Kataoka, T.
Osaka J. Math.
59 (2022), 417–452

STARK SYSTEMS AND EQUIVARIANT MAIN CONJECTURES

Takenori KATAOKA

(Received October 22, 2020, revised February 18, 2021)

Abstract

The theory of Stark systems due to Burns, Sakamoto, and Sano is an important tool toward main conjectures in Iwasawa theory. In this paper, we propose a new perspective of their results, which produces more refined consequences. As a principal application, we prove one divisibility of the equivariant main conjecture for elliptic curves, under certain conditions without $\mu = 0$ hypothesis.

1. Introduction

One of the main themes in Iwasawa theory is the main conjectures, which predict close relations between algebraic objects (Selmer groups) and analytic objects (p-adic L-functions) in various situations. It is known that the theory of Euler systems plays an essential role in proofs of main conjectures. In fact, given an appropriate Euler system in general, we can prove "one half" of the main conjecture, that is, a bound of Selmer groups. The theory of Euler systems was developed by many works, including Rubin [21], Mazur-Rubin [15], among others.

For example, the cyclotomic units constitute an Euler system for $\mathbb{G}_m$ over $\mathbb{Q}$. Another important example is the Euler systems of Beilinson-Kato zeta elements, constructed by Kato [11], for elliptic modular forms. By applying the general results to those Euler systems, we can prove (halves of) the main conjectures in those situations.

The theory of Euler systems was further developed by Burns, Sakamoto, and Sano [4], [5], [22]. One of the features of their works is the notion of the *exterior power biduals*, which enables us to develop higher rank theory. At the same time, they succeeded in developing equivariant theory, which had not been achieved even in the rank one case. Using the exterior power biduals, they defined the notion of Stark systems, proved that each Euler system yields a Stark system (via a Kolyvagin system), and proved that each Stark system provides a bound of Selmer groups.

The main purpose of this paper is to obtain refined consequences of the existence of a Stark system. In order to achieve that, we introduce a novel notion of *(primitive) basic elements* for perfect complexes in general. Then a key theorem (Theorem 5.12) of this paper states that each (primitive) Stark system gives rise to a (primitive) basic element of an arithmetic complex. See Subsection 1.2 for more details.

As a fundamental application, we prove a half of the equivariant main conjecture for elliptic curves under a certain condition which is weaker than previous. Because the application is actually the main motivation of the present work, we firstly state that result in Subsection

2020 Mathematics Subject Classification. 11R23.

1.1.

1.1. Equivariant Iwasawa theory for elliptic curves. We explain the principal application of the key theorem of this paper to equivariant Iwasawa theory for elliptic curves, which was developed by the author in [9] based on many preceding works (see the introduction of [9]). We give only a minimal explanation here and refer to [9] for more details.

Fix a prime number $p \geq 5$. Let E be an elliptic curve over $\mathbb{Q}$ which has good reduction at p. Let F be a finite abelian extension of $\mathbb{Q}$ and we denote by $S_{\mathrm{ram}}(F/\mathbb{Q})$ the set of prime numbers which are ramified in $F/\mathbb{Q}$. We suppose that $S_{\mathrm{ram}}(F/\mathbb{Q})$ is disjoint from $S_{\mathrm{bad}}(E)$, the set of bad primes for E. Let F_∞ be the cyclotomic $\mathbb{Z}_p$-extension of F and put $\mathcal{R}_F = \mathbb{Z}_p[[\mathrm{Gal}(F_\infty/\mathbb{Q})]]$. Let S be a set of prime numbers $\neq p$ such that $S \cup \{p\} \supset S_{\mathrm{ram}}(F/\mathbb{Q})$.

We will often assume the following *non-anomalous condition* ([9, Assumption 3.7]):

Assumption 1.1. *The group $E(\mathbb{Q}(\mu_{pm}) \otimes \mathbb{Q}_p)$ is p-torsion-free, where m is the conductor of $F/\mathbb{Q}$.*

This condition is slightly stronger than that the group $E(F \otimes \mathbb{Q}_p)$ is p-torsion-free. The author expects that the weaker condition is more appropriate, but for the sake of safety, we suppose Assumption 1.1.

It is known that Iwasawa-theoretic analysis of elliptic curves has a different flavor depending on the reduction type at p. If E has ordinary reduction at p, then set $\bullet = \emptyset$, meaning "no symbol," and otherwise fix $\bullet \in \{+, -\}$. We will soon formulate the main conjecture between $\bullet$-Selmer groups and $\bullet$-p-adic L-functions. It should be noted here that, in Section 6, we will reformulate the main conjecture in a form that does not depend on the reduction type.

As usual, let $E[p^\infty]$ be the group of p-power torsion elements of E. Then, as in [9, §2.1], the $\bullet$-Selmer group $\mathrm{Sel}_S^\bullet(E/F_\infty)$ is defined by

$$(1.1)\quad \mathrm{Sel}_S^\bullet(E/F_\infty) = \mathrm{Ker}\left(H^1(F_\infty, E[p^\infty]) \to \frac{H^1(F_\infty \otimes \mathbb{Q}_p, E[p^\infty])}{E^\bullet(F_\infty \otimes \mathbb{Q}_p) \otimes (\mathbb{Q}_p/\mathbb{Z}_p)} \times \prod_{l \notin S \cup \{p\}} H^1(F_\infty \otimes \mathbb{Q}_l, E[p^\infty]) \right),$$

where, in the supersingular case, $E^\pm(F_\infty \otimes \mathbb{Q}_p)$ is the submodule of $E(F_\infty \otimes \mathbb{Q}_p)$ defined by Kobayashi [13]. It is known that $\mathrm{Sel}_S^\bullet(E/F_\infty)$ is a finitely generated cotorsion $\mathcal{R}_F$-module.

On the analytic side, by Amice-Velu [1], Višik [24], or Mazur-Tate-Teitelbaum [16], with an idea of Pollack [19] in the supersingular case, we have the $\bullet$-p-adic L-function

$$\mathcal{L}_S^\bullet(E/F_\infty) \in \mathcal{R}_F \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

with convention as in [9, §2.2].

In [9, (1,1)], we proposed the equivariant main conjecture as follows. We denote by $(-)^\vee$ the Pontryagin dual and by $\mathrm{Fitt}_{\mathcal{R}_F}(-)$ the initial Fitting ideal.

Conjecture 1.2. *Under* Assumption 1.1*, we have*

$$W_F^\bullet \,\mathrm{Fitt}_{\mathcal{R}_F}(\mathrm{Sel}_S^\bullet(E/F_\infty)^\vee) = (\mathcal{L}_S^\bullet(E/F_\infty))$$

as principal ideals of $\mathcal{R}_F$.

Here, $W_F^\bullet$ is a completely explicit principal ideal of $\mathcal{R}_F$ (we do not recall the definition here). Since we have

$$\mathrm{pd}_{\mathcal{R}_F}(\mathrm{Sel}_S^\bullet(E/F_\infty)^\vee) \leq 1$$

by [9, Theorem 1.1], both sides in Conjecture 1.2 are principal. Here, pd denotes the projective dimension. Note also that Conjecture 1.2 implicitly claims the integrality of the p-adic L-function $\mathcal{L}_S^\bullet(E/F_\infty)$.

In order to state our main result of this paper, we have to introduce several assumptions (Assumptions 1.3, 1.4, and 1.5 below). Those are typical assumptions in the theory of Euler systems (see e.g. [9, Remark 1.6] for some discussion). Let T_pE be the p-adic Tate module of E.

Assumption 1.3. *For any prime number $l \notin S \cup \{p\}$, the $\mathbb{Z}_p$-module $H^0(F_\infty \otimes \mathbb{Q}_l, E[p^\infty])$ is divisible.*

Assumption 1.4. *The Galois representation*

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_{\mathbb{Z}_p}(T_pE) \simeq \mathrm{GL}_2(\mathbb{Z}_p)$$

is surjective.

Assumption 1.5. *For all $l \in S$, we have $H^0(F_\infty \otimes \mathbb{Q}_l, E[p^\infty]) = 0$.*

The main application of the key theorem (Theorem 5.12) of this paper is the following.

Theorem 1.6. *Suppose* Assumptions 1.1, 1.3, 1.4, *and* 1.5. *Then we have the inclusion* $\supset$ *in* Conjecture 1.2, *that is,*

$$W_F^\bullet \,\mathrm{Fitt}_{\mathcal{R}}(\mathrm{Sel}_S^\bullet(E/F_\infty)^\vee) \supset (\mathcal{L}_S^\bullet(E/F_\infty)).$$

The proof will be given in Subsection 6.3. If we further assume the $\mu = 0$ hypothesis for the fine Selmer group, then Theorem 1.6 essentially coincides with [9, Theorem 1.5]. Thus the progress is the removal of the $\mu = 0$ hypothesis. See Remark 6.5 for a comparison of the proof in this paper with that in [9].

We mention here that, though the progress of the main result might sound minor, the new perspective (explained in Subsection 1.2) proposed in this paper can be expected to be useful for other future applications. An evidence of the strength of the idea in this paper will also be illustrated in Section 7.

1.2. Outline and key idea of this paper. Section 2 is devoted to review of facts on determinant modules $\mathrm{Det}_R(-)$ and exterior power biduals $\bigcap_R^r(-)$.

In Section 3, we will introduce the notion of *(primitive) basic elements* for perfect complexes. The notion plays key role in this paper (the term “basic” comes from “basic Euler systems” in Burns-Sano [5]). More precisely, let C be a perfect complex satisfying certain conditions, including $H^i(C) = 0$ for $i \neq 1, 2$. We put $r = \chi_R(C)$ (the Euler characteristic) and we shall define a natural homomorphism

$$\Pi_C : \mathrm{Det}_R^{-1}(C) \to \bigcap_R^r H^1(C).$$

Then we call an element of $\bigcap_R^r H^1(C)$ a basic element (resp. a primitive basic element) for C if it is the image of an element (resp. a basis) of $\mathrm{Det}_R^{-1}(C)$ under Π_C.

The author admits that the notion of (primitive) basic elements has already appeared in several preceding works in quite implicit manners (e.g. Burns-Kurihara-Sano [2], Burns-Sano [5]). For instance, as we will show in Subsection 3.3, a property of primitive basic elements is that they compute the Fitting ideal of $H^2(C)$ (though this property is not essential in this paper), and this kind of computations can be found in those preceding works. For that reason, the notion of (primitive) basic elements does not seem essentially novel, but it certainly plays a key role in the present paper to prove Theorem 1.6.

In Sections 4 and 5, we study general p-adic Galois representations as in Subsection 1.3 below. In Section 4, we introduce and examine basic properties of perfect complexes arising from Galois cohomology complexes. Of the most importance is $\mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \mathbb{T}_F)$, to which we apply the notion of (primitive) basic elements (note that $\mathbb{T}_F$ is a representation which might be ramified at a prime outside $\overline{S}$ so the definition of the complex is not totally obvious). In Section 5, we define Stark systems in our setting, in the same manner as in [4], [5], [22]. We show that, under certain conditions, the module of Stark systems is free of rank one and moreover can be identified with $\mathrm{Det}^{-1}_{\mathcal{R}_F}(\mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \mathbb{T}_F))$ (see Remark 5.7 for a relation with a preceding work). From the isomorphism, we finally deduce the key theorem (Theorem 5.12) that each Stark system gives rise to a basic element for $\mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \mathbb{T}_F)$.

In Section 6, we first reformulate Conjecture 1.2 as a statement that the Beilinson-Kato zeta element $\mathbf{z}^{\mathrm{BK}}_{F,S}$ is a primitive basic element for $\mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \mathbb{T}_F)$. Then we deduce Theorem 1.6 from Theorem 5.12 and one of the main results of [4] that an Euler system gives rise to a Stark system.

In Section 7, we apply the ideas of this paper to the discussion in a recent paper by Burns-Kurihara-Sano [3] on Beilinson-Kato elements. This section can be seen as an illustration of the strength of the idea in this paper. In particular, we deduce a result toward a conjecture in [3] on the existence of Darmon-type derivatives. Moreover, we reformulate conjectures in [3] (generalized Perrin-Riou conjecture and refined Mazur-Tate conjecture) and, as a consequence, obtain illustrative proofs of equivalences between various conjectures.

REMARK 1.7. As we repeatedly remarked, this paper gives a refinement of parts of the works by Burns, Sakamoto, and Sano. However, we do not generalize their results in the sense that we do not deal with the *higher Fitting ideals*.

1.3. Notation. Though our main objective is the Tate modules of elliptic curves, we will deal with general p-adic representations when possible. We fix our notation in this subsection. Note that we will set the rational number field $\mathbb{Q}$ as the base field, but we can generalize the results to general number fields by standard modifications (the author would like to discuss this issue in a forthcoming paper).

Let p be a fixed odd prime number. Let T be a fixed free $\mathbb{Z}_p$-module of finite rank on which the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts continuously. We denote by $S_{\mathrm{bad}}(T)$ the set of prime numbers at which T is ramified, and we assume that $S_{\mathrm{bad}}(T)$ is a finite set.

For each finite abelian extension $F/\mathbb{Q}$ (possibly ramified at p), we denote by $S_{\mathrm{ram}}(F/\mathbb{Q})$ the set of prime numbers which are ramified in $F/\mathbb{Q}$. Let F_∞/F be the cyclotomic $\mathbb{Z}_p$-extension and F_n its n-th layer for each $n \geq 0$. Put $\mathcal{R}_F = \mathbb{Z}_p[[\mathrm{Gal}(F_\infty/\mathbb{Q})]]$, the Iwasawa algebra.

We denote by $\mathbb{T}_F = T \otimes_{\mathbb{Z}_p} \mathcal{R}_F$ the Galois representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ over $\mathcal{R}_F$, where the

Galois group acts on the second factor $\mathcal{R}_F$ via the inverse of the natural homomorphism

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(F_\infty/\mathbb{Q}) \hookrightarrow \mathcal{R}_F^\times.$$

Then Shapiro's lemma enables us to identify

$$H^i(\mathbb{Q}, \mathbb{T}_F) = \varprojlim_n H^i(F_n, T), \qquad H^i(\mathbb{Q}_p, \mathbb{T}_F) = \varprojlim_n H^i(F_n \otimes \mathbb{Q}_p, T)$$

where the projective limit is taken with respect to the corestriction maps. Namely, the cohomology groups of $\mathbb{T}_F$ can be regarded as the Iwasawa cohomology groups.

As zero-dimensional analogues, for an integer $m \geq 0$, we put $R_{F,m} = (\mathbb{Z}/p^m\mathbb{Z})[\mathrm{Gal}(F/\mathbb{Q})]$ and $T_{F,m} = T \otimes_{\mathbb{Z}_p} R_{F,m}$. We also put $R_F = \mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})]$ and $T_F = T \otimes_{\mathbb{Z}_p} R_F$. Then similarly we have

$$H^i(\mathbb{Q}, T_{F,m}) = H^i(F, T/p^mT), \qquad H^i(\mathbb{Q}_p, T_{F,m}) = H^i(F \otimes \mathbb{Q}_p, T/p^mT),$$

$$H^i(\mathbb{Q}, T_F) = H^i(F, T), \qquad H^i(\mathbb{Q}_p, T_F) = H^i(F \otimes \mathbb{Q}_p, T)$$

by Shapiro's lemma.

For a finite set S of prime numbers $\neq p$, we put

$$\overline{S} = S \cup \{p, \infty\}.$$

By a pair (F, S), we always mean that $F/\mathbb{Q}$ is a finite abelian extension and S is a finite set of prime numbers $\neq p$ such that $S \cup \{p\} \supset S_{\mathrm{ram}}(F/\mathbb{Q})$. We do not require that $S \cup \{p\} \supset S_{\mathrm{bad}}(T)$.

We introduce assumptions which correspond to those in Subsection 1.1.

Assumption 1.8 (on F)**.** *We have*

$$H^0(\mathbb{Q}_p, \mathbb{T}_F^\vee(1)) = H^0(F_\infty \otimes \mathbb{Q}_p, T^\vee(1)) = 0,$$

namely,

$$H^0(F \otimes \mathbb{Q}_p, (T/pT)^\vee(1)) = 0.$$

Assumption 1.9 (on F)**.** *We have*

$$H^0(F, T/pT) = 0.$$

Assumption 1.10 (on (F, S))**.** *For any prime number $l \notin S \cup \{p\}$, the $\mathbb{Z}_p$-module*

$$H^0(F_\infty \otimes \mathbb{Q}_l, T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)$$

is divisible.

Assumption 1.11 (on (F, S))**.** *For all $l \in S$, we have $H^0(F_\infty \otimes \mathbb{Q}_l, (T/pT)^\vee(1)) = 0$.*

2. Preliminaries

2.1. Perfect complexes. In this subsection, we fix our conventions on perfect complexes.

Let R be a (commutative) noetherian ring. We denote by $D^{\mathrm{perf}}(R)$ the derived category of perfect complexes of R-modules. For integers $a \leq b$, let $D^{[a,b]}(R)$ be the full subcategory of $D^{\mathrm{perf}}(R)$ that consists of perfect complex which is quasi-isomorphic to a complex of the form $[C^a \to C^{a+1} \to \cdots \to C^b]$ concentrated in degrees $a, a+1, \dots, b$ such that each C^i ($a \le i \le b$) is finitely generated projective over R.

For a complex $C \in D^{\mathrm{perf}}(R)$, taking a quasi-isomorphism

$$C \simeq [\cdots \to C^i \to C^{i+1} \to \dots],$$

where each C^i is finitely generated projective over R, we define the Euler characteristic of C by

$$\chi_R(C) = \sum_i (-1)^{i-1} \operatorname{rank}_R(C^i).$$

This is a locally constant function on $\operatorname{Spec}(R)$. It is easy to show that the Euler characteristic is additive with respect to distinguished triangles.

