Münster J. of Math. **7** (2014), 149–223
urn:nbn:de:hbz:6-22359593713

Münster Journal of Mathematics

Refined Iwasawa theory for p-adic representations and the structure of Selmer groups

Masato Kurihara

(Communicated by Christopher Deninger)

Dedicated to Peter Schneider on his 60th birthday

Abstract. In this paper, we develop the idea in [16] to obtain finer results on the structure of Selmer modules for p-adic representations than the usual main conjecture in Iwasawa theory. We determine the higher Fitting ideals of the Selmer modules under several assumptions. Especially, we describe the structure of the classical Selmer group of an elliptic curve over $\mathbf{Q}$, using the ideals defined from modular symbols. We also develop the theory of Euler systems and Kolyvagin systems of Gauss sum type.

1. Introduction

1.1. One of the most important and fascinating themes in number theory is to pursue the relationship between the arithmetic objects and the zeta values (L-values). In Iwasawa theory, such relationship is described by the main conjecture, or its variant, the computation of the initial Fitting ideal of the Selmer groups. In this paper, we prove the existence of finer relationship than such main conjectures.

Our strategy is to assume the main conjecture, and to study more detailed information on the Selmer groups. We assume that our p-adic representation V is coming from a critical motive over $\mathbf{Q}$, and it is good ordinary at p. In order to avoid the argument becoming unnecessarily complicated, we restrict ourselves to study the case of the cyclotomic $\mathbf{Z}_p$-extension $\mathbf{Q}_\infty/\mathbf{Q}$ though our method can be applied to a more general setting. We adopt Greenberg's definition of the Selmer group over the cyclotomic $\mathbf{Z}_p$-extension $\mathbf{Q}_\infty$ given in [6], and study the structure of the Selmer group $\mathrm{Sel}(\mathbf{Q}_\infty, A)$ where $A = T \otimes \mathbf{Q}_p/\mathbf{Z}_p$ for some $\mathbf{Z}_p$-lattice T of V (see Subsection 2.1).

Put $\Lambda = \mathbf{Z}_p[[\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})]]$ for the moment. If the Pontrjagin dual $\mathrm{Sel}(\mathbf{Q}_\infty, A)^\vee$ has no nontrivial finite Λ-submodule, we know that $\mathrm{Sel}(\mathbf{Q}_\infty, A)^\vee$

has a presentation $0 \longrightarrow \Lambda^a \xrightarrow{f} \Lambda^a \longrightarrow \mathrm{Sel}(\mathbf{Q}_\infty, A)^\vee \longrightarrow 0$. Let $\mathcal{A}$ be the square matrix corresponding to the Λ-homomorphism f. The main conjecture in the generalized Iwasawa theory for $(V, \mathbf{Q}_\infty/\mathbf{Q})$ by Greenberg is the statement that $\det \mathcal{A}$ coincides with the p-adic L-function up to unit. What we really want to do is to know not only $\det \mathcal{A}$ but also $\mathcal{A}$ itself (up to conjugation) from the analytic information on V, namely the zeta values (L-values). Very roughly speaking, we construct in this paper elements $x_{m,\ell}$ in a certain cohomology group from which we get equations of the form $\mathcal{A}\mathbf{x} = \mathbf{y}$ where $\mathbf{x}$, $\mathbf{y}$ are vectors in Λ^a and some components of $\mathbf{x}$, $\mathbf{y}$ are described by zeta values. We get information on $\mathcal{A}$ from the above equations. This element $x_{m,\ell}$ is a modification of a Kolyvagin system $\kappa_{m,\ell}$ of Gauss sum type on which we will explain a little in this introduction later. (In the proof of Theorem B, we use $\kappa_{m,\ell}$ instead of $x_{m,\ell}$.)

We use the (higher) Fitting ideals to formulate our results. In the above context, the i-th Fitting ideal is the ideal of Λ generated by all $(a-i)\times(a-i)$ minors of $\mathcal{A}$ for any i such that $0 \leq i < a$. The initial Fitting ideal (namely the case $i = 0$) of $\mathrm{Sel}(\mathbf{Q}_\infty, A)^\vee$ is generated by $\det \mathcal{A}$, so by the p-adic L-function if we assume the main conjecture. We first consider the case that V is not self-dual. More precisely, we assume the condition (C) in Subsection 9.1. In this situation we will prove in Theorem A that all higher Fitting ideals of the Selmer module are determined by analytic elements, namely some elements coming from p-adic L-functions.

We will state our theorem. We assume that $\mathcal{F}_\wp$ is a local field such that $\mathcal{F}_\wp/\mathbf{Q}_p$ is finite and unramified, and that V is an $\mathcal{F}_\wp$-vector space on which $G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts $\mathcal{F}_\wp$-linearly and continuously. We take an O-lattice T where O is the integer ring of $\mathcal{F}_\wp$, and consider $A = V/T$. We put $\Lambda = O[[\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})]]$, and study the Λ-module $\mathrm{Sel}(\mathbf{Q}_\infty, A)^\vee$. A very simple example is $V = \mathbf{Q}_p(\chi)$ where χ is an odd Dirichlet character of order prime to p such that $\chi \neq \omega$.

For any $i \geq 0$ we define the higher Stickelberger ideal Θ_i of Λ in Subsection 4.3, using the p-adic L-functions over the cyclotomic $\mathbf{Z}_p$-extension K_∞ for many K which are abelian p-extensions of $\mathbf{Q}$. Under certain assumptions, we determine all higher Fitting ideals of $\mathrm{Sel}(\mathbf{Q}_\infty, A)^\vee$, which will give us much finer information on the structure of the Selmer group as a $\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})$-module than the usual main conjecture.

Theorem A. *We assume (I), (II-1), (II-3), (III) (especially the main conjecture), (I)* in Subsection 2.1, (IV-1), (IV-2), (IV-3) in Subsection 5.1, (V-1), (V-2) in Subsection 5.8, and (C) in Subsection 9.1. Then we have*

$$\mathrm{Fitt}_{i,\Lambda}(\mathrm{Sel}(\mathbf{Q}_\infty, A)^\vee) = \Theta_i$$

for all $i \geq 0$.

The assumptions of Theorem A are satisfied for $V = \mathbf{Q}_p(\chi)$ where χ is an odd Dirichlet character of order prime to p such that $\chi \neq \omega$ and $\chi(p) \neq 1$.

This case was treated in our previous paper [16], so Theorem A is a generalization of the main result in [16] to a p-adic representation satisfying some conditions. (In [16, Rem. 2.2(4)], we announced that the condition $\chi(p) \neq 1$ can be removed, but it was premature and we still need this assumption to get the above equality.)

This theorem determines the structure of the ψ-quotient $\mathrm{Sel}(\mathbf{Q}_\infty, A)^\vee \otimes_\Lambda \mathbf{Z}_p[\mathrm{Image}\,\psi]$ completely for any character ψ of $\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})$ including $\psi = 1$ because knowing the higher Fitting ideals is equivalent to knowing the structure over a discrete valuation ring. Mazur and Rubin have a structure theorem ([19, Thm. 4.5.9]) for the Selmer group over a discrete valuation ring. The difference between our theorem and their theorem is that the structure is described by analytic objects in our theorem, and the analytic elements in Θ_i can be numerically computable, in principle, at least for the ideal class groups of CM-fields and for the Selmer groups of elliptic modular forms.

