(T,\mathcal{F})$ *defined in* [24, Lemma 5.4] *is an isomorphism.*

(2) *For any square-free ideal $\mathfrak{d} \in \mathcal{N}$ with $H^1_{(\mathcal{F}^*)_{\mathfrak{q}}(\mathfrak{d})}(K, T^\vee(1)) = 0$, the projection map*

$$\mathrm{KS}_0(T,\mathcal{F}) \longrightarrow H^1_{\mathcal{F}^{\mathfrak{q}}(\mathfrak{d})}(K,T) \otimes_{\mathbb{Z}} R$$

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

(3) *Let $\kappa \in \mathrm{KS}_0(T,\mathcal{F})$ be a basis. For any square-free ideal $\mathfrak{d} \in \mathcal{N}$, we have*

$$I_R(\delta(\kappa)_{\mathfrak{d}}) = \mathrm{Fitt}^0_R(H^1_{\mathcal{F}^*(\mathfrak{d})}(K, T^\vee(1))^\vee).$$

9. Applications

We first note that the set-up in the opening portion of this section is in effect for the entirety of this section.

Let α be a non-negative integer and $K/\mathbb{Q}$ a finite abelian 3-extension. We set

$$R := \mathbb{Z}_3/3^\alpha\mathbb{Z}_3[\mathrm{Gal}(K/\mathbb{Q})],$$

which is a zero dimensional Gorenstein local ring with residue field $\mathbb{F}_3$. Let E be an elliptic curve over $\mathbb{Q}$. Suppose that

- the image of $\rho_{E,3^\infty}\colon G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(T_3(E)) \cong \mathrm{GL}_2(\mathbb{Z}_3)$ contains $\mathrm{SL}_2(\mathbb{Z}_3)$. Here $T_3(E)$ is the 3-adic Tate module associated with the elliptic curve $E_{/\mathbb{Q}}$.

Remark 9.1. Note that by [27, p. 8 and 9], the condition $\mathrm{im}(\rho_{E,3^\infty}) \supset \mathrm{SL}_2(\mathbb{Z}_3)$ is equivalent to that $\mathrm{im}(\rho_{E,9}\colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})) \supset \mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$. We also note that the image of the mod 3 Galois representation $\rho_{E,3}\colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ have been classified by Reverter and Vila in [20] and elliptic curves with surjective mod 3 but not mod 9 representation have been classified by Elkies in [11].

We define an $R[G_{\mathbb{Q}}]$-module T by

$$T := \mathrm{Ind}_{G_K}^{G_{\mathbb{Q}}}(E[3^\alpha]).$$

Note that the residual representation $\overline{T}$ of T is $E[3]$. Then it is easy to see that the assumptions (H.1), (H.2), (H.3), and (H.SD) are satisfied (see the proof of [21, Proposition 3.5.8] for the assumptions (H.2) and (H.3)).

9.1. Canonical Selmer structure.

Definition 9.2. We define the canonical Selmer structure $\mathcal{F}_{\rm can}$ on T to be with the following data:

- $S(\mathcal{F}_{\rm can}) = \{3, \infty\} \cup S_{\rm bad}(E) \cup S_{\rm ram}(K/\mathbb{Q})$,
- $H^1_{\mathcal{F}_{\rm can}}(\mathbb{Q}_\ell, T) = \begin{cases} H^1_{\rm ur}(\mathbb{Q}_\ell, T) & \text{if } \ell \neq 3, \\ H^1(\mathbb{Q}_3, T) & \text{if } \ell = 3. \end{cases}$

Here, $S_{\rm bad}(E)$ is the set of rational primes at which E has bad reduction and $S_{\rm ram}(K/\mathbb{Q})$ is the set of rational primes at which $K/\mathbb{Q}$ is ramified. Note that these conditions are different from those in [17], and this difference is accounted by the Tamagawa numbers (see Lemma 9.3 and [21, Lemma 1.3.5]).

Lemma 9.3. *Suppose that*

- $E(\mathbb{Q}_\ell)[3] = 0$ *for any prime* $\ell \in S_{\rm ram}(K/\mathbb{Q}) \cup \{3\}$,
- *the Tamagawa factor of* $E_{/\mathbb{Q}}$ *at* ℓ *is coprime to* 3 *for any prime* $\ell \in S_{\rm bad}(E)$.