We define the determinant module for C as above by

$$\operatorname{Det}_R(C) = \bigotimes_{i \in \mathbb{Z}} \operatorname{Det}_R^{(-1)^i}(C^i),$$

where we put

$$\operatorname{Det}_R(F) = \bigwedge_R^{\operatorname{rank}(F)} F, \qquad \operatorname{Det}_R^{-1}(F) = \operatorname{Hom}_R(\operatorname{Det}_R(F), R)$$

for each finitely generated projective R-module F. Note that $\operatorname{rank}(F)$ is a locally constant function of $\operatorname{Spec}(R)$, so the exterior power should be taken locally. We also define $\operatorname{Det}_R^{-1}(C) = \operatorname{Hom}_R(\operatorname{Det}_R(C), R)$. We ignore the degrees of determinant modules since they are not essential in this paper.

2.2. Determinant modules and Fitting ideals. In this subsection, we review some results on determinant modules and Fitting ideals (one can find details in [10, Section 3]).

Let Δ be a finite abelian group and we treat the algebra $\mathcal{R} = \mathbb{Z}_p[\Delta][[T]]$. Let $\mathcal{P}_{\mathcal{R}}$ be the category of finitely generated torsion $\mathcal{R}$-modules with projective dimension at most one. Let $K_0(\mathcal{P}_{\mathcal{R}})$ be its Grothendieck group. Let $\mathcal{I}_{\mathcal{R}}$ be the group of invertible (fractional) ideals of $\mathcal{R}$. Then taking the Fitting ideals yields a group homomorphism

$$\operatorname{Fitt}_{\mathcal{R}} : K_0(\mathcal{P}_{\mathcal{R}}) \to \mathcal{I}_{\mathcal{R}}.$$

Let $Q(\mathcal{R})$ be the total ring of fractions of $\mathcal{R}$. Let $D^{\mathrm{perf}}_{\mathrm{tor}}(\mathcal{R})$ be the full subcategory of $D^{\mathrm{perf}}(\mathcal{R})$ whose objects are complexes with torsion cohomology groups. For each $C \in D^{\mathrm{perf}}_{\mathrm{tor}}(\mathcal{R})$, the complex $Q(\mathcal{R}) \otimes^{\mathbb{L}}_{\mathcal{R}} C$ is acyclic, so we have natural isomorphisms

$$\iota_C : Q(\mathcal{R}) \otimes_{\mathcal{R}} \operatorname{Det}^{-1}_{\mathcal{R}}(C) \simeq \operatorname{Det}^{-1}_{Q(\mathcal{R})}(Q(\mathcal{R}) \otimes^{\mathbb{L}}_{\mathcal{R}} C) \simeq Q(\mathcal{R}).$$

We put $\mathrm{d}_{\mathcal{R}}(C) = \iota_C(\operatorname{Det}^{-1}_{\mathcal{R}}(C)) \subset Q(\mathcal{R})$, which is an invertible submodule of $Q(\mathcal{R})$, so $\mathrm{d}_{\mathcal{R}}(C) \in \mathcal{I}_{\mathcal{R}}$.

Let $K_0(D^{\mathrm{perf}}_{\mathrm{tor}}(\mathcal{R}))$ be the Grothendieck group of $D^{\mathrm{perf}}_{\mathrm{tor}}(\mathcal{R})$. Then the above construction yields a group homomorphism

$$\mathrm{d}_{\mathcal{R}} : K_0(D^{\mathrm{perf}}_{\mathrm{tor}}(\mathcal{R})) \to \mathcal{I}_{\mathcal{R}}.$$

Proposition 2.1 ([10, Theorem 3.1])**.** *We have a natural homomorphism $\varphi_{\mathcal{R}} : K_0(\mathcal{P}_{\mathcal{R}}) \to K_0(D^{\mathrm{perf}}_{\mathrm{tor}}(\mathcal{R}))$ such that*

$$\mathrm{d}_{\mathcal{R}} \circ \varphi_{\mathcal{R}} = \mathrm{Fitt}_{\mathcal{R}}$$

(in the additive notation). Moreover, all of $\mathrm{Fitt}_{\mathcal{R}}$*,* $\mathrm{d}_{\mathcal{R}}$*, and* $\varphi_{\mathcal{R}}$ *are isomorphic as group homomorphisms.*

Indeed, $\varphi_{\mathcal{R}}$ is defined by

$$\varphi_{\mathcal{R}}[P] = [C^{-1} \stackrel{d^{-1}}{\to} C^0]$$

for each $P \in \mathcal{P}_{\mathcal{R}}$, where $0 \to C^{-1} \stackrel{d^{-1}}{\to} C^0 \to P \to 0$ is an exact sequence with C^{-1}, C^0 finitely generated projective.

2.3. Exterior power biduals. We recall the definition and properties of exterior power biduals. See [4, Section 2], [5, Sections 2.1 and A], [22, Section 2], or [23, Appendix B] for details.

Definition 2.2. Let R be a noetherian ring and M a finitely generated R-module. We put $M^* = \mathrm{Hom}_R(M, R)$; though the coefficient ring R is implicit, there is no afraid of confusion. Let r be a locally constant function on $\mathrm{Spec}(R)$ that takes values in non-negative integers. Then we define the r-th exterior power bidual of M by

$$\bigcap_R^r M = \left(\bigwedge_R^r (M^*) \right)^* .$$

Remark 2.3. We have a natural R-homomorphism

$$\bigwedge_R^r M \to \bigcap_R^r M$$

given locally by

$$x_1 \wedge \cdots \wedge x_r \mapsto \left[\varphi_1 \wedge \cdots \wedge \varphi_r \mapsto \det(\varphi_i(x_j))_{i,j} \right]$$

for $x_1, \ldots, x_r \in M$ and $\varphi_1, \ldots, \varphi_r \in M^*$. This is isomorphic if M is projective over R.

Remark 2.4. Suppose R is a zero-dimensional Gorenstein ring.

(1) For each finitely generated R-module M, the natural homomorphism

$$\mathrm{ev} : M \to \bigcap_R^1 M = (M^*)^*,$$

which sends $x \in M$ to the evaluation map $\mathrm{ev}_x : M^* \to R$, is isomorphic. This is a basic property of zero-dimensional Gorenstein rings.

(2) Let

$$0 \to M' \stackrel{\alpha}{\to} M \stackrel{\beta}{\to} F$$

be an exact sequence of finitely generated R-modules such that F is finitely generated projective with $a = \mathrm{rank}_R(F)$. Then, for each r, we have a natural R-homomorphism

$$\bigcap_R^{r+a} M \otimes_R \mathrm{Det}_R^{-1}(F) \to \bigcap_R^r M',$$

which is constructed as follows (see [22, Section 2] or [5, Proposition A.3]).

Consider the dual sequence

$$F^* \xrightarrow{\beta^*} M^* \xrightarrow{\alpha^*} (M')^* \to 0,$$

which is exact since R is zero-dimensional Gorenstein. This sequence induces

$$\bigwedge_R^r (M')^* \otimes_R \mathrm{Det}_R(F^*) \to \bigwedge_R^{r+a} M^*$$

given locally by

$$(\varphi_1 \wedge \cdots \wedge \varphi_r) \otimes (\psi_1 \wedge \cdots \wedge \psi_a) \mapsto (\alpha^*)^{-1}(\varphi_1) \wedge \cdots \wedge (\alpha^*)^{-1}(\varphi_r) \wedge \beta^*(\psi_1) \wedge \cdots \wedge \beta^*(\psi_a)$$

for $\varphi_1, \dots, \varphi_r \in (M')^*$, $\psi_1, \dots, \psi_a \in F^*$. Here, $(\alpha^*)^{-1}(\varphi_i)$ denotes any element of M^* which is sent to φ_i by α^*. The well-definedness (i.e. the independence from the choices of lifts) follows from $\bigwedge_R^{a+1} F^* = 0$. By taking the dual, we obtain the desired homomorphism.

We shall deal with a general commutative ring R which is of the form

$$R = \varprojlim_{j \in J} R_j, \tag{2.1}$$

where J is a directed set, R_j is a zero-dimensional Gorenstein ring of finite order for each $j \in J$, and we assume that the structure homomorphisms are all surjective. Typical examples of R are $\mathcal{R}_F$ and R_F.

Firstly we observe an easy characterization of $D^{[a,b]}(R)$ in $D^{\mathrm{perf}}(R)$.

Lemma 2.5. *Let R be of the form* (2.1). *Let $C \in D^{\mathrm{perf}}(R)$ be a perfect complex and let $a \leq b$ be any integers. Then C is in $D^{[a,b]}(R)$ if and only if $H^i(C \otimes_R^{\mathbb{L}} R_j) = 0$ for any $i \neq a, a+1, \dots, b$ and any $j \in J$.*

Proof. The "only if" part is clear. For the "if" part, we only have to show the following claim: *For an R-homomorphism $f : F \to F'$ between finitely generated projective R-modules, if the induced R_j-homomorphism $\overline{f} : F \otimes_R R_j \to F' \otimes_R R_j$ is injective for any $j \in J$, then f is a split injection.* We shall show this claim.

For each $j \in J$, we write $F_j = F \otimes_R R_j$ and $F'_j = F' \otimes_R R_j$. Since both F and F' are projective, we have a natural isomorphism

$$\mathrm{Hom}_R(F', F) \simeq \varprojlim_{j \in J} \mathrm{Hom}_{R_j}(F'_j, F_j).$$

For each $j \in J$, since R_j is a zero-dimensional Gorenstein ring, any injective R_j-homomorphism is a split injection. Therefore, the subset

$$G_j = \{g_j \in \mathrm{Hom}_{R_j}(F'_j, F_j) \mid g_j \circ \overline{f} \text{ is the identify on } F_j\}$$

is not empty. Moreover, since R_j is of finite order, the set G_j is also finite. Therefore, the projective limit $\varprojlim_{j \in J} G_j$ is not empty. Then any element g of $\varprojlim_{j \in J} G_j \subset \varprojlim_{j \in J} \mathrm{Hom}_{R_j}(F'_j, F_j) \simeq \mathrm{Hom}_R(F', F)$ satisfies the condition that $g \circ f$ is the identity on F. This completes the proof. □

We also record the following, due to Sakamoto [23].

Proposition 2.6 ([23, Lemmas B.13 and B.14])**.** *Let R be of the form* (2.1). *Let C be a perfect complex in $D^{[1,2]}(R)$ and $r \geq 0$ be a locally constant function on* Spec(R). *Then the system $\left\{\bigcap_{R_j}^{r} H^1(C \otimes_R^{\mathbb{L}} R_j)\right\}_{j\in J}$ naturally constitutes a projective system and we have a natural isomorphism*

$$\bigcap_{R}^{r} H^1(C) \xrightarrow{\sim} \varprojlim_{j} \left(\bigcap_{R_j}^{r} H^1(C \otimes_R^{\mathbb{L}} R_j) \right).$$

In particular, taking $r = 1$, we deduce that the natural map

$$H^1(C) \xrightarrow{\sim} \bigcap_{R}^{1} H^1(C) = (H^1(C)^*)^* \tag{2.2}$$

is isomorphic, that is, $H^1(C)$ is reflexive. Alternatively, we can directly show that $H^1(C)$ is reflexive since $H^1(C)$ is the kernel of a homomorphism between finitely generated projective modules.

3. Basic elements

In this section, we introduce the notion of basic elements, which is the key in the present paper as discussed in Subsection 1.2.

3.1. Definition of basic elements. For the definition of basic elements, we first deal with zero-dimensional Gorenstein rings such as $R_{F,m} = (\mathbb{Z}/p^m\mathbb{Z})[\mathrm{Gal}(F/\mathbb{Q})]$, and then by taking limit more general rings of the form (2.1) such as $R_F, \mathcal{R}_F$.

Definition 3.1. Let R be a zero-dimensional Gorenstein ring. Let $C \in D^{[1,2]}(R)$ be a perfect complex and put $r = \chi_R(C)$. Suppose that $r \geq 0$. Then we define a natural map

$$\Pi_C : \mathrm{Det}_R^{-1}(C) \to \bigcap_{R}^{r} H^1(C)$$

as follows (this is essentially the same as Π_ψ in [5, Proposition A.7(iv)], but our formulation is more canonical). Let us take a quasi-isomorphism $C \simeq [C^1 \to C^2]$ which is concentrated in degrees one and two and C^1, C^2 are both finitely generated projective. By applying Remark 2.4(2) to the exact sequence

$$0 \to H^1(C) \to C^1 \to C^2,$$

we obtain a homomorphism

$$\bigcap_{R}^{r+\mathrm{rank}(C^2)} C^1 \otimes_R \mathrm{Det}_R^{-1}(C^2) \to \bigcap_{R}^{r} H^1(C).$$

Since C^1 is finitely generated projective of rank $r + \mathrm{rank}_R(C^2)$, Remark 2.3 shows that

$$\bigcap_{R}^{r+\mathrm{rank}(C^2)} C^1 \simeq \bigwedge_{R}^{\mathrm{rank}(C^1)} C^1 = \mathrm{Det}_R(C^1).$$

Therefore, we can define Π_C as the above homomorphism.

An element of $\bigcap_R^r H^1(C)$ is called a basic element for C if it is in $\Pi_C(\mathrm{Det}_R^{-1}(C))$. Also, an element of $\bigcap_R^r H^1(C)$ is called a primitive basic element for C if it is the image of a basis of $\mathrm{Det}_R^{-1}(C)$ under Π_C.

We note that the map Π_C is not injective in general. The extreme case where Π_C is the zero map can occur, and in that case the zero element is the unique basic element.

Definition 3.2. Let R be of the form (2.1). Let C be a perfect complex in $D^{[1,2]}(R)$ and put $r = \chi_R(C)$. Suppose that $r \geq 0$. Then we define an R-homomorphism

$$\Pi_C : \mathrm{Det}_R^{-1}(C) \to \bigcap_R^r H^1(C)$$

as the projective limit of $\Pi_{C\otimes_R^{\mathbb{L}} R_j}$ in Definition 3.1, using Proposition 2.6. Via Π_C, we define (primitive) basic elements in the same manner as in Definition 3.1.

The following proposition follows immediately from the definition.

Proposition 3.3. *Let R be of the form* (2.1). *Let C be a perfect complex in $D^{[1,2]}(R)$ with $r = \chi_R(C) \geq 0$. Let $z \in \bigcap_R^r H^1(C)$ be an element and we denote by z_j the image of z in $\bigcap_{R_j}^r H^1(C \otimes_R^{\mathbb{L}} R_j)$. Then z is a basic element (resp. primitive basic element) for C if and only if z_j is a basic element (resp. primitive basic element) for $C \otimes_R^{\mathbb{L}} R_j$ for any $j \in J$.*

3.2. Concrete description in rank one case. We give a concrete description of a primitive basic element in the rank one case. We identify $H^1(C)$ and $\bigcap_R^1 H^1(C)$ by (2.2).

Proposition 3.4. *Let R be of the form* (2.1). *Consider a perfect complex $C = [R^s \xrightarrow{A} R^{s-1}]$ concentrated in degrees one and two with $s \geq 1$, where A is regarded as a matrix of size $(s-1) \times s$. Let $e_1, \dots, e_s$ be the standard basis of R^s. For each $1 \leq i \leq s$, we denote by A_i the $(s-1) \times (s-1)$ matrix which is obtained by removing the i-th column of A. Then*

$$\sum_{i=1}^{s} (-1)^{i-1} \det(A_i) e_i \in R^s$$

is contained in $H^1(C)$ and indeed is a primitive basic element for C.

Proof. This description has already given in different expressions in the literature (e.g. [5, Lemma A.7]), but we give a complete proof here. By Proposition 3.3, we may assume that R is a zero-dimensional Gorenstein ring. Let $f_1, \dots, f_{s-1}$ be the standard basis of R^{s-1} and $f_1^*, \dots, f_{s-1}^*$ the dual basis. We shall show that the homomorphism

$$\Pi_C : \bigwedge_R^s (R^s) \otimes \bigwedge_R^{s-1} (R^{s-1})^* \to H^1(C)$$

satisfies

$$\Pi_C \left((e_1 \wedge \cdots \wedge e_s) \otimes (f_1^* \wedge \cdots \wedge f_{s-1}^*) \right) = \sum_{i=1}^{s} (-1)^{i-1} \det(A_i) e_i.$$

Let $\alpha : H^1(C) \to R^s$ be the inclusion map and $\beta : R^s \to R^{s-1}$ be the map represented by A. Then the map

$$H^1(C)^* \otimes_R \bigwedge_R^{s-1}(R^{s-1})^* \to \bigwedge_R^{s}(R^s)^*$$

as in Remark 2.4(2) is given by

$$\varphi \otimes (\psi_1 \wedge \cdots \wedge \psi_{s-1}) \mapsto (\alpha^*)^{-1}(\varphi) \wedge \beta^*(\psi_1) \wedge \cdots \wedge \beta^*(\psi_{s-1}).$$

Thus the element $x = \Pi_C((e_1 \wedge \cdots \wedge e_s) \otimes (f_1^* \wedge \cdots \wedge f_{s-1}^*)) \in H^1(C)$ is characterized by

$$\varphi(x) = \left((\alpha^*)^{-1}(\varphi) \wedge \beta^*(f_1^*) \wedge \cdots \wedge \beta^*(f_{s-1}^*)\right)(e_1 \wedge \cdots \wedge e_s)$$

for any $\varphi \in H^1(C)^*$. By taking $\varphi = e_i^*$ (the dual basis) for each $1 \le i \le s$, we obtain

$$e_i^*(x) = \det \begin{pmatrix} 0 & \\ \vdots & \\ 1 & {}^tA \\ \vdots & \\ 0 & \end{pmatrix} = (-1)^{i-1}\det(A_i),$$

where, in the displayed matrix, ${}^tA$ denotes the transpose of A and the first column is 1 at the i-th row and 0 at the other rows. Thus we have $x = \sum_{i=1}^{s}(-1)^{i-1}\det(A_i)e_i$. □

In the rest of this subsection, let us consider an algebra $\mathcal{R} = \mathbb{Z}_p[\Delta][[T]]$ with Δ a finite abelian group as in Subsection 2.2. We will give another characterization (Proposition 3.6) of primitive basic elements over $\mathcal{R}$ in the rank one case. It will play an important role when we discuss main conjectures for elliptic curves in Section 6.