1.2. First of all, we will determine the initial Fitting ideal of certain cohomology groups. For an abelian p-extension $K/\mathbf{Q}$ satisfying some conditions, we will study a certain Selmer module $H^1_{\mathrm{Gr}}(O_{K_\infty}[1/S], A)^\vee$ as an $O[[\mathrm{Gal}(K_\infty/\mathbf{Q}]]$-module in Section 3. We will prove that it is of projective dimension at most 1 and that the initial Fitting ideal is generated by a certain p-adic L-function

$$\mathrm{Fitt}_{0,\Lambda_{K_\infty}}(H^1_{\mathrm{Gr}}(O_{K_\infty}[1/S], A)^\vee) = (\xi_{K_\infty,S}) \tag{1}$$

(see Theorem 3.4 and Corollary 3.5). Using (1), we get an annihilation result

$$\theta_K H^1_{\mathrm{Gr}}(O_K, A)^\vee = 0$$

(see Theorem 6.7). Using (1), we also prove the inclusion from right to left in Theorem A (see Corollary 4.5). We also get the modulo p^N-version of this inclusion (see Corollary 6.5), which is useful for numerical computations (see Subsection 10.15).

1.3. In this paper we develop the theory of Euler systems and Kolyvagin systems of Gauss sum type. The Euler system of Gauss sums was studied as a very important example in the fundamental work of Kolyvagin [12], but it seems to the author that the theory of Euler systems of Gauss sum type has been neglected after Kolyvagin's work. This theory of Euler systems and Kolyvagin systems is used to obtain the other inclusion of Theorem A. We proceed by following the argument in [16] where we studied the ideal class groups. The author suggests the readers who are not familiar with this topic to take a look at the paper [16] at first where we treated the classical setting because it would be helpful to understand the whole picture. (Section 4 in this paper corresponds to Sections 8 and 9 in [16], Section 6 in this paper corresponds to Section 4 in [16], Section 7 in this paper corresponds to Sections 5 and 6 in [16], and Section 9 in this paper corresponds to Section 10 in [16].)

But there appear many differences between our general case and the ideal class group case treated in [16], and many difficulties occur. One of the difficulties lies in the fact that "the tame part" in the cohomology group is very

small in general. (In the class group case, it is the whole.) By this reason, we always work over mod p^N cohomologies. We first construct an Euler system g_ℓ of Gauss sum type, using the annihilation result we mentioned above (g_ℓ corresponds to the Gauss sum supported over a prime above ℓ). Although the usual Gauss sum is almost characterized by the prime decomposition, our element g_ℓ is not characterized by the corresponding property, and we need more properties to define g_ℓ. This element g_ℓ is a very subtle element and lives only in mod p^N cohomology, namely the cohomology with coefficients in T^*/p^N, and there is no corresponding element in the cohomology with coefficients in T^* where $T^* = \mathrm{Hom}(A, \mathbf{Q}_p/\mathbf{Z}_p(1))$ is a Galois representation which is a free $\mathbf{Z}_p$-module of finite rank.

Using this g_ℓ, we construct $\kappa_{m,\ell}$, a Kolyvagin system of Gauss sum type for a positive integer m and a prime ℓ satisfying certain conditions by a similar strategy as in [16], but by a different method which is needed because we always work over mod p^N cohomologies. We take m, ℓ such that $m\ell$ is a squarefree product whose prime divisors are all in $\mathcal{P}_1$ which is defined in Subsection 5.8. (The Kolyvagin derivative $\kappa_{m,\ell}$ is defined by the usual method if ℓ satisfies some condition (see Proposition 7.7), but we need $\kappa_{m,\ell}$ for $\ell \in \mathcal{P}_1$. It is not straightforward to define $\kappa_{m,\ell}$ from g_ℓ for a prime $\ell \in \mathcal{P}_1$, see Subsection 7.10.) These elements satisfy the following four important properties;

(1) $\partial_r(\kappa_{m,\ell}) = \phi_r(\kappa_{\frac{m}{r},\ell})$ for any prime divisor r of m,
(2) $\partial_\ell(\kappa_{m,\ell}) = \delta_m$,
(3) $\phi_r(\kappa_{m,\ell}) = 0$ for any prime divisor r of m,
(4) $\phi_\ell(\kappa_{m,\ell}) = -\delta_{m\ell}$,

where ∂_r is a "boundary map", ϕ_r is a kind of "reciprocity map", and δ_m, $\delta_{m\ell}$ are elements defined from the values of L-functions (∂_r is the divisor map and ϕ_r is the reciprocity map in the classical setting in [16]; for the precise definition and properties of these maps and these elements, see Section 7 and Propositions 7.13, 7.15, 7.16). Property (1) is a usual property of Euler system, Property (3) is a property of Kolyvagin system which was discovered by Mazur and Rubin [19], and (2), (4) are new properties for our Kolyvagin systems. They describe the relations between our Kolyvagin systems and zeta values. Property (2) is deduced directly from the definition. Property (4) is the deepest among these 4 properties, and is a beautiful property of our Euler system. We note that the standard argument cannot be applied even for the proof of Property (1) since our Euler system is not a usual Euler system but a "finite" Euler system (namely, this Euler system exists only over a finite extension of number fields, and does not extend to an infinite extension; for example, our Euler system does not give a norm compatible system for a $\mathbf{Z}_p$-extension). In the usual theory of Euler systems, it is very difficult to compute the order of the Kolyvagin derivative κ_m. But we get some information on $\kappa_{m,\ell}$ from the Properties (2) and (4) in our theory, because the elements δ_m, $\delta_{m\ell}$ are computable in several cases. This is an advantage of our Euler (Kolyvagin) system of Gauss sum type.

Finally we construct elements $x_{m,\ell}$ using these Kolyvagin systems by the same method as [16]. Then these elements $x_{m,\ell}$ yield information on the matrix $\mathcal{A}$, which is then used in order to prove Theorem A.

1.4. The above Theorem A cannot be applied to the Tate module $V = V_p(E)$ of an elliptic curve E over $\mathbf{Q}$ because V is self-dual (it does not satisfy (C)). The main reason why the above argument does not work for $V_p(E)$ is that we cannot apply Proposition 9.3 which is an argument using the Chebotarev density theorem. In fact, the equality between the higher Fitting ideal and the higher Stickelberger ideal does not hold in this case. (This fact is also related to the functional equation of the p-adic L-functions, see the end of Subsection 10.15.) In this paper, we study only the case that V is the Tate module of an elliptic curve instead of studying general self-dual motives, for simplicity. We cannot prove a theorem over Λ in this case, and only prove a structure theorem of the classical Selmer group over $\mathbf{Q}$.

Suppose that E is an elliptic curve defined over $\mathbf{Q}$, p is a good ordinary prime > 2, p does not divide $\mathrm{Tam}(E)$, the action of $G_{\mathbf{Q}}$ is surjective on $T_p(E)$, the μ-invariant of $(E, \mathbf{Q}_\infty/\mathbf{Q})$ is zero, and p is not anomalous ($\#E(\mathbf{F}_p) \not\equiv 0 \pmod p$). We also assume that the p-adic height pairing is nondegenerate, and use the main conjecture for $(E, \mathbf{Q}_\infty/\mathbf{Q})$, which was proved by Skinner and Urban [34] under mild conditions. We define the ideals $\Theta_i(\mathbf{Q})$ of $\mathbf{Z}_p$ by the same method as above, which can be computed by using modular symbols (see Subsection 10.15). Actually, in this case $\Theta_i(\mathbf{Q})$ is essentially generated by some analytic elements $\tilde{\delta}_m$ which can be computed by modular symbols (see (53) and (65)). In this setting, we prove the following structure theorem on the (classical) Selmer group $\mathrm{Sel}(\mathbf{Q}, E[p^\infty])$ with respect to $E[p^\infty]$. This theorem says that the structure of the Selmer group is completely determined by the ideals $\Theta_i(\mathbf{Q})$.