Then $\mathcal{F}_{\rm can}$ *is cartesian with* $\chi(\mathcal{F}_{\rm can}) = 1$ *and residually coisotropic. Moreover,* $E(\mathcal{F}_{\rm can}) = \{3\}$.

Proof. Let ℓ be a rational prime. First, suppose that $\ell \in S_{\rm ram}(K/\mathbb{Q})$ and $\ell \neq 3$. Since $H^0(\mathbb{Q}_\ell, E[3]) = 0$ by assumption, the fact that $E[3] \cong E[3]^\vee(1)$ as $\mathbb{F}_3[G_K]$-modules together with local Tate duality shows that $H^2(\mathbb{Q}_\ell, E[3]) = 0$. Hence, the local Euler characteristic formula implies that

$$\# H^1(\mathbb{Q}_\ell, E[3]) = \# H^0(\mathbb{Q}_\ell, E[3]) \cdot \# H^2(\mathbb{Q}_\ell, E[3]) = 1.$$

Since we have the natural isomorphism $\mathbf{R}\Gamma(\mathbb{Q}_\ell, T) \otimes^{\mathbf{L}}_R \mathbb{F}_3 \xrightarrow{\sim} \mathbf{R}\Gamma(\mathbb{Q}_\ell, E[3])$, we conclude that $H^1(\mathbb{Q}_\ell, T) = 0$. In particular, $\mathcal{F}_{\rm can}$ is cartesian at ℓ, that is, the R-homomorphism $H^1_{/\overline{\mathcal{F}}_{\rm can}}(\mathbb{Q}_\ell, E[3]) \longrightarrow H^1_{/\mathcal{F}_{\rm can}}(\mathbb{Q}_\ell, T)$ is injective, and we have $H^1_{\overline{\mathcal{F}}^*_{\rm can}}(\mathbb{Q}_\ell, E[3]) = H^1_{\overline{\mathcal{F}}_{\rm can}}(\mathbb{Q}_\ell, E[3])$.

We asuume that $\ell = 3$. The same argument for the case where $\ell \in S_{\rm ram}(K/\mathbb{Q})$ and $\ell \neq 3$ yields $H^2(\mathbb{Q}_3, E[3]) = 0$. Since the cohomological dimension of $G_{\mathbb{Q}_3}$ is 2, the natural homomorphism $H^1(\mathbb{Q}_3, T) \longrightarrow H^1(\mathbb{Q}_3, E[3])$ is surjective. Hence $H^1_{\overline{\mathcal{F}}_{\rm can}}(\mathbb{Q}_3, E[3]) = H^1(\mathbb{Q}_3, E[3])$, and $\mathcal{F}_{\rm can}$ is cartesian at 3. Moreover, $H^1_{\overline{\mathcal{F}}^*_{\rm can}}(\mathbb{Q}_3, E[3]) = 0$ and

$$\dim_{\mathbb{F}_3}\Big(H^1_{\overline{\mathcal{F}}_{\rm can}}(\mathbb{Q}_3, E[3])\Big) = \dim_{\mathbb{F}_3}(E[3]) = 2$$

by the local Euler characteristic formula. In particular, $3 \in E(\mathcal{F}_{\rm can})$.

Suppose that $\ell \in S_{\rm bad}(E) \setminus (S_{\rm ram}(K/\mathbb{Q}) \cup \{3\})$. Note that this case relies critically on the triviality of the 3-parts of the Tamagawa numbers.

Since $K/\mathbb{Q}$ is unramified at ℓ, the fact that the cohomological dimension of $\widehat{\mathbb{Z}} \cong \mathrm{Gal}(\mathbb{Q}_\ell^{\mathrm{ur}}/\mathbb{Q}_\ell)$ is 1 imply that

$$H^1_{\overline{\mathcal{F}}_{\mathrm{can}}}(\mathbb{Q}_\ell, E[3]) = H^1_{\mathrm{ur}}(\mathbb{Q}_\ell, E[3]).$$