In general, if C is a complex over a noetherian ring R such that $H^i(C) = 0$ for $i \le 0$, then each element $z \in H^1(C)$ induces a morphism of complexes

$$R[-1] \xrightarrow{z} C$$

in the derived category, which, at degree one, induces the homomorphism $R \to H^1(C)$ which sends 1 to z.

We show a lemma which will be used in the proof of Proposition 3.6 below.

Lemma 3.5. *Let C be a perfect complex in $D^{[1,2]}(\mathcal{R})$ such that $\chi_{\mathcal{R}}(C) = 1$ and $H^2(C)$ is torsion as an $\mathcal{R}$-module. Let $\mathbf{z} \in H^1(C)$ and $\mathbf{z}' \in H^1(C)$ be elements such that* $\mathrm{Ann}_{\mathcal{R}}(\mathbf{z}) = 0$ *and* $\mathrm{Ann}_{\mathcal{R}}(\mathbf{z}') = 0$. *Suppose that the cones of $\mathcal{R}[-1] \xrightarrow{\mathbf{z}} C$ and $\mathcal{R}[-1] \xrightarrow{\mathbf{z}'} C$ represent the same element in $K_0(D^{\mathrm{perf}}_{\mathrm{tor}}(\mathcal{R}))$. Then there exists a unit $u \in \mathcal{R}^\times$ such that $\mathbf{z}' = u\mathbf{z}$.*

Proof. For a while let $a \in \mathcal{R}$ be any non-zero-divisor. We consider a morphism between triangles

$$\begin{array}{ccccccc} \mathcal{R}[-1] & \xrightarrow{\mathbf{z}} & C & \longrightarrow & \mathrm{Cone}(\mathbf{z}) & \longrightarrow & \\ {\scriptstyle a}\uparrow & & \| & & \uparrow & & \\ \mathcal{R}[-1] & \xrightarrow{a\mathbf{z}} & C & \longrightarrow & \mathrm{Cone}(a\mathbf{z}) & \longrightarrow & . \end{array}$$

Here, we simply write Cone($\mathbf{z}$) for the cone of $\mathcal{R}[-1] \xrightarrow{\mathbf{z}} C$, and similarly for Cone($a\mathbf{z}$). This diagram induces a triangle

$$\mathrm{Cone}(a\mathbf{z}) \to \mathrm{Cone}(\mathbf{z}) \to \mathcal{R}/a\mathcal{R}[0] \to .$$

Recall the group homomorphism $\mathrm{d}_{\mathcal{R}} : K_0(D^{\mathrm{perf}}_{\mathrm{tor}}(\mathcal{R})) \to \mathcal{I}_{\mathcal{R}}$ defined just before Proposition 2.1. Then the above triangle implies

$$\mathrm{d}_{\mathcal{R}}(\mathrm{Cone}(\mathbf{z})) = \mathrm{d}_{\mathcal{R}}(\mathrm{Cone}(a\mathbf{z}))\, \mathrm{d}_{\mathcal{R}}(\mathcal{R}/a\mathcal{R}[0]) = a\, \mathrm{d}_{\mathcal{R}}(\mathrm{Cone}(a\mathbf{z}))$$

in $\mathcal{I}_{\mathcal{R}}$, where the last equality follows from Proposition 2.1.

Now we begin the proof of the lemma. By the assumptions, the module $H^1(C)$ is generically of rank one, so there exists a unique element $u \in \mathrm{Frac}(\mathcal{R})^\times$ such that $\mathbf{z}' = u\mathbf{z}$. We have to show $u \in \mathcal{R}^\times$. We write $u = a/b$ with non-zero-divisors $a, b \in \mathcal{R}$. Then the above observation implies

$$\mathrm{d}_{\mathcal{R}}(\mathrm{Cone}(\mathbf{z})) = a\, \mathrm{d}_{\mathcal{R}}(\mathrm{Cone}(a\mathbf{z})) = \frac{a}{b}\, \mathrm{d}_{\mathcal{R}}\left(\mathrm{Cone}\left(\frac{a}{b}\mathbf{z}\right)\right) = u\, \mathrm{d}_{\mathcal{R}}(\mathrm{Cone}(\mathbf{z}'))$$

in $\mathcal{I}_{\mathcal{R}}$. Since we have $\mathrm{d}_{\mathcal{R}}(\mathrm{Cone}(\mathbf{z})) = \mathrm{d}_{\mathcal{R}}(\mathrm{Cone}(\mathbf{z}'))$ by the assumption, this shows $u \in \mathcal{R}^\times$ as desired. □

Proposition 3.6. *Let C be a perfect complex in $D^{[1,2]}(\mathcal{R})$ and suppose $\chi_{\mathcal{R}}(C) = 1$. Then, for each $\mathbf{z} \in H^1(C)$, the following are equivalent.*

(i) *$\mathbf{z} \in H^1(C)$ is a primitive basic element for C and* $\mathrm{Ann}_{\mathcal{R}}(\mathbf{z}) = 0$.

(ii) *The cone of $\mathcal{R}[-1] \xrightarrow{\mathbf{z}} C$ is in $D^{\mathrm{perf}}_{\mathrm{tor}}(\mathcal{R})$ and moreover represents the zero element in $K_0(D^{\mathrm{perf}}_{\mathrm{tor}}(\mathcal{R}))$.*

Moreover, if these conditions hold, then $H^2(C)$ is torsion as an $\mathcal{R}$-module.

Proof. Let us take a quasi-isomorphism $C \simeq [\mathcal{R}^s \xrightarrow{A} \mathcal{R}^{s-1}]$ and use the same notation as in Proposition 3.4.

Suppose first that (i) holds. Write $\mathbf{z} = \sum_{i=1}^s c_i e_i$ with $c_i \in \mathcal{R}$. By the assumption $\mathrm{Ann}_{\mathcal{R}}(\mathbf{z}) = 0$, it is not hard to show that, by changing the basis of $\mathcal{R}^s$ if necessary, we may assume that $c_1 \in \mathcal{R}$ is a non-zero-divisor. Since the condition (ii) on $\mathbf{z}$ is stable under multiplication by $\mathcal{R}^\times$, by Proposition 3.4, we may also assume that $c_i = (-1)^{i-1}\det(A_i)$ for each i. Since $c_1 = \det(A_1)$ is a non-zero-divisor, we see that $H^2(C)$ is torsion.

In order to show (ii), we observe that the cone of $\mathcal{R}[-1] \xrightarrow{\mathbf{z}} C$ is quasi-isomorphic to the complex

$$C' : \mathcal{R} \xrightarrow{\mathbf{z}} \mathcal{R}^s \xrightarrow{A} \mathcal{R}^{s-1}$$

concentrated in degrees zero, one, and two. Let $\mathrm{pr}_1 : \mathcal{R}^s \to \mathcal{R}$ denote the projection to the first component, and $\mathrm{incl}_1 : \mathcal{R}^{s-1} \to \mathcal{R}^s$ denote the map which sends $(x_2, \dots, x_s) \in \mathcal{R}^{s-1}$ to $(0, x_2, \dots, x_s) \in \mathcal{R}^s$. Let us consider the following commutative diagram

$$\begin{array}{ccccccccc}
 & & & & \mathcal{R}^{s-1} & \xrightarrow{A_1} & \mathcal{R}^{s-1} & & \\
 & & & & \downarrow{\scriptstyle \mathrm{incl}_1} & & \| & & \\
0 & \longrightarrow & \mathcal{R} & \xrightarrow{\mathbf{z}} & \mathcal{R}^s & \xrightarrow{A} & \mathcal{R}^{s-1} & \longrightarrow & 0 \\
 & & \| & & \downarrow{\scriptstyle \mathrm{pr}_1} & & & & \\
 & & \mathcal{R} & \xrightarrow[c_1]{} & \mathcal{R} & & & &
\end{array}$$

which can be regarded as an exact sequence of complexes. Then we obtain

$$[C'] = [0 \to \mathcal{R}^{s-1} \xrightarrow{A_1} \mathcal{R}^{s-1}] + [\mathcal{R} \xrightarrow{c_1} \mathcal{R} \to 0]$$

in $K_0(D^{\mathrm{perf}}_{\mathrm{tor}}(\mathcal{R}))$, where the complexes in the right hand side are also concentrated in degrees zero, one, and two. Using the homomorphism $\varphi_{\mathcal{R}}$ in Proposition 2.1, the two terms in the right hand side are $\varphi_{\mathcal{R}}(\mathrm{Coker}(A_1))$ and $-\varphi_{\mathcal{R}}(\mathcal{R}/c_1\mathcal{R})$, respectively. Then by Proposition 2.1 we have

$$\mathrm{d}_{\mathcal{R}}(C') = \mathrm{Fitt}_{\mathcal{R}}(\mathrm{Coker}(A_1))\,\mathrm{Fitt}_{\mathcal{R}}(\mathcal{R}/c_1\mathcal{R})^{-1} = (1),$$

where the final equation follows from $c_1 = \det(A_1)$. Since $\mathrm{d}_{\mathcal{R}}$ is isomorphic, we have $[C'] = 0$ in $K_0(D^{\mathrm{perf}}_{\mathrm{tor}}(\mathcal{R}))$. Thus (ii) holds.

Suppose (ii). Since the second cohomology of the cone of $\mathcal{R}[-1] \xrightarrow{\mathbf{z}} C$ is $H^2(C)$, the condition (ii) implies that $H^2(C)$ is torsion. Let $\mathbf{z}' \in H^1(C)$ be a primitive basic element for C. Then, by the description in Proposition 3.4, we have $\mathrm{Ann}_{\mathcal{R}}(\mathbf{z}') = 0$. Hence the above discussion implies that $\mathbf{z}'$ also satisfies the condition (ii). Then Lemma 3.5 shows that $\mathbf{z}$ and $\mathbf{z}'$ coincide up to unit, so $\mathbf{z}$ is also a primitive basic element for C. □

3.3. Computing Fitting ideals via primitive basic elements. In this subsection, we show that primitive basic elements have information on the initial Fitting ideals of $H^2(-)$.

The results of this subsection are not essentially novel. Historically, it was Burns-Kurihara-Sano [2] that first obtained the same kind of results, concerning Rubin-Stark elements (see [2, Theorem 7.5]). That striking observation was subsequently generalized by Burns-Sano [5, Section A.1] to more general algebraic situations. The results of this subsection can be regarded as reinterpretations of those preceding works. However, by introducing the notion of primitive basic elements, the formulations become much more clear.

In general, for an element $z \in \bigcap_R^r M$ where M is a finitely generated module over a noetherian ring R, we define $\mathrm{Im}(z)$ as the image of z, regarded as a homomorphism $\bigwedge_R^r M^* \to R$.

Proposition 3.7. *Let R be a zero-dimensional Gorenstein ring. Let $C \in D^{[1,2]}(R)$ be a complex with $r = \chi_R(C) \geq 1$. Let $z \in \bigcap_R^r H^1(C)$ be a primitive basic element. Then we have*

$$\mathrm{Fitt}_R(H^2(C)) = \mathrm{Im}(z)$$

as ideals of R.

Proof. Taking a quasi-isomorphism $C \simeq [R^s \xrightarrow{A} R^{s-r}]$ with $s \geq r$, we can obtain an explicit description of a primitive basic element for C as in Proposition 3.4. Then the proposition follows from that description and the definition of (initial) Fitting ideals. We omit the detail.

See also [5, Proposition A.2(ii)]. □

Corollary 3.8. *Let R be of the form (2.1). Let $C \in D^{[1,2]}(R)$ be a complex with $r = \chi_R(C) \geq 1$. Let $z \in \bigcap_R^r H^1(C)$ be a primitive basic element. For each $j \in J$, we denote by $z_j \in \bigcap_{R_j}^r H^1(C \otimes_R^{\mathbb{L}} R_j)$ the natural image of z. Then we have*

$$\mathrm{Fitt}_R(H^2(C)) = \varprojlim_{j \in J} \mathrm{Im}(z_j)$$

as ideals of R.

Proof. This corollary follows from Proposition 3.7 and $H^2(C) \otimes_R R_j \simeq H^2(C \otimes_R^{\mathbb{L}} R_j)$. □

We shall deduce more explicit formulas from Corollary 3.8 when $r = 1$ and R is either R_F or $\mathcal{R}_F$ for some finite abelian extension $F/\mathbb{Q}$.

For a finitely generated module M over a noetherian ring R, we denote by $\mathrm{ev} : M \to M^{**}$ the natural homomorphism as in Remark 2.4(1). Then we can associate an ideal $\mathrm{Im}(\mathrm{ev}_x)$ of R for each element $x \in M$.

Proposition 3.9. *Let $F/\mathbb{Q}$ be a finite abelian extension. Let $C \in D^{[1,2]}(R_F)$ be a complex with $\chi_{R_F}(C) = 1$. Let $z \in H^1(C)$ be a primitive basic element. Then we have*

$$\mathrm{Fitt}_{R_F}(H^2(C)) = \mathrm{Im}(\mathrm{ev}_z)$$

as ideals of R_F.

Proof. By Corollary 3.8, it is enough to show that

$$\mathrm{Im}(\mathrm{ev}_z) = \varprojlim_m \mathrm{Im}(\mathrm{ev}_{z_m})$$

as ideals of R_F, where $z_m \in H^1(C \otimes_{R_F}^{\mathbb{L}} R_{F,m})$ is the natural image of z.

Let us take a quasi-isomorphism $C \simeq [C^1 \to C^2]$, where both C^1 and C^2 are finitely generated projective over R_F. By definition of the cohomology groups, the cokernel of the injective map $H^1(C) \hookrightarrow C^1$ is a submodule of C^2, so in particular is free over $\mathbb{Z}_p$. Since the R_F-linear dual is isomorphic to the $\mathbb{Z}_p$-linear dual, it follows that the dual map

$$C^{1,*} \to H^1(C)^*$$

is surjective.

For each m, we have $C \otimes_{R_F}^{\mathbb{L}} R_{F,m} \simeq [C^1 \otimes_{R_F} R_{F,m} \to C^2 \otimes_{R_F} R_{F,m}]$. Note that the dual map $(C^1 \otimes_{R_F} R_{F,m})^* \to H^1(C \otimes_{R_F}^{\mathbb{L}} R_{F,m})^*$ is surjective since $R_{F,m}$ is a zero-dimensional Gorenstein ring. Now we consider the natural commutative diagram

$$\begin{array}{ccccc}
C^{1,*} & \twoheadrightarrow & H^1(C)^* & \xrightarrow{\mathrm{ev}_z} & R_F \\
\downarrow & & \downarrow & & \downarrow \\
(C^1 \otimes_{R_F} R_{F,m})^* & \twoheadrightarrow & H^1(C \otimes_{R_F}^{\mathbb{L}} R_{F,m})^* & \xrightarrow[\mathrm{ev}_{z_m}]{} & R_{F,m}.
\end{array}$$

Note that $(-)^*$ means R_F-linear dual (resp. $R_{F,m}$-linear dual) in the upper (resp. lower) sequence. Here, the surjectivities of the two horizontal arrows are already observed, and those of the left and the right vertical arrows are obvious. It follows that the middle vertical arrow is also surjective. Therefore, the claim also follows. □

Finally, we consider $\mathcal{R}_F$. The result is unfortunately not so nice as the previous propositions. For ideals $\mathcal{I}, \mathcal{J}$ of $\mathcal{R}_F$, we write $\mathcal{I} \subset_{\text{fin}} \mathcal{J}$ if $\mathcal{I} \subset \mathcal{J}$ and the quotient $\mathcal{J}/\mathcal{I}$ is finite.

Proposition 3.10. *Let $F/\mathbb{Q}$ be a finite abelian extension. Let $C \in D^{[1,2]}(\mathcal{R}_F)$ be a complex with $\chi_{\mathcal{R}_F}(C) = 1$. Let $\mathbf{z} \in H^1(C)$ be a primitive basic element.*

(1) *We have*

$$\mathrm{Fitt}_{\mathcal{R}_F}(H^2(C)) \subset_{\text{fin}} \mathrm{Im}(\mathrm{ev}_{\mathbf{z}})$$

as ideals of $\mathcal{R}_F$.

(2) *Suppose* $\mathrm{Ann}_{\mathcal{R}_F}(\mathbf{z}) = 0$. *Then we have*

$$\mathrm{Im}(\mathrm{ev}_{\mathbf{z}}) = \mathrm{Fitt}_{\mathcal{R}_F}\left(\mathrm{Ext}^1_{\mathcal{R}_F}\left(\frac{H^1(C)}{\mathcal{R}_F\mathbf{z}}, \mathcal{R}_F\right)\right).$$

Proof. This proposition can be proved in a similar manner as in [9, Theorem 7.11], but we sketch the proof here for convenience. To each the notation, we put $\mathcal{R} = \mathcal{R}_F$ and $R_{m,n} = R_{F_n,m}$ for each m, n.