Theorem B. *If* $\operatorname{rank} \mathrm{Sel}(\mathbf{Q}, E[p^\infty])^\vee = r$ *(*$\in \mathbf{Z}_{\geq 0}$*), we have*

$$\Theta_0(\mathbf{Q}) = \cdots = \Theta_{r-1}(\mathbf{Q}) = 0$$

and

$$\mathrm{Fitt}_{i,\mathbf{Z}_p}(\mathrm{Sel}(\mathbf{Q}, E[p^\infty])^\vee) = \Theta_i(\mathbf{Q})$$

for any $i \geq r$ *such that* $i \equiv r \pmod 2$*. More concretely, suppose that* $\mathrm{Sel}(\mathbf{Q}, E[p^\infty])^\vee$ *is generated by exactly* a *elements. We write* $\Theta_i(\mathbf{Q}) = p^{n_i}\mathbf{Z}_p$ *for some* $n_i \in \mathbf{Z}_{\geq 0} \cup \{\infty\}$ *for each* $i \in \mathbf{Z}_{\geq 0}$*. Then we have*

$$\begin{aligned} &n_0 = \cdots = n_{r-1} = \infty, \\ &n_r = \mathrm{ord}_p(\#(\mathrm{Sel}(\mathbf{Q}, E[p^\infty])^\vee)_{\mathrm{tors}}), \\ &n_a = 0, \end{aligned}$$

and

$$(\mathrm{Sel}(\mathbf{Q}, E[p^\infty])^\vee)_{\mathrm{tors}} \simeq (\mathbf{Z}/p^{\frac{n_r - n_{r+2}}{2}})^{\oplus 2} \oplus (\mathbf{Z}/p^{\frac{n_{r+2} - n_{r+4}}{2}})^{\oplus 2} \oplus \cdots \oplus (\mathbf{Z}/p^{\frac{n_{a-2} - n_a}{2}})^{\oplus 2}.$$

Concerning $\Theta_i(\mathbf{Q})$ for i such that $i \not\equiv r \pmod 2$, we have

$$\Theta_i(\mathbf{Q}) = \Theta_{i-1}(\mathbf{Q}) \tag{2}$$

for any $i > r$ (this will be proved in the end of Subsection 10.15). In particular, we do not have the equality $\mathrm{Fitt}_{i,\mathbf{Z}_p}(\mathrm{Sel}(\mathbf{Q}, E[p^\infty])^\vee) = \Theta_i(\mathbf{Q})$ in general if $(\mathrm{Sel}(\mathbf{Q}, E[p^\infty])^\vee)_{\mathrm{tors}} \neq 0$. This phenomenon is very different from that for the ideal class groups in [14] and [16] where the equality always holds. Even so, the above theorem tells us that the ideals $\Theta_i(\mathbf{Q})$ for all i determine the structure of $\mathrm{Sel}(\mathbf{Q}, E[p^\infty])$.

1.5. Although Theorem B is a statement on the Selmer group over $\mathbf{Q}$, in order to prove it, we have to study the Selmer group $\mathrm{Sel}(\mathbf{Q}_n, E[p^\infty])$ over $\mathbf{Q}_n$ which is an intermediate field of the cyclotomic $\mathbf{Z}_p$-extension $\mathbf{Q}_\infty/\mathbf{Q}$. Because of the self-duality of the motive, we can take a relation matrix of the dual $\mathrm{Sel}(\mathbf{Q}_n, E[p^\infty])^\vee$ of the Selmer group to be skew-Hermitian. Such a matrix is called an organizing matrix in Mazur and Rubin [20]. In our theory this skew-Hermitian matrix appears very naturally from the localization sequence of Selmer groups and a certain homomorphism Φ_S which is essentially defined from the reciprocity map (see Subsection 10.1, especially the exact sequences (41) and (43)). In this case, we do not need the elements $x_{m,\ell}$. Instead of $x_{m,\ell}$, the Kolyvagin systems $\kappa_{m,\ell}$ play an essential role. In the usual Euler system argument, when we bound the size of a Selmer group, we use a step-by-step argument which studies the difference between the orders of κ_m and $\kappa_{m'}$ such that m divides m' and m'/m is a prime. For our Euler system in the elliptic curve case, the difference between $\mathrm{ord}_p(\delta_m)$ and $\mathrm{ord}_p(\delta_{m'})$ carries no meaning when m divides m' and m'/m is a prime (because we have (2)). We give a new argument which relates $\mathrm{ord}_p(\delta_m)$ with $\mathrm{ord}_p(\delta_{m'})$ where m divides m' and m'/m is a *product of two primes* (see the proof of Theorem 10.12).

1.6. We remark on the numerical computation of the ideals Θ_i. Currently, we do not have an algorithm to determine Θ_i; in other words, we need infinite time to compute them, or we do not know when the computation stops. We know Θ_i is generated by the elements of the form $\tilde{\delta}_m$, so we have to study the upper bound of m, but we have not yet studied it. We propose in our paper [17] a slightly different method which is suitable for numerical computations, by which we get information on the structure of the Selmer group from a finite number of computations of $\tilde{\delta}_m$.

We can get similar results for nonordinary Galois representations, for example, in the case that V is the Tate module of an elliptic curve which has good supersingular reduction at p. We will study this case in our forthcoming paper.

Finally, the author would like to propose a problem on the Euler system in this paper. He thinks it is an important and interesting problem to construct g_ℓ in this paper directly without using the main conjecture in Iwasawa theory for the Tate module $T_p(f)$ of a modular form.

I would like to thank heartily Kazuya Kato for his constant interest in the results of this paper. I also thank John Coates heartily for his warm encouragement and useful advice. A part of this paper was written when I was staying in Emmanuel College in Cambridge and the Department of Pure Mathematics and Mathematical Statistics of the University of Cambridge in 2012. I would like to express my hearty thanks to them for their giving me stimulating environment and for their wonderful hospitality. Finally, I would like to thank the referee of this paper for his/her careful reading and valuable advice.

It is our great pleasure to dedicate this paper to Peter Schneider who proved a beautiful formula on the order of the Tate Shafarevich group of an abelian variety using the p-adic L-function in [30] (this formula on the Tate Shafarevich group and the argument on the p-adic height pairing in [30] are essentially used in the proof of our Theorem B), and who worked on Iwasawa theory for general motives (for example, [31]).

2. Preliminaries

2.1. **Assumptions.** Throughout this paper, p denotes an odd prime number. Our theory can be applied in a more general setting, but for simplicity, in this paper we work over abelian fields over $\mathbf{Q}$. (For example, we worked on the class groups of CM-fields over a totally real base field in our previous paper [16].)