Hence the proof of [25, Proposition 2.9] shows that $\mathcal{F}_{\mathrm{can}}$ is cartesian at ℓ. Moreover, since $E[3] \cong E[3]^\vee(1)$ as $\mathbb{F}_3[G_{\mathbb{Q}}]$-modules, we have

$$H^1_{\overline{\mathcal{F}}^*_{\mathrm{can}}}(\mathbb{Q}_\ell, E[3]) = H^1_{\mathrm{ur}}(\mathbb{Q}_\ell, E[3])^\perp \supset H^1_{\mathrm{ur}}(\mathbb{Q}_\ell, E[3]),$$

$$\dim_{\mathbb{F}_3}(H^1_{\mathrm{ur}}(\mathbb{Q}_\ell, E[3])) = \dim_{\mathbb{F}_3}(H^0(\mathbb{Q}_\ell, E[3])) = \frac{1}{2}\dim_{\mathbb{F}_3}(H^1(\mathbb{Q}_\ell, E[3])).$$

These facts imply $H^1_{\overline{\mathcal{F}}^*_{\mathrm{can}}}(\mathbb{Q}_\ell, E[3]) = H^1_{\overline{\mathcal{F}}_{\mathrm{can}}}(\mathbb{Q}_\ell, E[3])$. □

Remark 9.4. Under the assumptions in Proposition 9.5, one can show that the dual Selmer module $H^1_{\mathcal{F}^*_{\mathrm{can}}}(\mathbb{Q}, T^\vee(1))$ coincides with the strict 3^α-Selmer group $\mathrm{Sel}_{\mathrm{str}}(K, E[3^\alpha])$ associated with the elliptic curve $E_{/K}$, that is,

$$H^1_{\mathcal{F}^*_{\mathrm{can}}}(\mathbb{Q}, T^\vee(1)) = \ker\left(\mathrm{Sel}(K, E[3^\alpha]) \longrightarrow \bigoplus_{\mathfrak{p}|3} H^1(K_{\mathfrak{p}}, E[3^\alpha])\right),$$

where $\mathfrak{p}$ runs over the primes of K above 3 (see [25, Lemma 2.6 and Remark 2.7]).

Let

$$(z_L^{\mathrm{Kato}})_{L\in\Omega} \in \prod_{L\in\Omega} H^1(L, T_3(E))$$

denote the Kato's Euler system (see [12, Example 13.3]), where Ω is the set of finite abelian extensions of $\mathbb{Q}$ unramified outside $S_{\mathrm{bad}}(E)\setminus\{3\}$. The cohomology class z_K^{Kato} is related to the L-values $L(E, \chi, 1)$ for $\chi\colon \mathrm{Gal}(K/\mathbb{Q}) \longrightarrow \mathbb{C}^\times$ via the dual exponential map (see [12, Theorems 6.6 and 9.7]).

Mazur and Rubin showed in [17, Theorem 3.2.4] that one can construct a Kolyvagin system (of rank 1) from an Euler system. Applying this result to the Kato's Euler system $(z_L^{\mathrm{Kato}})_{L\in\Omega} \in \prod_{L\in\Omega} H^1(L, T_3(E))$, we obtain a Kolyvagin system

$$(\kappa_{\mathfrak{d}}^{\mathrm{Kato}})_{\mathfrak{d}\in\mathcal{N}} \in \mathrm{KS}_1(T, \mathcal{F}_{\mathrm{can}})$$

such that

$$\kappa_1^{\mathrm{Kato}} = z_K^{\mathrm{Kato}} \bmod p^\alpha$$

via the R-isomorphism $H^1(\mathbb{Q}, T) \cong H^1(K, E[p^\alpha])$ induced by the Shapiro's Lemma. Therefore, the main result of the present paper (Theorem 4.4) combined with Lemma 9.3 implies the following proposition.

Proposition 9.5. *Suppose that*

- $E(\mathbb{Q}_\ell)[3] = 0$ *for any prime* $\ell \in S_{\mathrm{ram}}(K/\mathbb{Q}) \cup \{3\}$,
- *the Tamagawa factor of* E *at* ℓ *is coprime to* 3 *for any prime* $\ell \in S_{\mathrm{bad}}(E)$.