(1) Let $\mathcal{Z} \subset \mathcal{R}$ be the annihilator ideal of $H^2(C)_{\text{fin}}$, the maximal finite submodule of $H^2(C)$. Let $\pi_{m,n} : \mathcal{R} \to R_{m,n}$ be the natural projection map. Then we shall actually show that

$$\pi_{m,n}\left(\mathcal{Z}\,\mathrm{Im}(\mathrm{ev}_{\mathbf{z}})\right) \subset \mathrm{Im}(\mathrm{ev}_{z_{m,n}}) \subset \pi_{m,n}\left(\mathrm{Im}(\mathrm{ev}_{\mathbf{z}})\right). \tag{3.1}$$

Then (3.1) together with Corollary 3.8 would imply

$$\mathcal{Z}\,\mathrm{Im}(\mathrm{ev}_{\mathbf{z}}) \subset \mathrm{Fitt}_{\mathcal{R}}(H^2(C)) \subset \mathrm{Im}(\mathrm{ev}_{\mathbf{z}}),$$

and (1) would follow.

Let $J_{m,n}$ be the kernel of $\pi_{m,n}$. Then we have an exact sequence

$$0 \to H^2(C)[J_{m,n}] \to H^1(C) \otimes_{\mathcal{R}} R_{m,n} \to H^1(C \otimes^{\mathbb{L}}_{\mathcal{R}} R_{m,n})$$

(see [22, Lemma 6.9]). Note that the last arrow sends $\mathbf{z} \otimes 1$ to $z_{m,n}$. By assuming that m, n are enough large, we have $H^2(C)[J_{m,n}] = H^2(C)_{\text{fin}}$. We then have

$$\mathrm{Im}(\mathrm{ev}_{z_{m,n}}) = \{\Phi(\mathbf{z}) \mid \Phi \in \mathrm{Hom}_{R_{m,n}}(H^1(C) \otimes_{\mathcal{R}} R_{m,n}, R_{m,n}), \Phi|_{H^2(C)_{\text{fin}}} = 0\}.$$

By $C \in D^{[1,2]}(\mathcal{R})$, the cohomology group $H^1(C)$ is the kernel of a homomorphism between finitely generated projective $\mathcal{R}$-modules. As $\mathcal{R}$ is free over the subring $\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/F)]]$, which is a regular local ring of dimension two, it follows that $H^1(C)$ is free over $\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/F)]]$. Then by [9, Lemma 7.15], the natural map

$$\mathrm{Hom}_{\mathcal{R}}(H^1(C), \mathcal{R}) \to \mathrm{Hom}_{R_{m,n}}(H^1(C) \otimes_{\mathcal{R}} R_{m,n}, R_{m,n})$$

is surjective. These observations show the claim (3.1).

(2) Since $H^1(C)/\mathcal{R}\mathbf{z}$ is torsion and $H^1(C)$ is free over $\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/F)]]$, the linear dual of the exact sequence $0 \to \mathcal{R} \xrightarrow{\mathbf{z}} H^1(C) \to \frac{H^1(C)}{\mathcal{R}\mathbf{z}} \to 0$ yields an exact sequence

$$0 \to \mathrm{Hom}_{\mathcal{R}}(H^1(C), \mathcal{R}) \overset{\mathrm{ev}_{\mathbf{z}}}{\to} \mathcal{R} \to \mathrm{Ext}^1_{\mathcal{R}}\left(\frac{H^1(C)}{\mathcal{R}\mathbf{z}}, \mathcal{R}\right) \to 0.$$

Thus we obtain the formula. □

Example 3.11. Fix an isomorphism $\mathcal{R} \simeq \mathbb{Z}_p[\Delta][[T]]$ where Δ is a finite abelian group and T denotes a formal variable. Consider a perfect complex

$$C = \left[\mathcal{R}^2 \overset{(p,T)}{\to} \mathcal{R}\right],$$

where the map sends the basis e_1, e_2 to p, T, respectively. Then, by Proposition 3.4, $\mathbf{z} = Te_1 - pe_2$ is a primitive basic element for C. We also have

$$H^1(C) = \mathcal{R}\mathbf{z}, \qquad H^2(C) = \mathcal{R}/(p,T)\mathcal{R} \simeq \mathbb{F}_p[\Delta].$$

Therefore, in this case, the inclusion stated in Proposition 3.10(1) is not an equality.

Moreover, this example indicates that the ideal $\mathrm{Fitt}_{\mathcal{R}}(H^2(C))$ cannot be described only by the information on the embedding $\mathcal{R}\mathbf{z} \subset H^1(C)$. This is a different phenomenon from Propositions 3.7 and 3.9.

4. Arithmetic complexes

As in Subsection 1.3, we fix a Galois representation T and a finite abelian extension $F/\mathbb{Q}$. In this section, we introduce local and global complexes and review their basic properties. See, e.g., the book [17] by Nekovář as a comprehensive reference.

Throughout this paper, we use the following standard notations. For a field K, we denote by $\mathsf{R}\Gamma(K, -)$ the complex in a derived category whose cohomology groups are the Galois cohomology groups $H^i(K, -) = H^i(\mathrm{Gal}(\overline{K}/K), -)$. More generally, for a Galois extension K'/K of fields, we denote by $\mathsf{R}\Gamma(K'/K, -)$ the complex with cohomology groups $H^i(K'/K, -) = H^i(\mathrm{Gal}(K'/K), -)$.

We often deal with the Galois representations $\mathbb{T}_F$, $T_{F,m}$, and T_F simultaneously. In that case, we denote by $\widetilde{R}$ the coefficient ring $\mathcal{R}_F$, $R_{F,m}$, or R_F, and put $\widetilde{T} = T \otimes_{\mathbb{Z}_p} \widetilde{R}$.

4.1. Local complexes. In this subsection, we fix a prime number $l \notin S_{\mathrm{ram}}(F/\mathbb{Q}) \cup \{p\}$. We do *not* assume that $l \notin S_{\mathrm{bad}}(T)$. Since $\widetilde{T}$ is free over $\widetilde{R}$, it is known that the complex $\mathsf{R}\Gamma(\mathbb{Q}_l, \widetilde{T})$ is perfect over $\widetilde{R}$ and actually in $D^{[0,2]}(\widetilde{R})$ (see e.g. [17, Proposition 4.2.9]). The main purpose of this subsection is to review the finite part $\mathsf{R}\Gamma_f(\mathbb{Q}_l, \widetilde{T})$ and the singular part $\mathsf{R}\Gamma_{/f}(\mathbb{Q}_l, \widetilde{T})$ which will be defined in Definition 4.2 below.

First we reformulate Assumption 1.10.

Lemma 4.1. *The following are equivalent.*

(i) *The $\mathbb{Z}_p$-module $H^0(F_\infty \otimes \mathbb{Q}_l, T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)$ is divisible.*

(ii) *The $\mathbb{Z}_p$-module $H^1(F_\infty \otimes \mathbb{Q}_l, T)$ is torsion-free.*

Proof. Suppose (ii). Then for any $m \geq 0$, the exact sequence $0 \to T \overset{p^m}{\to} T \to T/p^mT \to 0$ induces

$$H^0(F_\infty \otimes \mathbb{Q}_l, T) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p/p^m\mathbb{Z}_p \simeq H^0(F_\infty \otimes \mathbb{Q}_l, T/p^mT).$$

By taking the inductive limit, we obtain

$$H^0(F_\infty \otimes \mathbb{Q}_l, T) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p \simeq H^0(F_\infty \otimes \mathbb{Q}_l, T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p),$$

from which (i) follows.

Suppose (i). Then for any $m \geq 0$, the exact sequence $0 \to T/p^mT \to T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{p^m} T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p \to 0$ induces

$$H^1(F_\infty \otimes \mathbb{Q}_l, T/p^mT) \simeq H^1(F_\infty \otimes \mathbb{Q}_l, T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)[p^m].$$

By taking the projective limit, we obtain

$$H^1(F_\infty \otimes \mathbb{Q}_l, T) \simeq \varprojlim_m H^1(F_\infty \otimes \mathbb{Q}_l, T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)[p^m].$$

Since the p-cohomological dimension of $F_\infty \otimes \mathbb{Q}_l$ is one, the $\mathbb{Z}_p$-module $H^1(F_\infty \otimes \mathbb{Q}_l, T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)$ is divisible. Hence (ii) follows. □

We denote by $\mathbb{Q}_l^{\mathrm{ur}}$ and $\mathbb{Q}_l^{\mathrm{cyc}}$, respectively, the maximal unramified extension of $\mathbb{Q}_l$ and the unramified $\mathbb{Z}_p$-extension of $\mathbb{Q}_l$. Then $\mathbb{Q}_l^{\mathrm{ur}}/\mathbb{Q}_l^{\mathrm{cyc}}$ is a $\prod_{q \neq p} \mathbb{Z}_q$-extension, where q runs over all prime numbers other than p.

Definition 4.2. For each $(\widetilde{R}, \widetilde{T})$ as above, put

$$\begin{aligned} \mathsf{R}\Gamma_f(\mathbb{Q}_l, \widetilde{T}) &= \mathsf{R}\Gamma(\mathbb{Q}_l^{\mathrm{ur}}/\mathbb{Q}_l, H^0(\mathbb{Q}_l^{\mathrm{ur}}, \widetilde{T})) \\ &\simeq \mathsf{R}\Gamma(\mathbb{Q}_l^{\mathrm{cyc}}/\mathbb{Q}_l, H^0(\mathbb{Q}_l^{\mathrm{cyc}}, \widetilde{T})), \end{aligned}$$

where the isomorphism is induced by the inflation. We define $\mathsf{R}\Gamma_{/f}(\mathbb{Q}_l, \widetilde{T})$ by a distinguished triangle

$$\mathsf{R}\Gamma_f(\mathbb{Q}_l, \widetilde{T}) \xrightarrow{\mathrm{Inf}} \mathsf{R}\Gamma(\mathbb{Q}_l, \widetilde{T}) \to \mathsf{R}\Gamma_{/f}(\mathbb{Q}_l, \widetilde{T}) \to . \tag{4.1}$$

We denote by $H^i_f(\mathbb{Q}_l, \widetilde{T})$ and $H^i_{/f}(\mathbb{Q}_l, \widetilde{T})$ the i-th cohomology groups of $\mathsf{R}\Gamma_f(\mathbb{Q}_l, \widetilde{T})$ and $\mathsf{R}\Gamma_{/f}(\mathbb{Q}_l, \widetilde{T})$, respectively. Note that $H^i_f(\mathbb{Q}_l, \widetilde{T})$ is the usual unramified cohomology group.

Lemma 4.3. *Suppose the equivalent conditions in* Lemma 4.1. *Then the following hold.*

(1) *For each $(\widetilde{R}, \widetilde{T})$ as above, we have* $\mathsf{R}\Gamma(\mathbb{Q}_l, \widetilde{T}) \in D^{[0,2]}(\widetilde{R})$, $\mathsf{R}\Gamma_f(\mathbb{Q}_l, \widetilde{T}) \in D^{[0,1]}(\widetilde{R})$, *and* $\mathsf{R}\Gamma_{/f}(\mathbb{Q}_l, \widetilde{T}) \in D^{[1,2]}(\widetilde{R})$.

(2) *Let $\square \in \{\emptyset, f, /f\}$, where $\emptyset$ denotes "no symbol." Then we have isomorphisms*

$$\mathsf{R}\Gamma_\square(\mathbb{Q}_l, \mathbb{T}_F) \otimes^{\mathbb{L}}_{\mathcal{R}_F} R_F \simeq \mathsf{R}\Gamma_\square(\mathbb{Q}_l, T_F),$$
$$\mathsf{R}\Gamma_\square(\mathbb{Q}_l, T_F) \otimes^{\mathbb{L}}_{R_F} R_{F,m} \simeq \mathsf{R}\Gamma_\square(\mathbb{Q}_l, T_{F,m}).$$

(3) *Again let $\square \in \{\emptyset, f, /f\}$. For a subfield F' of F, we have*

$$\mathsf{R}\Gamma_\square(\mathbb{Q}_l, \mathbb{T}_F) \otimes^{\mathbb{L}}_{\mathcal{R}_F} \mathcal{R}_{F'} \simeq \mathsf{R}\Gamma_\square(\mathbb{Q}_l, \mathbb{T}_{F'}).$$

Proof. We first show the following claims:

(i) $H^0(\mathbb{Q}_l^{\mathrm{cyc}}, \mathbb{T}_F)$ is projective over $\mathcal{R}_F$,
(ii) $H^0(\mathbb{Q}_l^{\mathrm{cyc}}, \mathbb{T}_F) \otimes_{\mathcal{R}_F} R_F \simeq H^0(\mathbb{Q}_l^{\mathrm{cyc}}, T_F)$,
(iii) $H^0(\mathbb{Q}_l^{\mathrm{cyc}}, T_F) \otimes_{R_F} R_{F,m} \simeq H^0(\mathbb{Q}_l^{\mathrm{cyc}}, T_{F,m})$.

Note first that $H^0(\mathbb{Q}_l^{\mathrm{cyc}}, \mathbb{T}_F)$ is a direct summand of $H^0(F \otimes \mathbb{Q}_l^{\mathrm{cyc}}, \mathbb{T}_F)$. This is because each component of $F \otimes \mathbb{Q}_l^{\mathrm{cyc}}$ is a finite extension of $\mathbb{Q}_l^{\mathrm{cyc}}$ of order prime to p. We have

$$H^0(F \otimes \mathbb{Q}_l^{\mathrm{cyc}}, \mathbb{T}_F) \simeq H^0(F \otimes \mathbb{Q}_l^{\mathrm{cyc}}, T) \otimes_{\mathbb{Z}_p} \mathcal{R}_F, \tag{4.2}$$

which is clearly free over $\mathcal{R}_F$. Thus (i) follows. Similarly, we also have

$$\begin{aligned} H^0(F \otimes \mathbb{Q}_l^{\mathrm{cyc}}, T_F) &\simeq H^0(F \otimes \mathbb{Q}_l^{\mathrm{cyc}}, T) \otimes_{\mathbb{Z}_p} R_F \\ &\simeq H^0(F \otimes \mathbb{Q}_l^{\mathrm{cyc}}, \mathbb{T}_F) \otimes_{\mathcal{R}_F} R_F. \end{aligned}$$

Thus (ii) follows.

By Assumption 1.10 together with Lemma 4.1, we have

$$H^0(F \otimes \mathbb{Q}_l^{\mathrm{cyc}}, T/p^m T) \simeq H^0(F \otimes \mathbb{Q}_l^{\mathrm{cyc}}, T) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p/p^m\mathbb{Z}_p.$$

Then we have

$$\begin{aligned} H^0(F \otimes \mathbb{Q}_l^{\mathrm{cyc}}, T_{F,m}) &\simeq H^0(F \otimes \mathbb{Q}_l^{\mathrm{cyc}}, T/p^m T) \otimes_{\mathbb{Z}_p/p^m\mathbb{Z}_p} R_{F,m} \\ &\simeq H^0(F \otimes \mathbb{Q}_l^{\mathrm{cyc}}, T) \otimes_{\mathbb{Z}_p} R_{F,m} \\ &\simeq H^0(F \otimes \mathbb{Q}_l^{\mathrm{cyc}}, T_F) \otimes_{R_F} R_{F,m}. \end{aligned}$$

Hence (iii) follows.

Now we begin the proof of the lemma.

(1) As already remarked, we have $\mathsf{R}\Gamma(\mathbb{Q}_l, \widetilde{T}) \in D^{[0,2]}(\widetilde{R})$ by e.g. [17, Proposition 4.2.9]. The same proposition combined with the claims (i)(ii)(iii) shows $\mathsf{R}\Gamma_f(\mathbb{Q}_l, \widetilde{T}) \in D^{[0,1]}(\widetilde{R})$. Since we have $H^i_{/f}(\mathbb{Q}_l, \widetilde{T}) = 0$ unless $i = 1, 2$ for each $\widetilde{T}$, Lemma 2.5 together with the assertion (2) proved below shows that $\mathsf{R}\Gamma_{/f}(\mathbb{Q}_l, \widetilde{T}) \in D^{[1,2]}(\widetilde{R})$.

(2) When $\square = \emptyset$, this follows from [6, Proposition 1.6.5(3)]. The same proposition combined with the claims (i)(ii)(iii) shows the case where $\square = f$. Then by the triangle (4.1), the case where $\square = /f$ also follows.

(3) By (4.2) for F and F', we obtain

$$H^0(F \otimes \mathbb{Q}_l^{\mathrm{cyc}}, \mathbb{T}_F) \otimes_{\mathcal{R}_F} \mathcal{R}_{F'} \simeq H^0(F \otimes \mathbb{Q}_l^{\mathrm{cyc}}, \mathbb{T}_{F'}),$$

so

$$H^0(\mathbb{Q}_l^{\mathrm{cyc}}, \mathbb{T}_F) \otimes_{\mathcal{R}_F} \mathcal{R}_{F'} \simeq H^0(\mathbb{Q}_l^{\mathrm{cyc}}, \mathbb{T}_{F'}).$$

Thus (3) follows again by [6, Proposition 1.6.5(3)]. □

Proposition 4.4. *We have*

$$H^0_f(\mathbb{Q}_l, \mathbb{T}_F) \simeq H^0(\mathbb{Q}_l, \mathbb{T}_F) = 0, \qquad H^1_{/f}(\mathbb{Q}_l, \mathbb{T}_F) = 0.$$

Proof. The first vanishing follows from local Tate duality and the fact that the p-cohomological dimension of $F_\infty \otimes \mathbb{Q}_l$ is one. The second vanishing follows from [21, Proposition B.3.3]. □

4.2. Global complexes. In this subsection, we fix a pair (F, S) as in Subsection 1.3, that is, F is a finite abelian extension of $\mathbb{Q}$ and S is a finite set of finite prime numbers such that $p \notin S$ and $S \cup \{p\} \supset S_{\mathrm{ram}}(F/\mathbb{Q})$. Recall that we put $\overline{S} = S \cup \{p, \infty\}$.