We consider a motive $\mathcal{M}$ over $\mathbf{Q}$ with $\mathcal{F}$-coefficient where $\mathcal{F}$ is a finite extension over $\mathbf{Q}$. We consider the associated p-adic representation V which is a finite dimensional $\mathcal{F}_\wp$-vector space on which $G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts $\mathcal{F}_\wp$-linearly and continuously. Here, $\mathcal{F}_\wp$ is the $\wp$-adic completion of $\mathcal{F}$ for a prime $\wp$ above p. We assume that $\wp$ is unramified in $\mathcal{F}/\mathbf{Q}$. We denote by O the ring of integers of $\mathcal{F}_\wp$. We assume V is critical and ordinary at p (we mainly consider the good ordinary case). We take an O-lattice T of V, which is invariant under the action of $G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, and put $A = V/T$.

We denote by P (resp. P_{bad}) the set of finite primes (prime numbers) of $\mathbf{Q}$ (resp. the set of bad primes for V), and put $\mathcal{P} = P \setminus (P_{\mathrm{bad}} \cup \{p\})$. We also define

$$\mathcal{K} = \{K \mid K/\mathbf{Q} \text{ is a finite abelian } p\text{-extension in which } P_{\mathrm{bad}} \cup \{p\} \text{ is unramified}\}.$$

For $K \in \mathcal{K}$, we denote by K_∞/K the cyclotomic $\mathbf{Z}_p$-extension. We work under the following assumptions.

(I) $H^0(\mathbf{Q}, A) = 0$.

(II) Selmer groups: Put $\Lambda_{K_\infty} = O[[\mathrm{Gal}(K_\infty/\mathbf{Q})]]$ for $K \in \mathcal{K}$. We also use the notation $\Lambda = \Lambda_{\mathbf{Q}_\infty}$. We regard Λ as a subring of Λ_{K_∞} by the identification $\Lambda = \Lambda_{\mathbf{Q}_\infty} \simeq O[[\mathrm{Gal}(K_\infty/K)]] \subset \Lambda_{K_\infty} \simeq \Lambda[\mathrm{Gal}(K/\mathbf{Q})]$ for $K \in \mathcal{K}$. For a character $\psi : \mathrm{Gal}(K/\mathbf{Q}) \longrightarrow \overline{\mathbf{Q}}^\times$ with $K \in \mathcal{K}$, we put $O_\psi = O[\mathrm{Image}(\psi)]$ and $\Lambda_\psi = O_\psi[[\mathrm{Gal}(K_\infty/K)]]$. Since $\mathrm{Gal}(K_\infty/\mathbf{Q}) =$

$\mathrm{Gal}(K/\mathbf{Q}) \times \mathrm{Gal}(K_\infty/K)$, ψ is naturally extended to a ring homomorphism $\Lambda_{K_\infty} \longrightarrow \Lambda_\psi$, which we also denote by ψ.

Since we assumed that p is an ordinary prime for V, we can define Greenberg's Selmer group $\mathrm{Sel}(K_\infty, A)$ which is a subgroup of $H^1(K_\infty, A)$, defined by the local conditions, see [6] and Subsection 2.2 below. The Selmer group $\mathrm{Sel}(K_\infty, A)$ and its Pontrjagin dual $\mathrm{Sel}(K_\infty, A)^\vee$ are Λ_{K_∞}-modules.

We assume for any $K \in \mathcal{K}$ that

(II-1) $\mathrm{Sel}(K_\infty, A)^\vee$ is a finitely generated torsion Λ-module,

(II-2) $\mathrm{Sel}(K_\infty, A)^\vee$ has no nontrivial finite Λ-submodule, and also that

(II-3) the μ-invariant of $\mathrm{Sel}(K_\infty, A)^\vee$ as a Λ-module is zero.

(III) Existence of the p-adic L-function and the validity of the main conjecture in the sense of Greenberg [6]. There is an element $\theta_{K_\infty} \in \Lambda_{K_\infty}$ which is the p-adic L-function related to the L-values of V and which satisfies the following properties (see [2]). (The p-adic L-function θ_{K_∞} depends on the choice of the lattice T. Also, for simplicity we assume θ_{K_∞} is in the integral group ring. This would occur at least when V satisfies (I) and (I)* which we will state below (see the end of Section 1 in Greenberg [6])).

We put $P_\ell(x) = \det(1 - \mathrm{Frob}_\ell^{-1}\, x_{|V})$ where Frob_ℓ is the (arithmetic) Frobenius of ℓ. Suppose that K, L are in $\mathcal{K}$ and $K \subset L$. We denote by $c_{L_\infty/K_\infty} : \Lambda_{L_\infty} \longrightarrow \Lambda_{K_\infty}$ the natural ring homomorphism induced by the restriction map of the Galois groups. We have

$$c_{L_\infty/K_\infty}(\theta_{L_\infty}) = \Bigg(\prod_{\ell \in \mathcal{R}(L/K)} P_\ell(\mathrm{Frob}_{\ell,K_\infty}^{-1}) \Bigg) \theta_{K_\infty} \tag{3}$$

where $\mathcal{R}(L/K)$ is the subset of $\mathcal{P}$ consisting of primes which are ramified in L and unramified in K, and $\mathrm{Frob}_{\ell,K_\infty}$ is the Frobenius of ℓ in $\mathrm{Gal}(K_\infty/\mathbf{Q})$.

Suppose that $K \in \mathcal{K}$ and $\psi : \mathrm{Gal}(K/\mathbf{Q}) \longrightarrow \overline{\mathbf{Q}}^\times$ is a Dirichlet character. We define the ψ-quotient $(\mathrm{Sel}(K_\infty, A)^\vee)_\psi$ by $(\mathrm{Sel}(K_\infty, A)^\vee) \otimes_{\Lambda_{K_\infty}} \Lambda_\psi$. We assume the main conjecture for (V, ψ). Namely, for any such character ψ, the equality

$$\mathrm{char}_{\Lambda_\psi}((\mathrm{Sel}(K_\infty, A)^\vee)_\psi) = (\psi(\theta_{K_\infty})) \tag{MC}$$

holds as ideals in Λ_ψ. Note that we are assuming that (T, θ_{K_∞}) is chosen suitably such that this equality holds.

We will use another normalization of the p-adic L-functions later (see Subsection 3.1).

We also consider the Kummer dual $V^* = \mathrm{Hom}(V, \mathbf{Q}_p(1))$, $T^* = \mathrm{Hom}(A, \mathbf{Q}_p/\mathbf{Z}_p(1))$, and $A^* = V^*/T^*$. Then V^* is also an ordinary representation. We assume V^* is critical and assume the same properties for V^*, namely

(I)* $H^0(\mathbf{Q}, A^*) = 0$.

(II-2)* $\mathrm{Sel}(K_\infty, A^*)^\vee$ has no nontrivial finite Λ-submodule for $K \in \mathcal{K}$.

The other Properties (II-1), (II-3), (III) for V^* are consequences of our assumptions (II-1), (II-3), (III) for V by Theorem 2 in Greenberg [6].