Then we have

$$I_R(z_K^{\mathrm{Kato}} \bmod p^\alpha) \subset \mathrm{Fitt}^0_R(\mathrm{Sel}_{\mathrm{str}}(K, E[3^\alpha])^\vee),$$

where $R = \mathbb{Z}_3/3^\alpha\mathbb{Z}_3[\mathrm{Gal}(K/\mathbb{Q})]$.

For notational simplicity, we put

$$\widetilde{R} := \mathbb{Z}_3[\mathrm{Gal}(K/\mathbb{Q})],$$
$$H^1_{\mathcal{F}_{\mathrm{can}}}(K, T_3(E)) := \varprojlim_{\alpha>0} H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbb{Q}, \mathrm{Ind}^{G_\mathbb{Q}}_{G_K}(E[3^\alpha])) \subset H^1(K, T_3(E)).$$

Then we have the ideal $I_{\tilde{R}}(z_K^{\mathrm{Kato}})$ of $\widetilde{R}$ defined by

$$I_{\tilde{R}}(z_K^{\mathrm{Kato}}) = \{ f(z_K^{\mathrm{Kato}}) \mid f \in \mathrm{Hom}_{\tilde{R}}(H^1_{\mathcal{F}_{\mathrm{can}}}(K, T_3(E)), \widetilde{R}) \}.$$

Corollary 9.6. *Suppose that*

- $E(\mathbb{Q}_\ell)[3] = 0$ *for any prime* $\ell \in S_{\mathrm{ram}}(K/\mathbb{Q}) \cup \{3\}$,
- *the Tamagawa factor of* E *at* ℓ *is coprime to* 3 *for any prime* $\ell \in S_{\mathrm{bad}}(E)$.

Then we have

$$I_{\tilde{R}}(z_K^{\mathrm{Kato}}) \subset \mathrm{Fitt}^0_{\tilde{R}}(\mathrm{Sel}_{\mathrm{str}}(K, E[3^\infty])^\vee).$$

Proof. This corollary follows from Proposition 9.5 and Lemma 9.7 below. □

Lemma 9.7. *Let* S *be a complete Gorenstein local ring of Krull dimension 1. Let* $x \in S$ *be a regular element. Put* $S_\beta := S/x^\beta S$ *for each positive integer* $\beta > 0$. *Let* M *be a finitely generated* S*-module and take* $m \in M$. *Let* $m_\beta \in M/x^\beta M$ *be the image of* m *under the natural homomorphism* $M \longrightarrow M/x^\beta M$. *Then we have*

$$I_S(m) = \varprojlim_{\beta>0} I_{S_\beta}(m_\beta).$$

Proof. Since we have a natural homomorphism

$$\mathrm{Hom}_S(M, S) \longrightarrow \mathrm{Hom}_S(M, S_\beta) = \mathrm{Hom}_{S_\beta}(M/x^\beta M, S_\beta),$$

we see that $I_S(m) \subset \varprojlim_{\beta>0} I_{S_\beta}(m_\beta)$. Let us show the opposite inclusion. Since x is a regular element, we have an exact sequence of S-modules

$$0 \longrightarrow S \xrightarrow{\times x^\beta} S \longrightarrow S_\beta \longrightarrow 0.$$

Applying the functor $\mathrm{Hom}_S(M, -)$ to this exact sequence, we obtain an exact sequence of S-modules

$$0 \longrightarrow \mathrm{Hom}_S(M, S) \otimes_S S_\beta \longrightarrow \mathrm{Hom}_S(M/x^\beta M, S_\beta) \longrightarrow \mathrm{Ext}^1_S(M, S)[x^\beta] \longrightarrow 0.$$

Taking the inverse limits, we get an exact sequence of S-modules

$$0 \longrightarrow \mathrm{Hom}_S(M,S) \longrightarrow \varprojlim_{\beta>0} \mathrm{Hom}_S(M/x^\beta M, S_\beta) \longrightarrow \varprojlim_{\beta>0} \mathrm{Ext}^1_S(M,S)[x^\beta],$$

where the transition map $\mathrm{Ext}^1_S(M,S)[x^{\beta+1}] \longrightarrow \mathrm{Ext}^1_S(M,S)[x^\beta]$ is the multiplication by x. Since the S-module $\bigcup_{\beta>0}\mathrm{Ext}^1_S(M,S)[x^\beta]$ is finitely generated, there is a positive integer γ such that

$$\bigcup_{\beta>0}\mathrm{Ext}^1_S(M,S)[x^\beta] = \mathrm{Ext}^1_S(M,S)[x^\gamma].$$