DEFINITION 4.5. For each $(\widetilde{R}, \widetilde{T})$, we define a complex $\mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \widetilde{T})$ by a distinguished triangle

$$\mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \widetilde{T}) \to \mathsf{R}\Gamma(\mathbb{Q}_{\Sigma}/\mathbb{Q}, \widetilde{T}) \to \bigoplus_{l \in \Sigma \setminus \overline{S}} \mathsf{R}\Gamma_{/f}(\mathbb{Q}_l, \widetilde{T}) \to, \tag{4.3}$$

where Σ is a finite set of places of $\mathbb{Q}$ such that $\Sigma \supset \overline{S} \cup S_{\mathrm{bad}}(T)$ and $\mathbb{Q}_\Sigma$ denotes the maximal algebraic extension of $\mathbb{Q}$ which is ramified outside Σ. We denote by $H^i(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \widetilde{T})$ the i-th cohomology group of $\mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \widetilde{T})$.

As the notation implies, this definition does not depend on the choice of Σ, thanks to a distinguished triangle ([17, Proposition (7.8.8)])

$$\mathsf{R}\Gamma(\mathbb{Q}_{\Sigma}/\mathbb{Q}, \widetilde{T}) \to \mathsf{R}\Gamma(\mathbb{Q}_{\Sigma'}/\mathbb{Q}, \widetilde{T}) \to \bigoplus_{l \in \Sigma' \setminus \Sigma} \mathsf{R}\Gamma_{/f}(\mathbb{Q}_l, \widetilde{T}) \to \tag{4.4}$$

for $\Sigma' \supset \Sigma$.

We also recall the Poitou-Tate duality (cf. [17, Proposition (5.4.3)])

$$\mathsf{R}\Gamma(\mathbb{Q}_{\Sigma}/\mathbb{Q}, \widetilde{T}) \to \bigoplus_{l \in \Sigma \setminus \{\infty\}} \mathsf{R}\Gamma(\mathbb{Q}_l, \widetilde{T}) \to \mathsf{R}\Gamma(\mathbb{Q}_{\Sigma}/\mathbb{Q}, \widetilde{T}^\vee(1))^\vee[-2] \to,$$

which induces a triangle

$$\mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \widetilde{T}) \to \bigoplus_{l \in S \cup \{p\}} \mathsf{R}\Gamma(\mathbb{Q}_l, \widetilde{T}) \oplus \bigoplus_{l \in \Sigma \setminus \overline{S}} \mathsf{R}\Gamma_f(\mathbb{Q}_l, \widetilde{T}) \to \mathsf{R}\Gamma(\mathbb{Q}_{\Sigma}/\mathbb{Q}, \widetilde{T}^\vee(1))^\vee[-2] \to . \tag{4.5}$$

Lemma 4.6. *Suppose* Assumption 1.10.

(1) *For each* $(\widetilde{R}, \widetilde{T})$, *we have* $\mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \widetilde{T}) \in D^{[0,2]}(\widetilde{R})$. *Moreover, under* Assumption 1.9, *we have* $\mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \widetilde{T}) \in D^{[1,2]}(\widetilde{R})$.

(2) *We have isomorphisms*

$$\mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \mathbb{T}_F) \otimes^{\mathbb{L}}_{\mathcal{R}_F} R_F \simeq \mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T_F),$$
$$\mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T_F) \otimes^{\mathbb{L}}_{R_F} R_{F,m} \simeq \mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T_{F,m}).$$

(3) *For a subfield F' of F, we have*

$$\mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \mathbb{T}_F) \otimes^{\mathbb{L}}_{\mathcal{R}_F} \mathcal{R}_{F'} \simeq \mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \mathbb{T}_{F'}).$$

Proof. Taking Σ as in Definition 4.5, we have $\mathsf{R}\Gamma(\mathbb{Q}_\Sigma/\mathbb{Q}, \widetilde{T}) \in D^{[0,2]}(\widetilde{R})$ by [17, Proposition 4.2.9]. Then $\mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \widetilde{T})$ is also perfect by Lemma 4.3(1), and is actually in $D^{[0,2]}(\widetilde{R})$. Under Assumption 1.9, we have $H^0(\mathbb{Q}, T_{F_n,m}) = H^0(F_n, T/p^mT) = 0$ for any n, m, so the latter half of (1) follows by Lemma 2.5. The assertions (2)(3) follow from [6, Proposition 1.6.5(3)] and Lemma 4.3(2)(3). □

DEFINITION 4.7. Let $T^\pm$ denote the $\mathbb{Z}_p$-submodule of T on which a complex conjugation acts as ± 1; since p is odd, we have $T = T^+ \oplus T^-$. Similarly, the ring $\mathcal{R}_F$ can be decomposed as $\mathcal{R}_F = \mathcal{R}_F^+ \times \mathcal{R}_F^-$ with respect to the complex conjugation ($\mathcal{R}_F^-$ is the zero ring when F is totally real).

Let $r(T)$ be the locally constant function on $\mathrm{Spec}(\mathcal{R}_F)$ defined by

$$r(T) = \begin{cases} \mathrm{rank}_{\mathbb{Z}_p}(T^-) & (\text{on } \mathrm{Spec}(\mathcal{R}_F^+)) \\ \mathrm{rank}_{\mathbb{Z}_p}(T^+) & (\text{on } \mathrm{Spec}(\mathcal{R}_F^-)). \end{cases}$$

By abuse of notation, $r(T)$ also denotes the similar function on $\mathrm{Spec}(\widetilde{R})$ for $\widetilde{R} = R_F$ or $R_{F,m}$. This $r(T)$ is called the *core rank* of T, by virtue of Proposition 4.8 below.

Proposition 4.8. *Under* Assumption 1.10*, we have*

$$\chi_{\widetilde{R}}(\mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \widetilde{T})) = r(T).$$

Proof. Let F' be the maximal subfield of F such that the degree of $F'/\mathbb{Q}$ is prime to p. By Lemma 4.6, we may assume that $\widetilde{R} = R_{F',1} = \mathbb{F}_p[\mathrm{Gal}(F'/\mathbb{Q})]$, which is a product of finite fields. Over such a ring, the Euler characteristics of complexes are computed by simply counting the dimension of the cohomology groups. Hence the Euler characteristics of the second and the third complexes in (4.3) are computed by the global and local Euler-Poincare characteristic formula [18, (7.3.1), (8.7.4)]. In this way the Euler characteristic of $\mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T_{F',1})$ is computed and we obtain the formula. □

Let us suppose Assumptions 1.9 and 1.10. Then, thanks to Lemma 4.6(1) and Proposition 4.8, the complex $\mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \widetilde{T})$ satisfies the conditions in Definition 3.2. Therefore, for elements of $\bigcap_{\widetilde{R}}^{r(T)} H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \widetilde{T})$, we have the definition of (primitive) basic elements for $\mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \widetilde{T})$.

5. Stark systems

In this section, we define Stark systems and prove a key theorem (Theorem 5.12) that each Stark system yields a basic element for $\mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \mathbb{T}_F)$. The discussion in this section closely follows the works by Burns, Sakamoto, and Sano ([4], [5], [22]), but we make more use of the notion of determinant modules. As in Subsection 1.3, we fix a Galois representation T and a pair (F, S).

5.1. Stark systems over zero-dimensional rings. We fix $m, n \geq 0$ in this subsection. To ease the notation, put

$$R = R_{F_n,m}, \qquad A = T_{F_n,m}.$$

In the theory of Stark systems (also of Euler and of Kolyvagin systems), it is important to play with primes satisfying preferable conditions as follows (see e.g. [4, §3.1]):

DEFINITION 5.1. Let $\mathcal{P}(A)$ be the set of prime numbers $l \notin \overline{S} \cup S_{\mathrm{bad}}(T)$ (recall that $\overline{S} = S \cup \{p, \infty\}$) such that $l \equiv 1 \bmod p^m$ and that $A/(\mathrm{Fr}_l - 1)A$ is a free R-module of rank one, where Fr_l is the l-th power Frobenius automorphism.

Note that, for $l \notin \overline{S} \cup S_{\mathrm{bad}}(T)$, we have an isomorphism

$$H^1_f(\mathbb{Q}_l, A) \simeq A/(\mathrm{Fr}_l - 1)A.$$

It follows from standard facts on local cohomology groups that, for each $l \in \mathcal{P}(A)$, the modules $H^0(\mathbb{Q}_l, A)$, $H^1_f(\mathbb{Q}_l, A)$, $H^1_{/f}(\mathbb{Q}_l, A)$, and $H^2(\mathbb{Q}_l, A)$ are all free of rank one over R.

Definition 5.2. A finite subset $V \subset \mathcal{P}(A)$ is said to be *large* (for A) if the localization map

$$H^1(\mathbb{Q}_\Sigma/\mathbb{Q}, A^\vee(1)) \to \bigoplus_{l\in V} H^1(\mathbb{Q}_l, A^\vee(1))$$

is injective (cf. [5, Definition 3.13]). Here, we put $\Sigma = \overline{S} \cup S_{\mathrm{bad}}(T)$.

Trivially, for finite subsets $V \subset V' \subset \mathcal{P}(A)$, if V is large, then V' is also large.

The following is essential in the theory of Euler systems.

Assumption 5.3 (on F)**.** *For any m, n, there exists a finite subset $V \subset \mathcal{P}(T_{F_n,m})$ which is large (for $T_{F_n,m}$) in the sense of* Definition 5.2.

It is well-known that Assumption 5.3 can be checked by Chebotarev density theorem if we suppose that the image of the Galois representation

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_{\mathbb{Z}_p}(T) \simeq GL_{\mathrm{rank}(T)}(\mathbb{Z}_p)$$

is large enough in a certain sense (see [4, Lemma 3.9]). That is why we suppose Assumption 1.4 in Theorem 1.6.

Now we begin the definition of Stark systems, following [4, §4.1] and [22, Definition 4.2]. Let $r = r(T)$ be the core rank in Definition 4.7.

Definition 5.4. For a finite subset $V \subset \mathcal{P}(A)$, define

$$X_V^r(A) = \bigcap_R^{r+\#V} H^1(\mathbb{Q}_{\overline{S}\cup V}/\mathbb{Q}, A) \otimes_R \mathrm{Det}_R^{-1}\left(\bigoplus_{l\in V} H^1_{/f}(\mathbb{Q}_l, A)\right).$$

Note that $X_V^r(A)$ depends on the choice of S, but we omit S from the notation since no confusion can occur.

For example, we have

$$X_\emptyset^r(A) = \bigcap_R^{r} H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, A). \tag{5.1}$$

For finite subsets $V \subset V'$ of $\mathcal{P}(A)$, by the triangles (4.3) and (4.4), we have a triangle

$$\mathrm{R\Gamma}(\mathbb{Q}_{\overline{S}\cup V}/\mathbb{Q}, A) \to \mathrm{R\Gamma}(\mathbb{Q}_{\overline{S}\cup V'}/\mathbb{Q}, A) \to \bigoplus_{l\in V'\setminus V} \mathrm{R\Gamma}_{/f}(\mathbb{Q}_l, A). \tag{5.2}$$

By taking the first cohomology, we get an exact sequence

$$0 \to H^1(\mathbb{Q}_{\overline{S}\cup V}/\mathbb{Q}, A) \to H^1(\mathbb{Q}_{\overline{S}\cup V'}/\mathbb{Q}, A) \to \bigoplus_{l\in V'\setminus V} H^1_{/f}(\mathbb{Q}_l, A). \tag{5.3}$$

Since the last module is free of rank $\#(V' \setminus V)$, applying Remark 2.4(2) to this sequence induces a homomorphism

$$\bigcap_R^{r+\#V'} H^1(\mathbb{Q}_{\overline{S}\cup V'}/\mathbb{Q}, A) \otimes_R \mathrm{Det}_R^{-1}\left(\bigoplus_{l\in V'\setminus V} H^1_{/f}(\mathbb{Q}_l, A)\right) \to \bigcap_R^{r+\#V} H^1(\mathbb{Q}_{\overline{S}\cup V}/\mathbb{Q}, A).$$

Therefore, we obtain a natural homomorphism $X_{V'}^r(A) \to X_V^r(A)$. Thus we can regard $(X_V^r(A))_{V\subset\mathcal{P}(A)}$ as a projective system.

Definition 5.5. We define the module of Stark systems for A of rank r by

$$\mathrm{SS}_r(A) = \varprojlim_{V \subset \mathcal{P}(A)} X_V^r(A).$$

This module depends on S, but we again omit S from the notation.

By (5.1), we have a canonical map

$$\pi_A : \mathrm{SS}_r(A) \to X_\emptyset^r(A) \simeq \bigcap_R^r H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, A). \tag{5.4}$$

The following is the key theorem of Stark systems over zero-dimensional rings. Recall that, as remarked in the final paragraph of Section 4, we have the notion of (primitive) basic elements under Assumptions 1.9 and 1.10.

Theorem 5.6. *Suppose* Assumptions 1.8, 1.9, 1.10, 1.11, *and* 5.3. *Then the following hold.*

(1) *We have a natural isomorphism*

$$\mathrm{SS}_r(A) \simeq \mathrm{Det}_R^{-1} \mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, A).$$

In particular, $\mathrm{SS}_r(A)$ *is free of rank one over R. A basis of* $\mathrm{SS}_r(A)$ *is called a primitive Stark system.*

(2) *Let $\varepsilon \in \mathrm{SS}_r(A)$ be a (primitive) Stark system. Then $\pi_A(\varepsilon)$ is a (primitive) basic element for* $\mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, A)$.

Remark 5.7. Theorem 5.6(1) is essentially equivalent to [5, Theorem 3.12(ii)]. However, the determinant module in the right hand side is regarded as the module of horizontal determinantal systems in [5], and the proof seems quite different from ours below. According to those differences, it is not easy to deduce Theorem 5.6(2) from their formulations. For that reason, we will give an independent proof which is more suitable to deduce Theorem 5.6(2).

In the rest of this subsection, we prove Theorem 5.6. The following proposition is the key observation.

Proposition 5.8. *Suppose* Assumptions 1.8, 1.9, 1.10, *and* 1.11. *Let $V \subset \mathcal{P}(A)$ be a finite subset which is large in the sense of* Definition 5.2. *Then $H^1(\mathbb{Q}_{\overline{S} \cup V}/\mathbb{Q}, A)$ is a projective module over R of rank $r(T) + \#V$. Moreover, the triangle* (5.2) *(for $(\emptyset, V)$ in the place of (V, V')) induces a quasi-isomorphism*

$$\mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, A) \simeq \left[H^1(\mathbb{Q}_{\overline{S} \cup V}/\mathbb{Q}, A) \to \bigoplus_{l \in V} H^1_{/f}(\mathbb{Q}_l, A) \right],$$

where the right hand side is a perfect complex concentrated in degrees one and two.

Proof. We first show that the connecting homomorphism

$$\bigoplus_{l \in V} H^1_{/f}(\mathbb{Q}_l, A) \to H^2(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, A) \tag{5.5}$$

is surjective. This homomorphism factors through $H^1(\mathbb{Q}_\Sigma/\mathbb{Q}, A^\vee(1))^\vee$ with $\Sigma = \overline{S} \cup S_{\mathrm{bad}}(T)$, so we will prove both the two homomorphisms are surjective. The first map is surjective since the dual map

$$H^1(\mathbb{Q}_\Sigma/\mathbb{Q}, A^\vee(1)) \to \bigoplus_{l \in V} H^1_{/f}(\mathbb{Q}_l, A)^\vee \hookrightarrow \bigoplus_{l \in V} H^1(\mathbb{Q}_l, A^\vee(1))$$

is injective by the definition of V being large. On the other hand, by the triangle (4.5), we have an exact sequence

$$H^1(\mathbb{Q}_\Sigma/\mathbb{Q}, A^\vee(1))^\vee \to H^2(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, A) \to H^2(\mathbb{Q}_p, A) \oplus \bigoplus_{l \in S} H^2(\mathbb{Q}_l, A).$$

By Assumptions 1.8 and 1.11, the final module vanishes. This proves the surjectivity of (5.5).

By Lemma 4.6(1), we have $\mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, A), \mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}\cup V}/\mathbb{Q}, A) \in D^{[1,2]}(R)$. Therefore, the surjectivity of (5.5) implies that the induced homomorphism

$$H^2(\mathbb{Q}_{\overline{S}\cup V}/\mathbb{Q}, A) \to \bigoplus_{l \in V} H^2(\mathbb{Q}_l, A)$$

is isomorphic. Since the right hand side is free (of rank $\#V$) as remarked after Definition 5.1, this shows $H^2(\mathbb{Q}_{\overline{S}\cup V}/\mathbb{Q}, A)$ is free of the same rank. Then $\mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, A) \in D^{[1,2]}(R)$ implies that $H^1(\mathbb{Q}_{\overline{S}\cup V}/\mathbb{Q}, A)$ is also projective. Now the displayed isomorphism implies the proposition. □

Now we begin the proof of Theorem 5.6.

Proof of Theorem 5.6. (1) By Assumption 5.3, in the definition of Stark systems, we may take the limit only for large V in the sense of Definition 5.2. For each large V, Proposition 5.8 and the definition of $X^r_V(A)$ imply an isomorphism

$$X^r_V(A) \simeq \mathrm{Det}_R^{-1} \mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, A). \tag{5.6}$$

Moreover, if $V \subset V' \subset \mathcal{P}(A)$ are large, then the rank counting shows that (5.3) is a short exact sequence of projective modules, so the transition map $X^r_{V'}(A) \to X^r_V(A)$ is isomorphic. Thus we obtain the assertion (1).