When χ is an odd Dirichlet character of order prime to p and $\chi \neq \omega$ (where ω is the Teichmüller character), these conditions are satisfied for $V = \mathbf{Q}_p(\chi)$. Let E be an elliptic curve over $\mathbf{Q}$ such that p is a good ordinary prime and the representation attached to the p-torsion points $E[p]$ is irreducible. Take $V = V_p(E)$ the Tate module. Then (I) is satisfied, (II-1) is a theorem of Kato [11], (II-2) is proved by Greenberg [7, Prop. 4.14 and 4.15], and (II-3) is conjectured by Greenberg. Concerning (III), the main conjecture (MC) for $\mathbf{Q}_\infty$ was proved by Skinner and Urban in [34] under mild assumptions. The main conjecture (MC) for general $K \in \mathcal{K}$ is a consequence of the following results; (i) the validity of the main conjecture for $\mathbf{Q}_\infty$, (ii) the divisibility statement (half of the main conjecture) due to Kato [11], and (iii) both the algebraic and the analytic Kida's formulae due to Hachimori and Matsuno [10], [18] under the assumption (II-3). The conditions (I)* and (II-2)* are equivalent to (I) and (II-2), respectively. For a general Galois representation V, we will prove a related property to (II-2) in Proposition 2.10.

2.2. **Local conditions.** For a local field k such that $[k : \mathbf{Q}_p] < \infty$, we use the notation $H^1_*(k, V)$, $H^1_*(k, T)$, $H^1_*(k, A)$ where $* = e,\ f,\ g$, which are defined in Bloch and Kato [1]. Especially, $H^1_*(k, A)$ is the image of $H^1_*(k, V)$ in $H^1(k, A)$.

Suppose that V is an ordinary representation as above. We have the canonical subspace F^+V of V, and F^+A is defined to be the image of F^+V. We denote by k_∞/k the cyclotomic $\mathbf{Z}_p$-extension, and $k_{\infty,nr}$ the maximal unramified extension of k_∞. In this paper, we define Greenberg's local condition $H^1_{\mathrm{Gr}}(k, A)$ by

$$H^1_{\mathrm{Gr}}(k, A) = \mathrm{Ker}(H^1(k, A) \longrightarrow H^1(k_{\infty,nr}, A/F^+A)).$$

We know that V is semi-stable and that

$$H^1_g(k, V) = \mathrm{Ker}(H^1(k, V) \longrightarrow H^1(k_{nr}, V/F^+V))$$

by Flach [5, Prop. 2.4] where k_{nr} is the maximal unramified extension of k. This shows that

$$H^1_g(k, A) \subset H^1_{\mathrm{Gr}}(k, A).$$

For the cyclotomic $\mathbf{Z}_p$-extension k_∞/k, we define $H^1_*(k_\infty, A) = \varinjlim H^1_*(k_n, A)$ where k_n is the n-th layer of k_∞/k and $* = e,\ f,\ g,\ \mathrm{Gr}$. The subgroup $H^1_{\mathrm{Gr}}(k_\infty, A)$ is the local condition studied in Greenberg [6]. We have

$$H^1_e(k_\infty, A) \subset H^1_f(k_\infty, A) \subset H^1_g(k_\infty, A) \subset H^1_{\mathrm{Gr}}(k_\infty, A).$$

In many examples, we have $H^1_f(k_\infty, A) = H^1_{\mathrm{Gr}}(k_\infty, A)$. For example,

Lemma 2.3. *Suppose that $V = \mathbf{Q}_p(r)$ with $r \in \mathbf{Z}$ or $V = V_p(E)$ which is the Tate module of an elliptic curve over k with good ordinary reduction. Then we have*

$$H^1_f(k_\infty, A) = H^1_{\mathrm{Gr}}(k_\infty, A).$$

Proof. In fact, this follows from Examples 3.9 and 3.11 in Bloch and Kato [1] and Greenberg [6, Sec. 1 and 2] unless $r = 1$. For $r = 1$, since k_∞/k_n is totally ramified for $n \gg 0$, we have $H^1_f(k_\infty, \mathbf{Q}_p/\mathbf{Z}_p(1)) = \varinjlim (O^\times_{k_n}) \otimes \mathbf{Q}_p/\mathbf{Z}_p = \varinjlim (k_n^\times) \otimes \mathbf{Q}_p/\mathbf{Z}_p = H^1_{\mathrm{Gr}}(k_\infty, \mathbf{Q}_p/\mathbf{Z}_p(1))$. □

But if $V = V_p(E)$ is the Tate module of an elliptic curve over k with split multiplicative reduction at p, then we know that the index of $H^1_f(k_\infty, A)$ in $H^1_{\mathrm{Gr}}(k_\infty, A)$ is infinite (see [6, Prop. 9]). We put $V^* = \mathrm{Hom}_{\mathbf{Q}_p}(V, \mathbf{Q}_p(1))$, $T^* = \mathrm{Hom}(A, \mathbf{Q}_p/\mathbf{Z}_p(1))$, and $A^* = \mathrm{Hom}_{\mathbf{Z}_p}(T, \mathbf{Q}_p/\mathbf{Z}_p(1))$. Then V^* is also an ordinary representation, and we can define a subspace $F^+(V^*)$, which is nothing but $\mathrm{Ker}(V^* \longrightarrow (F^+V)^*)$.

Lemma 2.4. *We assume that*

i) $H^0(k_\infty, V/F^+V) = H^0(k_\infty, V^*/F^+(V^*)) = 0$,

ii) $D_{\mathrm{cris}}(V)^{\varphi = p^{-1}} = 0$ *where* φ *is the Frobenius on* $D_{\mathrm{cris}}(V)$, *and*

iii) $H^0(k_{\infty,nr,(p)}, A/F^+A)$ *is divisible where* $k_{\infty,nr,(p)}/k_\infty$ *is the unramified* $\mathbf{Z}_p$*-extension.*

Then we have $H^1_f(k_\infty, A) = H^1_{\mathrm{Gr}}(k_\infty, A)$.

Remark 2.5. The following p-adic representation V satisfies the above conditions i), ii). Let X be a proper smooth variety over k with potentially good reduction. We consider an etale cohomology group $V = H^i_{\mathrm{et}}(X_{\overline{k}}, \mathbf{Q}_p(r))$ with some $r \in \mathbf{Z}$ and some *odd* $i > 0$. Then V satisfies the above conditions i), ii) by Coates, Sujatha and Wintenberger [3, Cor. 1.6] (see also Kubo and Taguchi [13]; note that both $D_{st}(V/F^+V)$ and $D_{st}(V^*/F^+(V^*))$ have odd weights).

Assume that V is ordinary, then there is a decreasing filtration $\{F^iV\}$. Suppose that j is the minimal integer $\in \mathbf{Z}_{\geq 0}$ such that $F^{-j}V = V$. If $p > j+1$ and $k/\mathbf{Q}_p$ is a p-extension, we know that $H^0(k_{\infty,nr}, A/F^+A)$ is divisible by the argument of the proof of Proposition 10 in Greenberg [6]. This implies iii) because the (profinite) degree of $\mathrm{Gal}(k_{\infty,nr}/k_{\infty,nr,(p)})$ is prime to p. Therefore, for $V = H^i_{\mathrm{et}}(X_{\overline{k}}, \mathbf{Q}_p(r))$ with some odd i, if V is ordinary, p is big enough and $k/\mathbf{Q}_p$ is a p-extension, then we always have $H^1_f(k_\infty, A) = H^1_{\mathrm{Gr}}(k_\infty, A)$.