Hence we see that $\varprojlim_{\beta>0}\mathrm{Ext}^1_S(M,S)[x^\beta]=0$ and

$$\mathrm{Hom}_S(M,S) \xrightarrow{\sim} \varprojlim_{\beta>0} \mathrm{Hom}_S(M/x^\beta M, S_\beta).$$

Consider the following commutative diagram

$$\begin{array}{ccc} \mathrm{Hom}_S(M,S) & \xrightarrow{\cong} & \varprojlim_{\beta>0}\mathrm{Hom}_S(M/x^\beta M, S_\beta) \\ \Big\downarrow{\scriptstyle f\mapsto f(m)} & & \Big\downarrow{\scriptstyle (\mathrm{ev}_{m_\beta}\colon f_\beta\mapsto f_\beta(m_\beta))_{\beta>0}} \\ I_S(m) & \longrightarrow & \varprojlim_{\beta>0} I_{S_\beta}(m_\beta). \end{array}$$

The S_β-homomorphism $\mathrm{ev}_{m_\beta}\colon \mathrm{Hom}_S(M/x^\beta M, S_\beta) \longrightarrow I_{S_\beta}(m_\beta)$ is surjective by definition. Since the Krull dimension of S is 1, the S-length of $\ker(\mathrm{ev}_{m_\beta})$ is finite for any $\beta>0$, and hence the family $\{\ker(\mathrm{ev}_{m_\beta})\}_{\beta>0}$ forms a Mittag–Leffler sequence. Therefore the right vertical arrow of the above commutative diagram is indeed surjective, and this fact implies that $I_S(m)=\varprojlim_{\beta>0} I_{S_\beta}(m_\beta)$. □

9.2. Classical Selmer structure.

9.2.1. *Definition of classical Selmer structure.*

Definition 9.8. We define the classical Selmer structure $\mathcal{F}_{\mathrm{cl}}$ on T to be the following data:

- $S(\mathcal{F}_{\mathrm{cl}}) = \{3,\infty\}\cup S_{\mathrm{bad}}(E)$,
- $H^1_{\mathcal{F}_{\mathrm{cl}}}(\mathbb{Q}_\ell,T) = \begin{cases} H^1_{\mathrm{ur}}(\mathbb{Q}_\ell,T) & \text{if } \ell\neq 3, \\ \mathrm{im}\big(E(K\otimes_{\mathbb{Q}}\mathbb{Q}_3)\longrightarrow H^1(\mathbb{Q}_3,T)\big) & \text{if } \ell=3. \end{cases}$

Note that these conditions are different from those in [17, Example 2.1.3], and this difference is accounted by the Tamagawa numbers (see Lemma 9.9 and [21, Lemma 1.3.5]).

Lemma 9.9. *Suppose that*

- *E has a good ordinary reduction at* 3 *and* $E(\mathbb{F}_3)[3]=0$*,*
- $E(\mathbb{Q}_\ell)[3]=0$ *for any prime* $\ell\in S_{\mathrm{bad}}(E)$*,*

- *the Tamagawa factor of $E_{/\mathbb{Q}}$ at ℓ is coprime to 3 for any prime $\ell \in S_{\mathrm{bad}}(E)$.*

Then $\mathcal{F}_{\mathrm{cl}}$ is cartesian and residually self-dual.

Proof. Thanks to Lemma 9.3, we only need to show that $\mathcal{F}_{\mathrm{cl}}$ is cartesian at 3 and $H^1_{\overline{\mathcal{F}}_{\mathrm{cl}}}(\mathbb{Q}_3, E[3]) = H^1_{\overline{\mathcal{F}}^*_{\mathrm{cl}}}(\mathbb{Q}_3, E[3])$. The cartesian property of $\mathcal{F}_{\mathrm{cl}}$ at 3 follows from [25, Corollary 2.15].