(2) Let us take a large finite subset $V \subset \mathcal{P}(A)$. Then we have a commutative diagram

$$\begin{array}{ccccc} \mathrm{SS}_r(A) & \xrightarrow{\sim} & X^r_V(A) & \xrightarrow{\sim} & \mathrm{Det}_R^{-1} \mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, A) \\ & & \downarrow & & \downarrow \Pi_{\mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, A)} \\ & & X^r_\emptyset(A) & = & \bigcap^r_R H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, A) \end{array}$$

by (5.1), (5.6), and the proof of (1). The commutativity follows from the constructions of the maps. Moreover, the composite map coincides with π_A. Now the assertion (2) follows immediately from the definition of (primitive) basic elements. □

Remark 5.9. By combining Theorem 5.6 with Proposition 3.7, we immediately obtain a description of $\mathrm{Fitt}_R(H^2(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, A))$ using a primitive Stark system (we omit the statement). The description is nothing but the formulations of preceding works by Burns, Sakamoto, and Sano ([4, Theorem 4.6]) for initial Fitting ideals. The key idea of this paper is the intermediate statement that each primitive Stark system yields a primitive basic element.

5.2. Stark systems over $\mathcal{R}_F$. In this section, we define Stark systems over $\mathcal{R}_F$ and deduce the main theorem, by applying the discussion in the previous subsection to $R_{F_n,m}$ for various m and n. Put $R_{m,n} = R_{F_n,m}$ and $T_{m,n} = T_{F_n,m}$.

Lemma 5.10. *Let $m' \geq m$ and $n' \geq n$.*
(1) *We have $\mathcal{P}(T_{m',n'}) \subset \mathcal{P}(T_{m,n})$.*
(2) *Suppose* Assumption 1.8. *If a finite subset $V \subset \mathcal{P}(T_{m',n'})$ is large for $T_{m',n'}$, then V is also large for $T_{m,n}$.*

Proof. (1) This is clear from the definition.
(2) Consider the commutative diagram

$$\begin{array}{ccc} H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, (T_{m,n})^\vee(1)) & \longrightarrow & \bigoplus_{l\in V} H^1(\mathbb{Q}_l, (T_{m,n})^\vee(1)) \\ \downarrow & & \downarrow \\ H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, (T_{m',n'})^\vee(1)) & \longrightarrow & \bigoplus_{l\in V} H^1(\mathbb{Q}_l, (T_{m',n'})^\vee(1)) \end{array}$$

The lower horizontal arrow is injective by assumption. The left vertical arrow is injective by Assumption 1.8 (in fact, $H^0(F, (T/pT)^\vee(1)) = 0$ suffices). Hence the upper horizontal arrow is also injective. □

DEFINITION 5.11. Suppose Assumptions 1.8, 1.9, 1.10, 1.11, and 5.3. For $m' \geq m$ and $n' \geq n$, using (the proof of) Theorem 5.6, we define $\mathrm{SS}_r(T_{m',n'}) \to \mathrm{SS}_r(T_{m,n})$ by the commutative diagram

$$\begin{array}{ccc} \mathrm{SS}_r(T_{m',n'}) & \longrightarrow & \mathrm{SS}_r(T_{m,n}) \\ \wr\downarrow & & \downarrow\wr \\ X_V^r(T_{m',n'}) & \longrightarrow & X_V^r(T_{m,n}) \end{array}$$

where V is a finite subset of $\mathcal{P}(T_{m',n'})$ which is large for $T_{m',n'}$ (so also large for $T_{m,n}$ by Lemma 5.10), and the lower horizontal map is the natural map. This map does not depend on the choice of V. We define the module of Stark systems for $\mathbb{T}_F$ by

$$\mathrm{SS}_r(\mathbb{T}_F) = \varprojlim_{m,n} \mathrm{SS}_r(T_{m,n}).$$

By (5.4) for each $A = T_{m,n}$ and Proposition 2.6, we have a canonical map

$$\pi_{\mathbb{T}_F} : \mathrm{SS}_r(\mathbb{T}_F) \to \bigcap_{\mathcal{R}_F}^{r} H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \mathbb{T}_F). \tag{5.7}$$

The following is the key result of this paper.

Theorem 5.12. *Suppose* Assumptions 1.8, 1.9, 1.10, 1.11, *and* 5.3. *Then the following hold.*

(1) *We have an isomorphism*

$$\mathrm{SS}_r(\mathbb{T}_F) \simeq \mathrm{Det}_{\mathcal{R}_F}^{-1} \mathrm{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \mathbb{T}_F).$$

In particular, $\mathrm{SS}_r(\mathbb{T}_F)$ *is free of rank one over* $\mathcal{R}_F$*. A basis of* $\mathrm{SS}_r(\mathbb{T}_F)$ *is again called a primitive Stark system.*

(2) *Let* $\varepsilon \in \mathrm{SS}_r(\mathbb{T}_F)$ *be a (primitive) Stark system. Then* $\pi_{\mathbb{T}_F}(\varepsilon)$ *is a (primitive) basic element for* $\mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \mathbb{T}_F)$*.*

Proof. This theorem follows from Proposition 3.3 and Theorem 5.6. □

6. Application to elliptic curves

As in Subsection 1.1, let $E/\mathbb{Q}$ be an elliptic curve which has good reduction at $p \geq 5$. In this section, by applying the results in the previous sections to $T = T_pE$, we prove Theorem 1.6.

6.1. Review of relevant results. We briefly review some results in [9] and introduce the Beilinson-Kato zeta elements. Let (F, S) be a pair as usual. Throughout we suppose Assumption 1.1.

Recall that $\bullet = \emptyset$ if E is ordinary at p, and $\bullet \in \{+, -\}$ otherwise. We put

$$H^1_{/f}(\mathbb{Q}_p, \mathbb{T}_F)^\bullet = (E^\bullet(F_\infty \otimes \mathbb{Q}_p) \otimes (\mathbb{Q}_p/\mathbb{Z}_p))^\vee,$$

which is an $\mathcal{R}_F$-module with $\mathrm{pd}_{\mathcal{R}_F} \leq 1$. As the notation indicates, we have a natural surjective $\mathcal{R}_F$-homomorphism $H^1(\mathbb{Q}_p, \mathbb{T}_F) \to H^1_{/f}(\mathbb{Q}_p, \mathbb{T}_F)^\bullet$. We denote by $\mathrm{loc}^\bullet_{/f} : H^1(\mathbb{Q}, \mathbb{T}_F) \to H^1_{/f}(\mathbb{Q}_p, \mathbb{T}_F)^\bullet$ the composite of the localization map and the natural map.

On the other hand, in [9, Theorem 1.2], we constructed a $\bullet$-Coleman map

$$\mathrm{Col}^\bullet : H^1_{/f}(\mathbb{Q}_p, \mathbb{T}_F)^\bullet \to \mathcal{R}_F.$$

The kernel and the cokernel of this map is studied in [9]. In particular, for each element $\mathbf{u} \in H^1_{/f}(\mathbb{Q}_p, \mathbb{T}_F)^\bullet$ with $\mathrm{Ann}_{\mathcal{R}_F}(\mathbf{u}) = 0$, we have

$$W^\bullet_F \, \mathrm{Fitt}_{\mathcal{R}_F}\left(\frac{H^1_{/f}(\mathbb{Q}_p, \mathbb{T}_F)^\bullet}{\mathcal{R}_F\mathbf{u}}\right) = (\mathrm{Col}^\bullet(\mathbf{u})) \tag{6.1}$$

as principal ideals of $\mathcal{R}_F$, where $W^\bullet_F$ is the same as in Conjecture 1.2.

By the work [11] by Kato, we have the Beilinson-Kato zeta element

$$\mathbf{z}^{\mathrm{BK}}_{F,S} \in H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \mathbb{T}_F) \otimes \mathbb{Q}_p$$

(we keep the convention in [9, Theorem 6.1]), and these elements $\mathbf{z}^{\mathrm{BK}}_{F,S}$ for various (F, S) constitute an Euler system. The element $\mathbf{z}^{\mathrm{BK}}_{F,S}$ is characterized by a connection with L-values, from which the author [9, Theorem 1.3] obtained the formula

$$\mathrm{Col}^\bullet \circ \mathrm{loc}^\bullet_{/f}(\mathbf{z}^{\mathrm{BK}}_{F,S}) = \mathcal{L}^\bullet_S(E/F_\infty)^\iota, \tag{6.2}$$

where ι denotes the involution on $\mathcal{R}_F$ which inverts every group element. Moreover, if $E[p]$ is irreducible as a Galois representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, then we have $\mathbf{z}^{\mathrm{BK}}_{F,S} \in H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \mathbb{T}_F)$. It also follows that $\mathrm{Ann}_{\mathcal{R}_F}(\mathbf{z}^{\mathrm{BK}}_{F,S}) = 0$, since the right hand side of (6.2) is a non-zero-divisor by the result by Rohrlich [20] on the non-vanishing of L-values.

6.2. Reformulation of the main conjecture. We reformulate the main conjecture (Conjecture 1.2). As remarked in the final paragraph of Section 4, under Assumptions 1.1 and 1.3, we have the notion of (primitive) basic elements.

Conjecture 6.1. *Suppose* Assumptions 1.1 *and* 1.3*. Then* $\mathbf{z}_{F,S}^{\mathrm{BK}}$ *is a primitive basic element for* $\mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \mathbb{T}_F)$.

Proposition 6.2. *Suppose* Assumptions 1.1, 1.3*, and* 1.5*. Then* Conjecture 1.2 *is equivalent to* Conjecture 6.1*. Moreover, the inclusion* $W_F^\bullet \operatorname{Fitt}_{\mathcal{R}_F}(\mathrm{Sel}_S^\bullet(E/F_\infty)^\vee) \supset (\mathcal{L}_S^\bullet(E/F_\infty))$ *is equivalent to that* $\mathbf{z}_{F,S}^{\mathrm{BK}}$ *is a basic element for* $\mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \mathbb{T}_F)$.

In fact, the same equivalence as in Proposition 6.2 holds without assuming Assumption 1.5. However, the proof needs more detailed computation, so we omit that in this paper.

Proof of Proposition 6.2. By Assumption 1.5, the complex $\mathsf{R}\Gamma(\mathbb{Q}_l, \mathbb{T}_F)$ is acyclic for $l \in S$. Then by (4.5) we have a triangle

$$\mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \mathbb{T}_F) \to \mathsf{R}\Gamma(\mathbb{Q}_p, \mathbb{T}_F) \oplus \bigoplus_{l \in \Sigma \setminus \overline{S}} \mathsf{R}\Gamma_f(\mathbb{Q}_l, \mathbb{T}_F) \to \mathsf{R}\Gamma(\mathbb{Q}_\Sigma/\mathbb{Q}, \mathbb{T}_F^\vee(1))^\vee[-2] \to .$$

The cohomology groups of the middle (resp. the right) complex vanish except for degree one, by Proposition 4.4 (resp. the validity of the weak Leopoldt conjecture $H^2(\mathbb{Q}_\Sigma/\mathbb{Q}, \mathbb{T}_F^\vee(1)) = 0$). Hence (by Proposition 4.4) we have a quasi-isomorphism

$$\mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \mathbb{T}_F) \simeq \left[H^1(\mathbb{Q}_p, \mathbb{T}_F) \oplus \bigoplus_{l \in \Sigma \setminus \overline{S}} H^1(\mathbb{Q}_l, \mathbb{T}_F) \to H^1(\mathbb{Q}_\Sigma/\mathbb{Q}, \mathbb{T}_F^\vee(1))^\vee \right], \tag{6.3}$$

where the right hand side is a complex concentrated in degrees one and two.

As in [9, Proposition 5.6], the Selmer group $\mathrm{Sel}_S^\bullet(E/F_\infty)$ in (1.1) fits in an exact sequence

$$0 \to H^1_f(\mathbb{Q}_p, \mathbb{T}_F)^\bullet \oplus \bigoplus_{l \in \Sigma \setminus \overline{S}} H^1(\mathbb{Q}_l, \mathbb{T}_F) \to H^1(\mathbb{Q}_\Sigma/\mathbb{Q}, \mathbb{T}_F^\vee(1))^\vee \to \mathrm{Sel}_S^\bullet(E/F_\infty)^\vee \to 0,$$

where we put $H^1_f(\mathbb{Q}_p, \mathbb{T}_F)^\bullet = \operatorname{Ker}\left(H^1(\mathbb{Q}_p, \mathbb{T}_F) \to H^1_{/f}(\mathbb{Q}_p, \mathbb{T}_F)^\bullet\right)$. Then, by taking the quotient of the two modules in the right hand side of (6.3) by $H^1_f(\mathbb{Q}_p, \mathbb{T}_F)^\bullet \oplus \bigoplus_{l \in \Sigma \setminus \overline{S}} H^1(\mathbb{Q}_l, \mathbb{T}_F)$, we obtain a quasi-isomorphism

$$\mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \mathbb{T}_F) \simeq \left[H^1_{/f}(\mathbb{Q}_p, \mathbb{T}_F)^\bullet \to \mathrm{Sel}_S^\bullet(E/F_\infty)^\vee \right]. \tag{6.4}$$

Let $\mathbf{z} \in H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \mathbb{T}_F)$ be any primitive basic element for $\mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \mathbb{T}_F)$. Since $H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \mathbb{T}_F)$ is generically of rank one, there exists a unique element $u \in \operatorname{Frac}(\mathcal{R})^\times$ such that $\mathbf{z}_{F,S}^{\mathrm{BK}} = u\mathbf{z}$. By Proposition 3.6 and (6.4), the complex

$$\left[\frac{H^1_{/f}(\mathbb{Q}_p, \mathbb{T}_F)^\bullet}{\mathcal{R}_F \operatorname{loc}^\bullet_{/f}(\mathbf{z})} \to \mathrm{Sel}_S^\bullet(E/F_\infty)^\vee \right]$$

represents the zero element in $K_0(D^{\mathrm{perf}}_{\mathrm{tor}}(\mathcal{R}_F))$. By Proposition 2.1, this implies the first equality of

$$\operatorname{Fitt}_{\mathcal{R}_F}(\mathrm{Sel}_S^\bullet(E/F_\infty)^\vee) = \operatorname{Fitt}_{\mathcal{R}_F}\left(\frac{H^1_{/f}(\mathbb{Q}_p, \mathbb{T}_F)^\bullet}{\mathcal{R}_F \operatorname{loc}^\bullet_{/f}(\mathbf{z})} \right) = u^{-1} \operatorname{Fitt}_{\mathcal{R}_F}\left(\frac{H^1_{/f}(\mathbb{Q}_p, \mathbb{T}_F)^\bullet}{\mathcal{R}_F \operatorname{loc}^\bullet_{/f}(\mathbf{z}_{F,S}^{\mathrm{BK}})} \right),$$

where the second follows from the choice of u. By Assumption 1.5 and [9, Corollary 7.7], we have $(\mathcal{L}_S(E/F_\infty)^\iota) = (\mathcal{L}_S(E/F_\infty))$ as principal ideals of $\mathcal{R}_F$. Then (6.1) and (6.2) show

$$W_F^\bullet \operatorname{Fitt}_{\mathcal{R}_F}\left(\frac{H^1_{/f}(\mathbb{Q}_p, \mathbb{T}_F)^\bullet}{\mathcal{R}_F \operatorname{loc}^\bullet_{/f}(\mathbf{z}^{\mathrm{BK}}_{F,S})}\right) = (\mathcal{L}_S(E/F_\infty)).$$

Therefore, the ideal $W_F^\bullet \operatorname{Fitt}_{\mathcal{R}_F}(\operatorname{Sel}^\bullet_S(E/F_\infty)^\vee)$ coincides with (resp. contains) the ideal $(\mathcal{L}_S(E/F_\infty))$ if and only if $u \in \mathcal{R}^\times$ (resp. $u \in \mathcal{R}$), that is, if and only if $\mathbf{z}^{\mathrm{BK}}_{F,S}$ is a primitive basic element (resp. a basic element). This completes the proof. □

6.3. Proof of Theorem 1.6. Now we can prove the main theorem of this paper.

Under Assumptions 1.1, 1.3, 1.4, and 1.5, the assumptions in Theorem 5.12 hold. Therefore, we have an $\mathcal{R}_F$-module $\mathrm{SS}_1(\mathbb{T}_F)$, which is free of rank one, and a natural map

$$\pi_{\mathbb{T}_F} : \mathrm{SS}_1(\mathbb{T}_F) \to H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \mathbb{T}_F)$$

as in (5.7). Another key ingredient for the proof of Theorem 1.6 is the following result by Burns, Sakamoto, and Sano.

Theorem 6.3. *Suppose* Assumptions 1.1, 1.3, 1.4, *and* 1.5. *Then* $\mathbf{z}^{\mathrm{BK}}_{F,S}$ *is a component of a Stark system, namely, is in the image of* $\pi_{\mathbb{T}_F}$.

Proof. We can directly apply the results of [4] that each Euler system gives rise to a Stark system via a Kolyvagin system. We refer to [9, §7.2] for the verifications of various assumptions in [4]. □

Corollary 6.4. *Suppose* Assumptions 1.1, 1.3, 1.4, *and* 1.5. *Then* $\mathbf{z}^{\mathrm{BK}}_{F,S}$ *is a basic element for* $\mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \mathbb{T}_F)$.