Proof. For a cofinitely generated $\mathbf{Z}_p$-module M, we denote by M_{div} the maximal divisible subgroup of M. First of all, we have

$$\varinjlim H^1(k_n, F^+A)_{\mathrm{div}} = H^1(k_\infty, F^+A).$$

In fact, we have an injection $H^1(k_n, F^+A)/H^1(k_n, F^+A)_{\mathrm{div}} \longrightarrow H^2(k_n, F^+T) = H^0(k_n, (F^+A)^*)^\vee$, but the latter is finite and bounded by our assumption that $H^0(k_\infty, (F^+V)^*) = H^0(k_\infty, V^*/F^+(V^*)) = 0$. This shows that $\varinjlim H^1(k_n, F^+A)_{\mathrm{div}}$ is of finite index in $H^1(k_\infty, F^+A)$. But the latter is p-divisible because the p-cohomological dimension of k_∞ is 1. Therefore, we have $\varinjlim H^1(k_n, F^+A)_{\mathrm{div}} = H^1(k_\infty, F^+A)$.

We know that $H^1_g(k_n, V) = \mathrm{Ker}(H^1(k_n, V) \longrightarrow H^1(k_{n,nr}, V/F^+V))$ by Flach. Moreover, by Bloch and Kato [1, Cor. 3.8.4], our assumption ii) implies

that $H^1_f(k_n, V) = H^1_g(k_n, V)$. Since our assumption i) implies $H^0(k_n, V/F^+V) = 0$, we know that $H^1(k_{n,nr}/k_n, (V/F^+V)^{I_n}) = 0$ where $k_{n,nr}$ is the maximal unramified extension of k_n and I_n is the absolute Galois group of $k_{n,nr}$. Therefore, $H^1(k_n, V/F^+V) \longrightarrow H^1(k_{n,nr}, V/F^+V)$ is injective, and $H^1_f(k_n, V)$ coincides with the image of $H^1(k_n, F^+V)$ in $H^1(k_n, V)$. This shows that $H^1_f(k_n, A)$ coincides with the image of $H^1(k_n, F^+A)_{\mathrm{div}}$. Thus we know that $H^1_f(k_\infty, A)$ coincides with the image of $\varinjlim H^1(k_n, F^+A)_{\mathrm{div}} = H^1(k_\infty, F^+A)$.

Our assumption $H^0(k_\infty, V/F^+V) = 0$ implies that

$$H^1(k_{\infty,nr,(p)}/k_\infty, (A/F^+A)^{I_{\infty,(p)}})$$

is finite where $I_{\infty,(p)}$ is the absolute Galois group of $k_{\infty,nr,(p)}$. On the other hand, since $(A/F^+A)^{I_{\infty,(p)}}$ is divisible by iii), $H^1(k_{\infty,nr,(p)}/k_\infty, (A/F^+A)^{I_{\infty,(p)}})$ is also divisible, therefore it is zero. This shows that $H^1(k_\infty, A/F^+A) \longrightarrow H^1(k_{\infty,nr}, (A/F^+A))$ is injective. Therefore, the image of $H^1(k_\infty, F^+A)$ in $H^1(k_\infty, A)$ coincides with $H^1_{\mathrm{Gr}}(k_\infty, A)$. Thus we obtain $H^1_f(k_\infty, A) = H^1_{\mathrm{Gr}}(k_\infty, A)$. This completes the proof of Lemma 2.4. □

Next, suppose that $\ell \neq p$ and k is a local field with $[k : \mathbf{Q}_\ell] < \infty$. As in Bloch and Kato [1], $H^1_f(k, V)$ is defined to be $\mathrm{Ker}(H^1(k, V) \longrightarrow H^1(k_{nr}, V))$ where k_{nr} is the maximal unramified extension of k, and $H^1_f(k, A)$ is the image of $H^1_f(k, V)$ in $H^1(k, A)$. Let k_∞/k be the cyclotomic $\mathbf{Z}_p$-extension. We note that $k_\infty \subset k_{nr}$ and $k_{\infty,nr} = k_{nr}$. We define $H^1_{\mathrm{Gr}}(k, A)$ by

$$H^1_{\mathrm{Gr}}(k, A) = \mathrm{Ker}(H^1(k, A) \longrightarrow H^1(k_{nr}, A)).$$

Since $\mathrm{Gal}(k_{nr}/k_\infty)$ is profinite of order prime to p, we have $H^1_{\mathrm{Gr}}(k, A) = \mathrm{Ker}(H^1(k, A) \longrightarrow H^1(k_\infty, A))$. If $\ell \notin P_{\mathrm{bad}} \cup \{p\}$, it is well-known [28, Lemma 1.3.5(iv)] that

$$H^1_f(k, A) = H^1_{\mathrm{Gr}}(k, A) = H^1_{\mathrm{et}}(\mathrm{Spec}\, O_k, A) \tag{4}$$

where the right hand side is the etale cohomology of the integer ring of k. For the cyclotomic $\mathbf{Z}_p$-extension k_∞/k, $H^1_*(k_\infty, A)$ is defined by $H^1_*(k_\infty, A) = \varinjlim H^1_*(k_n, A)$ for $* = f$, Gr. When $\ell \neq p$, since k_{nr}/k_∞ is of degree prime to p, we have

$$H^1_f(k_\infty, A) = H^1_{\mathrm{Gr}}(k_\infty, A) = 0. \tag{5}$$

2.6. **Selmer groups over cyclotomic $\mathbf{Z}_p$-extensions.** Let K be a number field, and K_∞/K the cyclotomic $\mathbf{Z}_p$-extension. For $* = f$, Gr, we define

$$H^1_*(O_{K_\infty}, A) = \mathrm{Ker}(H^1(K_\infty, A) \longrightarrow \prod_v H^1(K_{\infty,v}, A)/H^1_*(K_{\infty,v}, A))$$

where v runs over all finite primes of K_∞ (since we are assuming p is odd, we need only finite primes). We also denote $H^1_{\mathrm{Gr}}(O_{K_\infty}, A)$ by $\mathrm{Sel}(K_\infty, A)$.

Let S be a set of prime numbers in $\mathbf{Q}$. For any algebraic extension $F/\mathbf{Q}$ and a finite prime v of F, we use the convention $v \in S$ which means that the prime of $\mathbf{Q}$ below v is in S. We also use the notation $v \notin S$ similarly. (When we

clarify the meaning, we denote by S_F the set of primes of F which are above S.) Let K_∞ be as above. We define

$$H^1_*(O_{K_\infty}[1/S], A) = \mathrm{Ker}(H^1(K_\infty, A) \longrightarrow \prod_{v \notin S} H^1(K_{\infty,v}, A)/H^1_*(K_{\infty,v}, A))$$

for $* = f$, Gr, namely no condition is imposed for the primes above S. In particular, $\mathrm{Sel}(K_\infty, A)$ corresponds to $H^1_{\mathrm{Gr}}(O_{K_\infty}[1/S], A)$ with empty S. By the definitions of $H^1_{\mathrm{Gr}}(O_{K_\infty}[1/S], A)$, $H^1_f(O_{K_\infty}[1/S], A)$ and what we mentioned in Subsection 2.2 we have

$$H^1_f(O_{K_\infty}[1/S], A) \subset H^1_{\mathrm{Gr}}(O_{K_\infty}[1/S], A).$$

For a number field K with $[K : \mathbf{Q}] < \infty$, we also use the notation

$$H^1_*(O_K[1/S], A) = \mathrm{Ker}(H^1(K, A) \longrightarrow \prod_{v \notin S} H^1(K_v, A)/H^1_*(K_v, A))$$

where $* = f$, Gr. We denote by $O_K[1/S]$ the ring of S-integers in K. If S is a finite set which contains $P_{\mathrm{bad}} \cup \{p\}$, we have

$$H^1_f(O_K[1/S], A) = H^1_{\mathrm{Gr}}(O_K[1/S], A) = H^1_{\mathrm{et}}(\mathrm{Spec}\, O_K[1/S], A) \tag{6}$$

by (4) where the right hand side is the etale cohomology group.