Let us show the self-duality of $\overline{\mathcal{F}}_{\mathrm{cl}}$ at 3. In the proof of Lemma 9.3, we show that $\dim_{\mathbb{F}_3}(H^1(\mathbb{Q}_3, E[3])) = 2$. Moreover, since $E(\mathbb{F}_3)[3] = 0$, we have

$$\mathbb{F}_3 \cong E(\mathbb{Q}_3)/3E(\mathbb{Q}_3) \xrightarrow{\sim} H^1_{\overline{\mathcal{F}}_{\mathrm{cl}}}(\mathbb{Q}_3, E[3]).$$

By the definition of the Weil pairing, we see that

$$H^1_{\overline{\mathcal{F}}_{\mathrm{cl}}}(\mathbb{Q}_3, E[3]) \subset H^1_{\overline{\mathcal{F}}_{\mathrm{cl}}}(\mathbb{Q}_3, E[3])^{\perp},$$

which implies $H^1_{\overline{\mathcal{F}}_{\mathrm{cl}}}(\mathbb{Q}_3, E[3]) = H^1_{\overline{\mathcal{F}}_{\mathrm{cl}}}(\mathbb{Q}_3, E[3])^{\perp}$ since

$$\dim_{\mathbb{F}_3}(H^1(\mathbb{Q}_3, E[3])) = 2 \quad \text{and} \quad \dim_{\mathbb{F}_3}(H^1_{\overline{\mathcal{F}}_{\mathrm{cl}}}(\mathbb{Q}_3, E[3])) = 1. \qquad \square$$

Remark 9.10. Under the assumptions in Lemma 9.3, using the fact in Remark 9.4, one can show that the dual Selmer module $H^1_{\mathcal{F}^*_{\mathrm{cl}}}(\mathbb{Q}, T^\vee(1))$ coincides with the 3^α-Selmer group $\mathrm{Sel}(K, E[3^\alpha])$ associated with the elliptic curve $E_{/K}$.

9.2.2. *Mazur–Tate modular element.* Suppose that E has a good ordinary reduction at 3 and $E(\mathbb{F}_3)[3] = 0$. Let f_E denote the newform of weight 2 associated with the elliptic curve $E_{/\mathbb{Q}}$. Take a square-free integer $d \in \mathcal{N}$. For any integer a with $(a, d) = 1$, we write $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\mu_d)/\mathbb{Q})$ for the field automorphism satisfying $\sigma_a(\zeta) = \zeta^a$ for any $\zeta \in \mu_d$. We then set

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

Since the image of $G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(T_3(E)) \cong \mathrm{GL}_2(\mathbb{Z}_3)$ contains $\mathrm{SL}_2(\mathbb{Z}_3)$, we have $\mathrm{Re}([a/d])/\Omega_E^+ \in \mathbb{Z}_3$ (see [15, Theorem 3.5]). Here Ω_E^+ is the Néron period of the elliptic curve E. Define the Mazur–Tate modular element $\widetilde{\theta}_{\mathbb{Q}(\mu_d)}$ by

$$\widetilde{\theta}_{\mathbb{Q}(\mu_d)} := \sum_{\substack{a=1 \\ (a,d)=1}}^{d} \frac{\mathrm{Re}([a/d])}{\Omega_E^+} \sigma_a \in \mathbb{Z}_3[\mathrm{Gal}(\mathbb{Q}(\mu_d)/\mathbb{Q})].$$

Then one can construct an Euler system (of rank 0)

$$\{\widetilde{\xi}_L\}_{L\in\Omega} \in \prod_{L\in\Omega} \mathbb{Z}_3[\![\mathrm{Gal}(L\mathbb{Q}^{\mathrm{cyc}}/\mathbb{Q})]\!]$$

from the Mazur–Tate modular elements $\widetilde{\theta}_{\mathbb{Q}(\mu_d)}$ (see [14, p. 324] or [25, §3.1]). Here $\mathbb{Q}^{\mathrm{cyc}}$ is the cyclotomic $\mathbb{Z}_3$-extension. Note that the element $\widetilde{\xi}_{\mathbb{Q}}$ coincides with the ordinary p-adic L-function up to the multiplication by a unit in $\mathbb{Z}_3[\![\mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc}}/\mathbb{Q})]\!]$. Moreover, exactly the same argument as in [25, §3.4] shows that one can construct a Kolyvagin system