Proof. This corollary follows from Theorems 5.12 and 6.3. □

Proof of Theorem 1.6. Now the theorem follows immediately from Corollary 6.4 and Proposition 6.2. □

REMARK 6.5. We compare the proof of Theorem 1.6 in this paper with that in [9] under $\mu = 0$. The quasi-isomorphism (6.4) induces an exact sequence

$$0 \to H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \mathbb{T}_F) \xrightarrow{\operatorname{loc}^\bullet_{/f}} H^1_{/f}(\mathbb{Q}_p, \mathbb{T}_F)^\bullet \to \operatorname{Sel}^\bullet_S(E/F_\infty)^\vee \to H^2(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \mathbb{T}_F) \to 0. \tag{6.5}$$

Suppose that $\mathbf{z}^{\mathrm{BK}}_{F,S}$ is a basic element for $\mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \mathbb{T}_F)$, as shown by Corollary 6.4 under the assumptions. Let $u \in \mathcal{R}_F$ be an element such that $\mathbf{z}^{\mathrm{BK}}_{F,S}$ is u times a primitive basic element. Then by Proposition 3.10, we have

$$u \operatorname{Fitt}_{\mathcal{R}_F}(H^2(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \mathbb{T}_F)) \subset_{\mathrm{fin}} \operatorname{Fitt}_{\mathcal{R}_F}\left(\operatorname{Ext}^1_{\mathcal{R}_F}\left(\frac{H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \mathbb{T}_F)}{\mathcal{R}_F \mathbf{z}^{\mathrm{BK}}_{F,S}}, \mathcal{R}_F\right)\right), \tag{6.6}$$

for (not necessarily principal) ideals. On the other hand, the inclusion ⊃ in Conjecture 1.2 is equivalent to

$$\operatorname{Fitt}_{\mathcal{R}_F}(\operatorname{Sel}^\bullet_S(E/F_\infty)^\vee) \supset \operatorname{Fitt}_{\mathcal{R}_F}\left(\frac{H^1_{/f}(\mathbb{Q}_p, \mathbb{T}_F)^\bullet}{\mathcal{R}_F \operatorname{loc}^\bullet_{/f}(\mathbf{z}^{\mathrm{BK}}_{F,S})}\right) \tag{6.7}$$

for principal ideals.

The sequence (6.5) indicates that (6.6) and (6.7) are closely related. In fact, (6.7) implies (6.6). However, the problem is that (6.6) does not imply (6.7) in general, unless we have $\mu = 0$ for $H^2(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \mathbb{T})$. In [9], we first showed (6.6) by a direct application of results of Burns-Sakamoto-Sano, and then we deduced (6.7) under $\mu = 0$. In this paper, we did not use (6.6) but instead we showed (6.7) directly.

7. Application to a work of Burns-Kurihara-Sano

We again consider the p-adic Tate module $T = T_pE$ associated to an elliptic curve $E/\mathbb{Q}$ which has good reduction at $p \geq 5$. In this section, we review the conjectures by Burns-Kurihara-Sano [3] and obtain an interpretation of them (see the diagram (7.7) below).

In this section, we fix (F, S) as in Subsection 1.3 and suppose Assumptions 1.1 and 1.3. Actually, we may weaken Assumption 1.1 to that the group $E(F \otimes \mathbb{Q}_p)$ is p-torsion-free.

In this section we always work under the following (one half of Conjecture 6.1).

Assumption 7.1 (on F). *The element* $\mathbf{z}_{F,S}^{\mathrm{BK}}$ *is a basic element for* $\mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \mathbb{T}_F)$.

Under Assumptions 1.4 and 1.5 (in addition to Assumptions 1.1 and 1.3), we have already shown (in Corollary 6.4) that Assumption 7.1 holds. Therefore, under those assumptions, the results in this section would be unconditional.

7.1. Further reformulation of main conjecture. We suppose Assumption 7.1. Note that we have a commutative diagram

$$\begin{array}{ccc}
\mathrm{Det}_{\mathcal{R}_F}^{-1} \mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \mathbb{T}_F) & \overset{\Pi_{F_\infty}}{\hookrightarrow} & H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \mathbb{T}_F) \\
\downarrow{\scriptstyle N_{F_\infty/F}} & & \downarrow \\
\mathrm{Det}_{R_F}^{-1} \mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T_F) & \underset{\Pi_F}{\longrightarrow} & H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T_F),
\end{array}$$

where Π_{F_∞} and Π_F are the homomorphisms in Definition 3.2, and the vertical arrows are the natural maps. Here, Π_{F_∞} is injective by Assumption 7.1 and $\mathrm{Ann}_{\mathcal{R}_F}(\mathbf{z}_{F,S}^{\mathrm{BK}}) = 0$.

DEFINITION 7.2. We define $\mathfrak{z}_{F_\infty,S} \in \mathrm{Det}_{\mathcal{R}_F}^{-1} \mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \mathbb{T}_F)$ as the unique element such that

$$\Pi_{F_\infty}(\mathfrak{z}_{F_\infty,S}) = \mathbf{z}_{F,S}^{\mathrm{BK}}$$

in $H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \mathbb{T}_F)$. We also define $\mathfrak{z}_{F,S} = N_{F_\infty/F}(\mathfrak{z}_{F_\infty,S}) \in \mathrm{Det}_{R_F}^{-1} \mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T_F)$. It follows that

$$\Pi_F(\mathfrak{z}_{F,S}) = z_{F,S}^{\mathrm{BK}}$$

in $H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T_F)$, where $z_{F,S}^{\mathrm{BK}} \in H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T_F)$ is the image of $\mathbf{z}_{F,S}^{\mathrm{BK}}$. However, this formula does not characterize $\mathfrak{z}_{F,S}$ since Π_F is not injective in general.

Proposition 7.3. *Suppose* Assumption 7.1 *for F. Then the following are equivalent.*

(i) Conjecture 6.1 *holds for F.*

(ii) *The element $\mathfrak{z}_{F_\infty,S}$ is a basis of* $\mathrm{Det}_{\mathcal{R}_F}^{-1} \mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \mathbb{T}_F)$.

(iii) *The element $\mathfrak{z}_{F,S}$ is a basis of* $\mathrm{Det}_{R_F}^{-1} \mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T_F)$.

Proof. (i) ⇔ (ii) is clear. (ii) ⇔ (iii) follows from Nakayama's lemma. □

Proposition 7.4. *Suppose* Assumption 7.1 *for* F. *Let* F' *be a subfield of* F *such that* F/F' *is a* p*-extension. Then* Conjecture 6.1 *for* F' *is equivalent to* Conjecture 6.1 *for* F.

Proof. We use the second (or the third) formulation in Proposition 7.3. Then the proposition follows from Nakayama's lemma again. □

In particular, we may take F' as the subfield of F such that F/F' is a p-extension and $[F' : \mathbb{Q}]$ is prime to p. Then Proposition 7.4 says that *equivariant main conjectures can be deduced from non-equivariant main conjectures*. This phenomenon is also observed by Kurihara [14, Theorem 6].

7.2. Existence of Darmon-type derivative. In this and the next subsections, we apply our discussion in this paper to the recent paper [3] by Burns-Kurihara-Sano.

Put $G_F = \mathrm{Gal}(F/\mathbb{Q})$, so $R_F = \mathbb{Z}_p[G_F]$. Let I_F be the augmentation ideal of R_F, which is by definition the kernel of $R_F \to \mathbb{Z}_p$. According to [3, Hypothesis 2.2], throughout we suppose the following.

Assumption 7.5. *The following hold.*
(1) $E(F)[p] = 0$.
(2) *The Mordell-Weil rank satisfies* $\mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q})) \geq 1$.
(3) *The Tate-Shafarevich group* $Ш(E/\mathbb{Q})$ *is finite.*

Actually in this subsection Assumption 7.5(3) may be weakened to the finiteness of $Ш(E/\mathbb{Q})[p^\infty]$, but the stronger hypothesis will be used in Subsection 7.3. We denote by $t = \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q})$ the Mordell-Weil rank, which is denoted by $r = r_{\mathrm{alg}}$ in [3]. Note that Assumption 7.5(1) implies that $H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T_F)$ is $\mathbb{Z}_p$-free.

Definition 7.6. Define a $\mathbb{Z}_p$-homomorphism

$$\mathcal{N}_F : H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T_F) \to H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T_F) \otimes_{\mathbb{Z}_p} R_F$$

by

$$\mathcal{N}_F(z) = \sum_{\sigma \in G_F} \sigma(z) \otimes \sigma^{-1}.$$

It is easy to check that

$$\mathcal{N}_F(az) = \sum_{\sigma \in G_F} \sigma(z) \otimes a\sigma^{-1} \tag{7.1}$$

for each $a \in R_F$.

We have a natural (restriction) map

$$H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T) \to H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T_F).$$

By Assumption 7.5(1), this is an injective map between $\mathbb{Z}_p$-free modules and its cokernel is also $\mathbb{Z}_p$-free. Hence this map induces an *injective* map

$$\iota_F : H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T) \otimes_{\mathbb{Z}_p} (I_F^{t-1}/I_F^t) \to H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T_F) \otimes_{\mathbb{Z}_p} (R_F/I_F^t).$$

For each $z \in H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T_F)$, the image of $\mathcal{N}_F(z)$ in the target module of ι_F is again denoted by $\mathcal{N}_F(z)$.

Definition 7.7. The Darmon-type derivative of $z_{F,S}^{\mathrm{BK}}$ is an element $\kappa_{F,S} \in H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T) \otimes_{\mathbb{Z}_p} (I_F^{t-1}/I_F^t)$ satisfying

$$\iota_F(\kappa_{F,S}) = \mathcal{N}_F(z_{F,S}^{\mathrm{BK}})$$

in $H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T_F) \otimes_{\mathbb{Z}_p} (R_F/I_F^t)$. If such an element exists, then it is unique.

As discussed in [3, Sections 4.1 and 4.2], they conjecture that the Darmon-type derivative of $z_{F,S}^{\mathrm{BK}}$ actually exists. However, they could provide only partial evidences for the existence. In this paper, we prove the conjecture under our running (mild) assumptions as in Corollary 7.9 below.

Theorem 7.8. *Consider the composite*

$$\mathrm{Det}_{R_F}^{-1} \mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T_F) \xrightarrow{\Pi_F} H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T_F) \xrightarrow{\mathcal{N}_F} H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T_F) \otimes_{\mathbb{Z}_p} (R_F/I_F^t).$$

Then the image of $\mathcal{N}_F \circ \Pi_F$ is contained in the image of ι_F.

The statement of Theorem 7.8 will be complemented in Theorem 7.11. Before the proof, we state an immediate consequence.

Corollary 7.9. *Under* Assumption 7.1*, the predicted element $\kappa_{F,S}$ exists. Therefore, under the assumptions as in* Corollary 6.4*, the same conclusion holds.*

Proof of Theorem 7.8. As in Proposition 3.4, take a quasi-isomorphism $\mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T_F) \simeq [R_F^s \xrightarrow{A} R_F^{s-1}]$. Let $e_1, \dots, e_s$ and $f_1, \dots, f_{s-1}$ be the standard bases of R_F^s and R_F^{s-1}, respectively. Then we have $\mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T) \simeq [\mathbb{Z}_p^s \xrightarrow{\overline{A}} \mathbb{Z}_p^{s-1}]$, where $\overline{A}$ denotes A modulo I_F. Since $H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T)$ is a free $\mathbb{Z}_p$-module of rank t (see (7.6) below), by changing the basis necessary, we may assume that

$$\mathrm{Ker}(\overline{A}) = \mathbb{Z}_p^t \oplus 0 \subset \mathbb{Z}_p^s.$$

In other words, we have $\overline{A}\overline{e_1} = \cdots = \overline{A}\overline{e_t} = 0$, where $\overline{e_1}, \dots, \overline{e_s}$ is the standard basis of $\mathbb{Z}_p^s$. This means that every component of A in the t columns from the first is in I_F. Therefore, we have

$$\begin{aligned} &\det(A_1), \dots, \det(A_t) \in I_F^{t-1}, \\ &\det(A_{t+1}), \dots, \det(A_s) \in I_F^t. \end{aligned} \tag{7.2}$$

Now we compute $\mathcal{N}_F \circ \Pi_F$. By Proposition 3.4, we can compute in $R_F^s \otimes_{\mathbb{Z}_p} (R_F/I_F^t)$ as follows:

$$\begin{aligned} &\mathcal{N}_F \circ \Pi_F((e_1 \wedge \cdots \wedge e_s) \otimes (f_1^* \wedge \cdots \wedge f_{s-1}^*)) \\ &= \mathcal{N}_F\left(\sum_{i=1}^s (-1)^{i-1} \det(A_i) e_i\right) \\ &= \sum_{i=1}^s (-1)^{i-1} \mathcal{N}_F(\det(A_i) e_i) \end{aligned}$$

$$\overset{(7.1)}{=} \sum_{i=1}^{s} (-1)^{i-1} \sum_{\sigma \in G_F} \sigma e_i \otimes \det(A_i) \sigma^{-1}$$

$$\overset{(7.2)}{=} \sum_{i=1}^{t} (-1)^{i-1} \sum_{\sigma \in G_F} \sigma e_i \otimes \det(A_i).$$

The final formula is equal to the image under ι_F of

$$\sum_{i=1}^{t} (-1)^{i-1} \overline{e_i} \otimes \det(A_i) \in H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T) \otimes_{\mathbb{Z}_p} I_F^{t-1}.$$

This completes the proof. □

REMARK 7.10. By Assumption 7.1 and Proposition 3.9, we obtain

$$\mathrm{Fitt}_{R_F}(H^2(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T_F)) \supset \{\Phi(z_{F,S}^{\mathrm{BK}}) \mid \Phi \in \mathrm{Hom}_{R_F}(H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T_F), R_F)\}.$$

The equality holds under Conjecture 6.1. Since the $\mathbb{Z}_p$-rank of $H^2(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T_F) \otimes_{R_F} \mathbb{Z}_p \simeq H^2(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T)$ is $t-1$, it follows that

$$\{\Phi(z_{F,S}^{\mathrm{BK}}) \mid \Phi \in \mathrm{Hom}_{R_F}(H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T_F), R_F)\} \subset I_F^{t-1}. \tag{7.3}$$

An idea in [3, Section 4.1] is to use a statement like (7.3) in order to prove the existence of $\kappa_{F,S}$. Our idea in Theorem 7.8 is that we should use the more refined fact that $z_{F,S}^{\mathrm{BK}}$ is a basic element.

In fact, the proof of Theorem 7.8 is inspired by the computation in [3, Section 7]; more precisely, by the proof of the commutative diagram [3, (7.4.1)]. In that paper, they deal with only fields contained in the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty$ of $\mathbb{Q}$. From our perspective, we can obtain a similar commutative diagram for general $F/\mathbb{Q}$:

Theorem 7.11. *We have a commutative diagram*

(7.4)

$$\begin{array}{ccccc}
\mathrm{Det}_{R_F}^{-1} \mathrm{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T_F) & \xrightarrow{\Pi_F} & H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T_F) & & \\
\downarrow{\scriptstyle N_{F/\mathbb{Q}}} & & & \searrow{\scriptstyle \mathcal{N}_F} & \\
\mathrm{Det}_{\mathbb{Z}_p}^{-1} \mathrm{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T) & \xrightarrow[\mathrm{Boc}_F]{} & H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T) \otimes_{\mathbb{Z}_p} (I_F^{t-1}/I_F^t) & \xhookrightarrow[\iota_F]{} & H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T_F) \otimes_{\mathbb{Z}_p} (R_F/I_F^t)
\end{array}$$

Here, $N_{F/\mathbb{Q}}$ is the natural map and Boc_F *is the Bockstein homomorphism, which is a slight modification of the definition in* [3].

We omit the proof, but we stress that the computation in the proof of Theorem 7.8 is essential in the proof of the commutativity.

In [3], an intensive study is done for the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty$ of $\mathbb{Q}$. Let $I_{\mathbb{Q}_\infty}$ be the augmentation ideal of $\mathcal{R}_{\mathbb{Q}} = \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]]$. By taking the projective limit of (7.4), we obtain a commutative diagram

$$\begin{array}{ccccc} \mathrm{Det}^{-1}_{\mathcal{R}_{\mathbb{Q}}} \mathrm{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \mathbb{T}_{\mathbb{Q}}) & \overset{\Pi_{\mathbb{Q}_\infty}}{\hookrightarrow} & H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, \mathbb{T}_{\mathbb{Q}}) & & \\ \downarrow N_{\mathbb{Q}_\infty/\mathbb{Q}} & & & \searrow \mathcal{N}_{\mathbb{Q}_\infty} & \\ \mathrm{Det}^{-1}_{\mathbb{Z}_p} \mathrm{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T) & \underset{\mathrm{Boc}_{\mathbb{Q}_\infty}}{\longrightarrow} & H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T) \otimes_{\mathbb{Z}_p} (I^{t-1}_{\mathbb{Q}_\infty}/I^t_{\mathbb{Q}_\infty}) & \underset{\iota_{\mathbb{Q}_\infty}}{\hookrightarrow} & \varprojlim_n H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T_{\mathbb{Q}_n}) \otimes_{\mathbb{Z}_p} (R_{\mathbb{Q}_n}/I^t_{\mathbb{Q}_n}) \end{array}$$

It is expected that the homomorphism $\mathrm{Boc}_{\mathbb{Q}_\infty}$ is injective. In fact, [3] shows that the injectivity is equivalent to the non-vanishing of a certain p-adic regulator.

7.3. Various conjectures. In this subsection, we recall the conjectures in [3] and reinterpret them from our perspective. We keep Assumption 7.5.

7.3.1. Birch–Swinnerton-Dyer conjecture and Tamagawa number conjecture. Keep in mind that in this subsubsection the field $\mathbb{Q}$ plays the role of F in the proceeding parts of this paper.