2.7. **mod p^N cohomologies.** In this subsection, we fix a positive integer $N > 0$. For a local field k (a finite extension of $\mathbf{Q}_\ell$ where ℓ is an arbitrary prime number), we defined $H^1_*(k, A)$ in Subsection 2.2, where $* = f$, Gr. We define $H^1_*(k, T/p^N)$ to be the inverse image of $H^1_*(k, A)$ under the natural map $H^1(k, T/p^N) \longrightarrow H^1(k, A)$. Note that H^1_{Gr} is an artificial local condition and does not give a good cohomology theory, while H^1_f gives a good cohomology theory. We know that $H^1_f(k, T/p^N)$ and $H^1_f(k, T^*/p^N)$ are orthogonal complements under the cup product pairing (see Rubin [28, Prop. 1.4.3]).

For the cyclotomic $\mathbf{Z}_p$-extension k_∞/k, we also define $H^1_*(k_\infty, T/p^N)$ to be the inverse image of $H^1_*(k_\infty, A)$ for $* = f$ and $* = Gr$.

If T is unramified as a G_k-module and the characteristic of the residue field of k is not p, $H^1(k_\infty, T/p^N) \longrightarrow H^1(k_\infty, A)$ is injective. Hence in this case we have

$$H^1_f(k, T/p^N) = H^1_{\mathrm{Gr}}(k, T/p^N) = \mathrm{Ker}(H^1(k, T/p^N) \longrightarrow H^1(k_{nr}, T/p^N))$$

(see [28, Lemma 1.3.8]).

For a number field K and a finite set S of primes of K, we define $H^1_*(O_K[1/S], T/p^N)$ to be the subgroup of $H^1(K, T/p^N)$ consisting of elements whose local images are in $H^1_*(K_v, T/p^N)$ for all finite primes v which are not in S where $* = f$, Gr. In the case S is empty, $H^1_*(O_K[1/S], T/p^N)$ is denoted by $H^1_*(O_K, T/p^N)$.

Let K_∞/K be the cyclotomic $\mathbf{Z}_p$-extension and K_n be the n-th layer. Put $\Lambda = O[[\mathrm{Gal}(K_\infty/K)]]$. We define $H^1_*(O_{K_\infty}[1/S], T/p^N)$ similarly.

Lemma 2.8. *Assume that $H^0(K,A)=0$, $H^1_{\mathrm{Gr}}(O_{K_\infty},A)^\vee(=\mathrm{Sel}(K_\infty,A)^\vee)$ is a finitely generated torsion Λ-module and the μ-invariant is zero. Then for any $N>0$ we have*

$$\varprojlim_n H^1_f(O_{K_n},T/p^N)=\varprojlim_n H^1_{\mathrm{Gr}}(O_{K_n},T/p^N)=0.$$

Proof. Since $H^1_f(O_{K_n},T/p^N)\subset H^1_{\mathrm{Gr}}(O_{K_n},T/p^N)$, it suffices to prove the above statement for $H^1_{\mathrm{Gr}}(O_{K_n},T/p^N)$. Since $H^0(K,A)=0$, the natural map $H^1_{\mathrm{Gr}}(O_{K_n},T/p^N)\longrightarrow H^1_{\mathrm{Gr}}(O_{K_\infty},T/p^N)$ is injective. We know that $H^1_{\mathrm{Gr}}(O_{K_\infty},T/p^N)$ is finite because we assumed that the μ-invariant of $H^1_{\mathrm{Gr}}(O_{K_\infty},A)^\vee$ is zero. Therefore, $H^1_{\mathrm{Gr}}(O_{K_n},T/p^N)=H^1_{\mathrm{Gr}}(O_{K_\infty},T/p^N)$ for sufficiently large n. This shows that the corestriction map $H^1_{\mathrm{Gr}}(O_{K_{n+N}},T/p^N)\longrightarrow H^1_{\mathrm{Gr}}(O_{K_n},T/p^N)$ is the multiplication by $p^N=0$ for $n\gg 0$, which implies that $\varprojlim_n H^1_{\mathrm{Gr}}(O_{K_n},T/p^N)=0$. □

2.9. **Finite torsion submodules.** Let K be a number field such that $K\in\mathcal{K}$. From this subsection, we assume (I), (II-1), (II-3), (I)*. By Greenberg [6, Thm. 2], $H^1_{\mathrm{Gr}}(O_{K_\infty},A^*)^\vee$ is also a finitely generated torsion $\Lambda=O[[\mathrm{Gal}(K_\infty/K)]]$-module and the μ-invariant is zero.

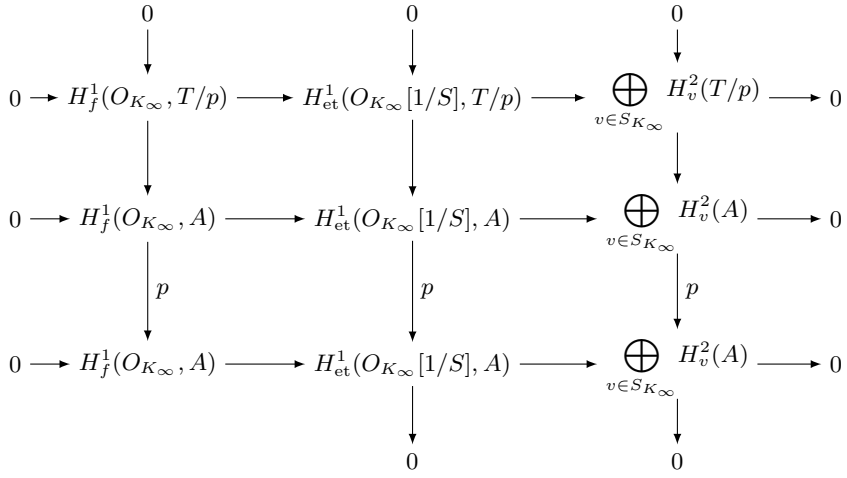
Proposition 2.10. *Under the above assumptions, $H^1_f(O_{K_\infty},A)^\vee$ has no non-trivial finite Λ-submodule.*

Proof. By the global duality theorem (Tate–Poitou duality), we have an exact sequence

$$\begin{aligned}\longrightarrow H^1_f(O_{K_n},T^*)\xrightarrow{p^N}H^1_f(O_{K_n},T^*)\longrightarrow H^1_f(O_{K_n},T^*/p^N)\\ \longrightarrow H^1_f(O_{K_n},A)^\vee\xrightarrow{p^N}H^1_f(O_{K_n},A)^\vee\longrightarrow\ .\end{aligned}$$

Since our assumptions imply that $H^1_{\mathrm{Gr}}(O_{K_\infty},A^*)$ is Λ-cotorsion, Lemma 2.8 implies that $\varprojlim_n H^1_f(O_{K_n},T^*/p^N)=0$. Taking the projective limit of the above exact sequence, we have an exact sequence $0\longrightarrow H^1_f(O_{K_\infty},A)^\vee\xrightarrow{p^N}H^1_f(O_{K_\infty},A)^\vee$. Since $H^1_f(O_{K_\infty},A)^\vee$ is Λ-torsion and the μ-invariant is zero, it is finitely generated over $\mathbf{Z}_p$. Therefore, the above exact sequence implies that $H^1_f(O_{K_\infty},A)^\vee$ is a free $\mathbf{Z}_p$-module of finite rank, which implies the conclusion.