$$\kappa_E := (\kappa_{E,\mathfrak{d}})_{\mathfrak{d}\in\mathcal{N}} \in \mathrm{KS}_0(T,\mathcal{F}_{\mathrm{cl}})$$

from the Euler system $\{\widetilde{\xi}_L\}_{L\in\Omega}$. Note that $\delta(\kappa_E)_1$ is the image of $\widetilde{\xi}_{\mathbb{Q}}$ in R and that the argument in [25, §4.1] shows that for any square-free integer $d \in \mathcal{N}$ we have

$$\delta(\kappa_E)_d \bmod \mathfrak{m}_R = \pm \sum_{\substack{a=1 \\ (a,d)=1}}^{d} \frac{\mathrm{Re}([a/d])}{\Omega_E^+} \prod_{\ell\mid d} \overline{\log}_{g_\ell}(\sigma_a) \otimes \bigotimes_{\ell\mid d} g_\ell.$$

Here $g_\ell \in \mathrm{Gal}(\mathbb{Q}(\mu_\ell)/\mathbb{Q})$ is a generator and $\overline{\log}_{g_\ell}\colon \mathrm{Gal}(\mathbb{Q}(\mu_\ell)/\mathbb{Q}) \xrightarrow{\sim} \mathbb{Z}/(\ell-1)\mathbb{Z} \longrightarrow \mathbb{F}_3; g_\ell^a \mapsto a \bmod 3$.

Following Kurihara's terminology, we say that $d \in \mathcal{N}$ is δ-minimal if $\delta(\kappa_E)_d \not\equiv 0 \pmod{\mathfrak{m}_R}$ and $\delta(\kappa_E)_e \equiv 0 \pmod{\mathfrak{m}_R}$ for any positive proper divisor e of d. Then Lemma 9.3 and Theorem 8.5 combined with the arguments of the proofs of [25, Corollary 4.3 and Theorem 4.8] show the following theorem:

Theorem 9.11.

(1) *The following claims are equivalent.*
  (a) *The Iwasawa main conjecture for $E_{/\mathbb{Q}}$ holds true.*
  (b) *The Kolyvagin system κ_E is a basis of* $\mathrm{KS}_0(T,\mathcal{F}_{\mathrm{cl}})$*.*
  (c) *There is a δ-minimal integer.*

(2) *In the case that $p = 3$, the conjecture of Kurihara* [14, Conjecture 2] *holds true, that is, for any δ-minimal integer $d \in \mathcal{N}$ the $\mathbb{F}_3$-homomorphism*

$$\mathrm{Sel}(\mathbb{Q}, E[3]) \longrightarrow \bigoplus_{\ell\mid d} E(\mathbb{Q}_\ell)/3E(\mathbb{Q}_\ell)$$

is an isomorphism.

Remark 9.12. When $p \geq 5$, the conjecture of Kurihara [14, Conjecture 2] is proved by the author in [25] and Chan-Ho Kim in [13], independently.

Remark 9.13. Skinner and Urban proved in [26] that if there exists a prime $q \neq 3$ such that $\mathrm{ord}_q(N_E) = 1$ and $E[3]$ is ramified at q, then the Iwasawa main conjecture for $E_{/\mathbb{Q}}$ is valid. Here N_E is the conductor of $E_{/\mathbb{Q}}$.

Theorems 8.5 and 9.11 have the following corollary:

Corollary 9.14. *For any square-free integer $d \in \mathcal{N}$ we have*

$$I(\delta(\kappa_E)_d) \subset \mathrm{Fitt}^0_R(H^1_{\mathcal{F}^*(d)}(\mathbb{Q}, T^\vee(1))^\vee),$$

with equality if the Iwasawa main conjecture for $E_{/\mathbb{Q}}$ holds true.

References

[1] D. Burns, R. Sakamoto & T. Sano, "On the theory of higher rank Euler, Kolyvagin and Stark systems, II", https://arxiv.org/abs/1805.08448.

[2] D. Burns & T. Sano, "On the theory of higher rank Euler, Kolyvagin and Stark systems", *Int. Math. Res. Not.* **2021** (2021), no. 13, p. 10118-10206.

[3] K. Büyükboduk, "Kolyvagin systems of Stark units", *J. Reine Angew. Math.* **631** (2009), p. 85-107.