First we recall the Birch–Swinnerton-Dyer conjecture. The (strong) BSD conjecture states

$$\text{(BSD)} \qquad \frac{L^*(E,1)}{\Omega_E \cdot \mathrm{Reg}_E} = \frac{c(E)\#Ш(E/\mathbb{Q})}{\#E(\mathbb{Q})^2_{\mathrm{tor}}},$$

where

- $L^*(E,1)$ is the leading coefficient of $L(E,s)$ at $s=1$;
- $\Omega_E = \Omega_E^+$ is the Néron period;
- Reg_E is the regulator;
- $c(E) = \prod_v c_v(E)$ is the Tamagawa factor.

Here, we fix a Néron differential ω_E (up to sign) and define Ω_E as the image of ω_E under the period map

$$(7.5) \qquad \Gamma(E, \Omega^1_{E/\mathbb{Q}}) \to \mathbb{C}, \qquad \omega \mapsto \int_{E(\mathbb{R})} |\omega|.$$

We shall review the definitions of elements $\eta_S^{\mathrm{an}}, \eta_S^{\mathrm{alg}}$ in [3, Definitions 2.4 and 2.17] (denoted by $\eta_{\mathbf{x}}^{\mathrm{BSD}}, \eta_{\mathbf{x}}^{\mathrm{alg}}$).

Let S be a finite set of prime numbers $\neq p$. As in [3, (2.2.1), (2.2.2)], we have a natural isomorphism

$$(7.6) \qquad \mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T) \simeq \mathbb{Q}_p \otimes_{\mathbb{Z}} E(\mathbb{Q})$$

and a natural exact sequence

$$0 \to (\mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T))^* \to \mathbb{Q}_p \otimes_{\mathbb{Z}} E(\mathbb{Q}) \to \mathbb{Q} \otimes_{\mathbb{Z}} E(\mathbb{Q}_p) \to 0.$$

These give rise to the second isomorphism in the following sequence of isomorphisms:

$$\begin{aligned} \lambda : & \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathrm{Det}^{-1}_{\mathbb{Z}_p} \mathrm{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T) \\ & \simeq \bigwedge_{\mathbb{Q}_p}^{t} (\mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^1(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T)) \otimes_{\mathbb{Q}_p} \bigwedge_{\mathbb{Q}_p}^{t-1} (\mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^2(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T))^* \end{aligned}$$

$$\simeq \bigwedge_{\mathbb{Q}_p}^{t}(\mathbb{Q}_p \otimes_{\mathbb{Z}} E(\mathbb{Q})) \otimes_{\mathbb{Q}_p} \bigwedge_{\mathbb{Q}_p}^{t}(\mathbb{Q}_p \otimes_{\mathbb{Z}} E(\mathbb{Q}))^* \otimes_{\mathbb{Q}_p} (\mathbb{Q} \otimes_{\mathbb{Z}} E(\mathbb{Q}_p))$$
$$\simeq \mathrm{Det}_{\mathbb{Q}_p}(\mathbb{Q}_p \otimes_{\mathbb{Z}} E(\mathbb{Q})) \otimes_{\mathbb{Q}_p} \mathrm{Det}_{\mathbb{Q}_p}(\mathbb{Q}_p \otimes_{\mathbb{Z}} E(\mathbb{Q})) \otimes_{\mathbb{Q}_p} (\mathbb{Q}_p \otimes_{\mathbb{Z}} \Gamma(E, \Omega^1_{E/\mathbb{Q}}))$$
$$\simeq \mathbb{Q}_p \otimes_{\mathbb{Z}} \left(\mathrm{Det}_{\mathbb{Z}}(E(\mathbb{Q})) \otimes_{\mathbb{Z}} \mathrm{Det}_{\mathbb{Z}}(E(\mathbb{Q})) \otimes_{\mathbb{Z}} \Gamma(E, \Omega^1_{E/\mathbb{Q}})\right),$$

where the third isomorphism is induced by the dual exponential map

$$\exp^* : (\mathbb{Q}_p \otimes_{\mathbb{Z}} E(\mathbb{Q}_p))^* \xrightarrow{\sim} \mathbb{Q}_p \otimes_{\mathbb{Z}} \Gamma(E, \Omega^1_{E/\mathbb{Q}}).$$

Definition 7.12. Let S be a finite set of prime numbers $\neq p$. We define $\eta_S^{\mathrm{an}} \in \mathbb{C}_p \otimes_{\mathbb{Z}_p} \mathrm{Det}^{-1}_{\mathbb{Z}_p} \mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T)$ by

$$\lambda(\eta_S^{\mathrm{an}}) = \frac{L^*_{S\cup\{p\}}(E,1)}{\Omega_E \cdot \mathrm{Reg}_E} \cdot (x_1 \wedge \cdots \wedge x_t) \otimes (x_1 \wedge \cdots \wedge x_t) \otimes \omega_E,$$

where $x_1, \ldots, x_t \in E(\mathbb{Q})$ is a basis of $E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tor}}$ (the right hand side is independent from the choice of $x_1, \ldots, x_t$). Here we fix an isomorphism $\mathbb{C} \simeq \mathbb{C}_p$ to regard the coefficient in the right hand side as an element of $\mathbb{C}_p$. Then the period map (7.5) and the Néron-Tate height pairing

$$\mathrm{Det}_{\mathbb{Q}}(E(\mathbb{Q})_{\mathbb{Q}}) \otimes \mathrm{Det}_{\mathbb{Q}}(E(\mathbb{Q})_{\mathbb{Q}}) \to \mathbb{R}, \qquad (y_1 \wedge \cdots \wedge y_t) \otimes (y'_1 \wedge \cdots \wedge y'_t) \mapsto \det(\langle y_i, y'_j \rangle)_{i,j}$$

send $\lambda(\eta_S^{\mathrm{an}})$ to $L^*_{S\cup\{p\}}(E,1)$.

As an algebraic counterpart, we define $\eta_S^{\mathrm{alg}} \in \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathrm{Det}^{-1}_{\mathbb{Z}_p} \mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T)$ by

$$\lambda(\eta_S^{\mathrm{alg}}) = \left(\prod_{l \in S\cup\{p\}} P_l(l^{-1})\right) \frac{c(E)\#\text{Ш}(E/\mathbb{Q})}{\#E(\mathbb{Q})^2_{\mathrm{tor}}} \cdot (x_1 \wedge \cdots \wedge x_t) \otimes (x_1 \wedge \cdots \wedge x_t) \otimes \omega_E.$$

Here, for each prime l (possibly $l = p$), we put

$$P_l(X) = \det(1 - \mathrm{Fr}_l X \mid T_p E^{I_l}) = 1 - a_l(E)X + \mathbf{1}_{N_E}(l) l X^2,$$

where $\mathbf{1}_{N_E}(l) = 1$ if $l \notin S_{\mathrm{bad}}(E)$ and $\mathbf{1}_{N_E}(l) = 0$ if $l \in S_{\mathrm{bad}}(E)$, so that $P_l(l^{-1})$ is the Euler factor at l of the L-function $L(E,s)$ for $s = 1$.

By definition, (BSD) is equivalent to $\eta_S^{\mathrm{an}} = \eta_S^{\mathrm{alg}}$, which is independent from S. On the other hand, Tamagawa number conjecture states that

(TNC) $\qquad \eta_S^{\mathrm{an}}$ is a $\mathbb{Z}_p$-basis of $\mathrm{Det}^{-1}_{\mathbb{Z}_p} \mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T)$

(see [3, proof of Proposition 2.6]), which is again independent from S.

Proposition 7.13. *For each finite set S of prime numbers $\neq p$, the element η_S^{alg} is a $\mathbb{Z}_p$-basis of* $\mathrm{Det}^{-1}_{\mathbb{Z}_p} \mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T)$.

Proof. This proposition is well-known. See [12] as a detailed reference. □

By Proposition 7.13, the conjecture (TNC) is equivalent to (BSD) up to $\mathbb{Z}_p^\times$.

7.3.2. Generalized Perrin-Riou conjecture and refined Mazur-Tate conjecture. Let (F, S) be as usual. Recall the diagram in Theorem 7.11. Then the generalized Perrin-Riou conjecture [3, Conjecture 2.12] claims that

$$\text{(gPRC)}_F \qquad \mathcal{N}_F(z_{F,S}^{\mathrm{BK}}) = \iota_F \circ \mathrm{Boc}_F(\eta_S^{\mathrm{an}}).$$

Similarly, the refined Mazur-Tate conjecture [3, Conjecture 2.19] claims that

$$\text{(rMTC)}_F \qquad \mathcal{N}_F(z_{F,S}^{\mathrm{BK}}) = \iota_F \circ \mathrm{Boc}_F(\eta_S^{\mathrm{alg}}).$$

Keep Assumption 7.1. By Theorem 7.8, we have the Darmon-type derivative $\kappa_{F,S}$ and thus (gPRC)_F (resp. (rMTC)_F) can be restated as $\kappa_{F,S} = \mathrm{Boc}_F(\eta_S^{\mathrm{an}})$ (resp. $\kappa_{F,S} = \mathrm{Boc}_F(\eta_S^{\mathrm{alg}})$).

We shall obtain a further reformulation. Recall that in Definition 7.2 we defined an element $\mathfrak{z}_{F,S} \in \mathrm{Det}_{R_F}^{-1} \mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T_F)$ such that $\Pi_F(\mathfrak{z}_{F,S}) = z_{F,S}^{\mathrm{BK}}$. We propose conjectures

$$\text{(gPRC)} \qquad \mathfrak{z}_{\mathbb{Q},S} = \eta_S^{\mathrm{an}}$$

and

$$\text{(rMTC)} \qquad \mathfrak{z}_{\mathbb{Q},S} = \eta_S^{\mathrm{alg}}.$$

Then all of (gPRC)_F, (rMTC)_F, (gPRC), and (rMTC) are independent from the choice of S.

Proposition 7.14. *Suppose that the homomorphism* $\mathrm{Boc}_{\mathbb{Q}_\infty}$ *is injective. Then the following are equivalent.*

(i) *(gPRC) (resp. (rMTC)) holds.*

(ii) *(gPRC)_F (resp. (rMTC)_F) holds for any finite abelian extension $F/\mathbb{Q}$.*

(iii) *(gPRC)_F (resp. (rMTC)_F) holds for any intermediate number field F of $\mathbb{Q}_\infty/\mathbb{Q}$.*

Proof. By Theorem 7.11, we have

$$\mathcal{N}_F(z_{F,S}^{\mathrm{BK}}) = \iota_F \circ \mathrm{Boc}_F \circ N_{F/\mathbb{Q}}(\mathfrak{z}_{F,S}) = \iota_F \circ \mathrm{Boc}_F(\mathfrak{z}_{\mathbb{Q},S}).$$

Therefore, (gPRC)_F (resp. (rMTC)_F) is equivalent to that $\eta_S^{\mathrm{an}} - \mathfrak{z}_{\mathbb{Q},S}$ (resp. $\eta_S^{\mathrm{alg}} - \mathfrak{z}_{\mathbb{Q},S}$) is in the kernel of Boc_F. Thus (i) $\Rightarrow$ (ii) holds. Trivially we have (ii) $\Rightarrow$ (iii). Finally, by the injectivity of $\mathrm{Boc}_{\mathbb{Q}_\infty}$, we have $\cap_n \mathrm{Ker}(\mathrm{Boc}_{\mathbb{Q}_n}) = 0$. Hence we have (iii) $\Rightarrow$ (i). □

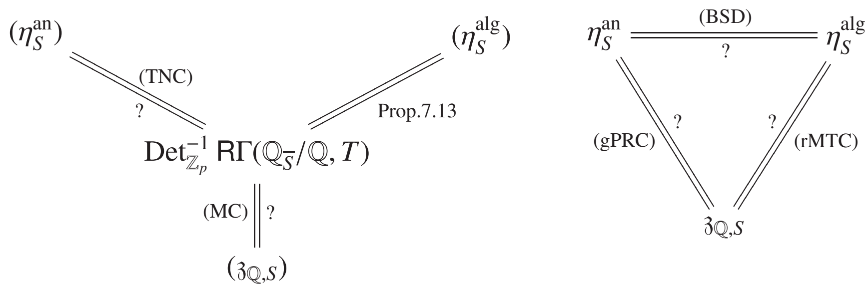
Note that, in [3, Conjecture 4.9 (resp. Conjecture 4.16)], the assertion (iii) is called the infinite analogue of the generalized Perrin-Riou conjecture (resp. the refined Mazur-Tate conjecture). Proposition 7.14 gives simple interpretations of those conjectures in [3].

7.3.3. Relations among conjectures. Keep Assumption 7.1. By Propositions 7.3 and 7.4, our main conjecture (Conjecture 6.1) for p-extensions $F/\mathbb{Q}$ is equivalent to

$$\text{(MC)} \qquad \mathfrak{z}_{\mathbb{Q},S} \text{ is a } \mathbb{Z}_p\text{-basis of } \mathrm{Det}_{\mathbb{Z}_p}^{-1} \mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T).$$

We can illustrate the relations between these conjectures in the following diagrams:

(7.7)



The left diagram concerns $\mathbb{Z}_p$-submodules of $\mathbb{C}_p \otimes_{\mathbb{Z}_p} \mathrm{Det}_{\mathbb{Z}_p}^{-1} \mathsf{R}\Gamma(\mathbb{Q}_{\overline{S}}/\mathbb{Q}, T)$, and the right concerns elements of it.

These diagrams (7.7) are so nice that we can deduce some main results of [3] at once. For example, we can deduce [3, Theorem 7.3] ((MC) implies (rMTC) up to $\mathbb{Z}_p^\times$) and [3, Theorem 7.6] ((MC) and (gPRC) imply (BSD) up to $\mathbb{Z}_p^\times$).

Acknowledgements. I am grateful to Masato Kurihara for his continuous support during the research. I also thank Takamichi Sano for various comments on earlier versions of this paper (e.g. the term “basic” was suggested by him). Thanks are also due to the anonymous referees for providing a number of suggestions. This research was supported by JSPS KAKENHI Grant Number 19J00763.

References

[1] Y. Amice and J. Vélu: *Distributions p-adiques associées aux séries de Hecke*; in Journées Arithmétiques de Bordeaux (Conf., Univ. Bordeaux, Bordeaux, 1974), Astérisque **24–25** (1975), 119–131.

[2] D. Burns, M. Kurihara and T. Sano: *On zeta elements for* $\mathbb{G}_m$, Doc. Math. **21** (2016), 555–626.

[3] D. Burns, M. Kurihara and T. Sano: *On derivatives of Kato's Euler system for elliptic curves*, arXiv:1910.07404.

[4] D. Burns, R. Sakamoto and T. Sano: *On the theory of higher rank Euler, Kolyvagin and Stark systems, II*, arXiv:1805.08448.

[5] D. Burns and T. Sano: *On the theory of higher rank Euler, Kolyvagin and Stark systems*, to appear in Int. Math. Res. Notices.

[6] T. Fukaya and K. Kato: *A formulation of conjectures on p-adic zeta functions in noncommutative Iwasawa theory*; in Proceedings of the St. Petersburg Mathematical Society. Vol. XII, Amer. Math. Soc. Transl. Ser. 2, **219** (2006), Amer. Math. Soc., Providence, RI, 1–85.

[7] R. Greenberg and V. Vatsal: *On the Iwasawa invariants of elliptic curves*, Invent. Math. **142** (2000), 17–63.

[8] C. Greither, T. Kataoka and M. Kurihara: *Fitting ideals of p-ramified Iwasawa modules over totally real fields*, arXiv:2006.05667.

[9] T. Kataoka: *Equivariant Iwasawa theory for elliptic curves*, to appear in Mathematische Zeitschrift.

[10] T. Kataoka: *Fitting ideals in two-variable equivariant Iwasawa theory and an application to CM elliptic curves*, to appear in Tokyo J. Math.

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

[12] G. Kings: *The equivariant Tamagawa number conjecture and the Birch–Swinnerton-Dyer conjecture*; in Arithmetic of L-functions, IAS/Park City Math. Ser. **18** (2011), Amer. Math. Soc., Providence, RI, 315–349.

[13] S. Kobayashi: *Iwasawa theory for elliptic curves at supersingular primes*, Invent. Math. **152** (2003), 1–36.

[14] M. Kurihara: *The structure of Selmer groups of elliptic curves and modular symbols*; in Iwasawa theory 2012, Contrib. Math. Comput. Sci. **7**, Springer, Heidelberg, 2014, 317–356.

[15] B. Mazur and K. Rubin: Kolyvagin systems, Mem. Amer. Math. Soc. **168** (2004), 799.

[16] B. Mazur, J. Tate and J. Teitelbaum: *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **84** (1986), 1–48.

[17] J. Nekovář: Selmer complexes, Astérisque **310**, 2006.

[18] J. Neukirch, A. Schmidt and K. Wingberg: Cohomology of number fields, second edition, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], **323**, Springer-Verlag, Berlin, 2008.

[19] R. Pollack: *On the p-adic L-function of a modular form at a supersingular prime*, Duke Math. J. **118** (2003), 523–558.

[20] D.E. Rohrlich: *On L-functions of elliptic curves and cyclotomic towers*, Invent. Math. **75** (1984), 409–423.

[21] K. Rubin: Euler systems, Annals of Mathematics Studies **147**, Princeton University Press, Princeton, NJ, 2000.

[22] R. Sakamoto: *Stark systems over Gorenstein local rings*, Algebra Number Theory **12** (2018), 2295–2326.

[23] R. Sakamoto: *A higher rank Euler system for the multiplicative group over a totally real field*, arXiv:2002.04871.

[24] M.M. Višik: *Nonarchimedean measures associated with Dirichlet series*, Mat. Sb. (N.S.) **99(141)** (1976), 248–260, 296.

Faculty of Science and Technology, Keio University
3–14–1 Hiyoshi, Kohoku-ku
Yokohama, Kanagawa 223–8522
Japan
e-mail: tkataoka@math.keio.ac.jp