[4] ———, "Stark units and the main conjectures for totally real fields", *Compos. Math.* **145** (2009), no. 5, p. 1163-1195.

[5] ———, "Λ-adic Kolyvagin systems", *Int. Math. Res. Not.* **2011** (2011), no. 14, p. 3141-3206.

[6] ———, "Stickelberger elements and Kolyvagin systems", *Nagoya Math. J.* **203** (2011), p. 123-173.

[7] ———, "Main conjectures for CM fields and a Yager-type theorem for Rubin-Stark elements", *Int. Math. Res. Not.* **2014** (2014), no. 21, p. 5832-5873.

[8] ———, "Deformations of Kolyvagin systems", *Ann. Math. Qué.* **40** (2016), no. 2, p. 251-302.

[9] ———, "On the Iwasawa theory of CM fields for supersingular primes", *Trans. Am. Math. Soc.* **370** (2018), no. 2, p. 927-966.

[10] K. Büyükboduk & A. Lei, "Coleman-adapted Rubin-Stark Kolyvagin systems and supersingular Iwasawa theory of CM abelian varieties", *Proc. Lond. Math. Soc. (3)* **111** (2015), no. 6, p. 1338-1378.

[11] N. Elkies, "Elliptic curves with 3-adic Galois representation surjective mod 3 but not mod 9", 2006, https://arxiv.org/abs/math/061273.

[12] K. Kato, "p-adic Hodge theory and values of zeta functions of modular forms", in *Cohomologies p-adiques et applications arithmétiques. III*, Astérisque, vol. 295, Société Mathématique de France, 2004, p. 117-290.

[13] C.-H. Kim, "The structure of Selmer groups and the Iwasawa main conjecture for elliptic curves", 2022, https://arxiv.org/abs/2203.12159.

[14] M. Kurihara, "The structure of Selmer groups of elliptic curves and modular symbols", in *Iwasawa theory 2012*, Contributions in Mathematical and Computational Sciences, vol. 7, Springer, 2014, p. 317-356.

[15] J. I. Manin, "Parabolic points and zeta functions of modular curves", *Izv. Akad. Nauk SSSR, Ser. Mat.* **36** (1972), p. 19-66.

[16] H. Matsumura, *Commutative ring theory*, second ed., Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge University Press, 1989, translated from the Japanese by M. Reid, xiv+320 pages.

[17] B. Mazur & K. Rubin, "Kolyvagin systems", *Mem. Am. Math. Soc.* **168** (2004), no. 799, p. viii+96.

[18] ———, "Controlling Selmer groups in the higher core rank case", *J. Théor. Nombres Bordeaux* **28** (2016), no. 1, p. 145-183.

[19] ———, "Refined class number formulas for $\mathbb{G}_m$", *J. Théor. Nombres Bordeaux* **28** (2016), no. 1, p. 185-211.

[20] A. Reverter & N. Vila, "Images of mod p Galois representations associated to elliptic curves", *Can. Math. Bull.* **44** (2001), no. 3, p. 313-322.

[21] K. Rubin, *Euler systems. (Hermann Weyl Lectures)*, Annals of Mathematics Studies, vol. 147, Princeton University Press, 2000, xii+227 pages.

[22] R. Sakamoto, "Stark systems over Gorenstein local rings", *Algebra Number Theory* **12** (2018), no. 10, p. 2295-2326.

[23] ———, "On the theory of higher rank Euler, Kolyvagin and Stark systems: a research announcement", *RIMS Kôkyûroku Bessatsu* **B83** (2020), p. 141-159.

[24] ———, "On the theory of Kolyvagin systems of rank 0", *J. Théor. Nombres Bordeaux* **33** (2021), no. 3, p. 1077-1102.
[25] ———, "p-Selmer group and modular symbols", *Doc. Math.* **27** (2022), p. 1891-1922.
[26] C. SKINNER & E. URBAN, "The Iwasawa main conjectures for GL_2", *Invent. Math.* **195** (2014), no. 1, p. 1-277.
[27] H. P. F. SWINNERTON-DYER, "On l-adic representations and congruences for coefficients of modular forms", in *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, Lecture Notes in Mathematics, vol. 350, Springer, 1973, p. 1-55.

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