This proposition can be also proved by the following method. We put $H^2_v(T/p)=H^1(K_{\infty,v},T/p)/H^1_f(K_{\infty,v},T/p)$ and we put $H^2_v(A)=H^1(K_{\infty,v},A)/H^1_f(K_{\infty,v},A)$ for any finite prime v of K_∞. We simply write $H^i_{\mathrm{et}}(O_{K_\infty}[1/S],M)$ for $H^i_{\mathrm{et}}(\mathrm{Spec}\,O_{K_\infty}[1/S],M)$. We have a diagram of exact sequences:



Here, the first horizontal row is exact by the global duality (see Mazur and Rubin [19, Thm. 2.3.4] and also Rubin [28, Thm. 1.7.3]) and $\varprojlim H^1_f(O_{K_n}, T^*/p) = 0$ which follows from Lemma 2.8. The second and the third horizontal rows are also exact by the global duality ([19, Thm. 2.3.4] and [28, Thm. 1.7.3]) and $\varprojlim_n H^1_f(O_{K_n}, T^*) = \varprojlim_{N}\varprojlim_n H^1_f(O_{K_n}, T^*/p^N) = 0$. The central vertical sequence is exact by $H^2_{\mathrm{et}}(O_{K_\infty}[1/S], T/p) = 0$ which follows from the vanishing of the μ-invariant. The right vertical sequence is exact because $\mathrm{cd}_p(K_{\infty,v}) = 1$ and $H^1_f(K_{\infty,v}, A)$ is divisible by definition. This diagram shows that $H^1_f(O_{K_\infty}, A)$ is divisible, which implies that $H^1_f(O_{K_\infty}, A)^\vee$ is a free $\mathbf{Z}_p$-module. □

2.11. **The action of Galois groups on Selmer groups.** Let $\mathcal{P}$ be the set of primes of $\mathbf{Q}$ defined in Subsection 2.1, and $\mathcal{K}$ be the set of number fields defined in Subsection 2.1. In this subsection, we still assume (I), (II-1), (II-2), (II-3), $(\mathrm{I})^*$.

Lemma 2.12 (Galois descent for H^1_{Gr})**.** *Let L/K be a finite extension such that L, $K \in \mathcal{K}$, and S be a finite subset of $\mathcal{P} = P \setminus (P_{\mathrm{bad}} \cup \{p\})$ such that S contains all ramifying primes in L/K. Then we have an isomorphism*

$$H^1_{\mathrm{Gr}}(O_{K_\infty}[1/S], A) \xrightarrow{\simeq} H^1_{\mathrm{Gr}}(O_{L_\infty}[1/S], A)^G$$

where $G = \mathrm{Gal}(L_\infty/K_\infty)$.

Proof. First of all, our assumption $H^0(\mathbf{Q}, A) = 0$ implies $H^0(L_\infty, A) = 0$. We put $S' = S \cup (P_{\mathrm{bad}} \cup \{p\})$, then the above implies that

$$H^1_{\mathrm{et}}(O_{K_\infty}[1/S'], A) \xrightarrow{\simeq} H^1_{\mathrm{et}}(O_{L_\infty}[1/S'], A)^G$$

is an isomorphism. If v is a bad prime of K_∞ or a prime above p, v is unramified in L_∞/K_∞ by our assumption. Therefore, if w is a prime of L_∞ above v, we have $L_{\infty,w,nr} = K_{\infty,v,nr}$. The conclusion now follows from the definition of $H^1_{\mathrm{Gr}}(O_{K_\infty}[1/S], A)$. □

Lemma 2.13 (Surjectivity lemma)**.** *Suppose that S is a finite set of prime numbers. Then the sequence*

$$0 \longrightarrow H^1_{\mathrm{Gr}}(O_{K_\infty}, A) \longrightarrow H^1_{\mathrm{Gr}}(O_{K_\infty}[1/S], A) \longrightarrow \bigoplus_{v \in S_{K_\infty}} H^1(K_{\infty,v}, A)/H^1_{\mathrm{Gr}}(K_{\infty,v}, A) \longrightarrow 0$$

is exact.

Proof. We have only to show that the first arrow in the second row is surjective. Since $H^1_f(O_{K_\infty}[1/S], A) \subset H^1_{\mathrm{Gr}}(O_{K_\infty}[1/S], A)$ and $H^1_f(K_{\infty,v}, A) \subset H^1_{\mathrm{Gr}}(K_{\infty,v}, A)$, it is enough to show

$$H^1_f(O_{K_\infty}[1/S], A) \longrightarrow \bigoplus_{v \in S} H^1(K_{\infty,v}, A)/H^1_f(K_{\infty,v}, A)$$

is surjective. Since our assumption implies that $H^1_{\mathrm{Gr}}(O_{K_\infty}, A^*)$ is Λ-cotorsion, we obtain the surjectivity of the above homomorphism from the global duality ([19, Thm. 2.3.4]) and $\varprojlim H^1_f(O_{K_n}, T^*) = 0$ which follows from Lemma 2.8 (cp. also the proof of Lemma 4.6 in Greenberg [7]). □

We note that we can deduce $\varprojlim H^1_f(O_{K_n}, T^*) = 0$ only from (II-1) for V^* without using Lemma 2.8.

Corollary 2.14. *We assume that S is a finite subset of $\mathcal{P}$. Then the sequence*

$$0 \longrightarrow H^1_{\mathrm{Gr}}(O_{K_\infty}, A) \longrightarrow H^1_{\mathrm{Gr}}(O_{K_\infty}[1/S], A) \longrightarrow \bigoplus_{v \in S_{K_\infty}} A(-1)^{\Gamma_{v,nr}} \longrightarrow 0$$

is exact where $\Gamma_{v,nr} = \mathrm{Gal}(K_{\infty,v,nr}/K_{\infty,v})$.

Proof. Since $v \in S_{K_\infty}$ is prime to p, we know by (5) that $H^1_{\mathrm{Gr}}(K_{\infty,v}, A) = 0$. Since $\Gamma_{v,nr}$ is profinite of order prime to p, we have $H^1(K_{\infty,v}, A) = H^1(K_{\infty,v,nr}, A)^{\Gamma_{v,nr}}$. The absolute Galois group $G_{K_{\infty,v,nr}}$ of $K_{\infty,v,nr}$ acts on A trivially because v is a good reduction prime. Therefore, we get

$$\begin{aligned} H^1(K_{\infty,v}, A)/H^1_{\mathrm{Gr}}(K_{\infty,v}, A) &= H^1(K_{\infty,v}, A) = H^1(K_{\infty,v,nr}, A)^{\Gamma_{v,nr}} \\ &= A(-1)^{\Gamma_{v,nr}}. \end{aligned}$$

Now, Corollary 2.14 follows from the surjectivity lemma (Lemma 2.13). □

Corollary 2.15. *Suppose $S \subset \mathcal{P}$. Then $H^1_{\mathrm{Gr}}(O_{K_\infty}[1/S], A)^\vee$ contains no nontrivial finite Λ-submodule, and the μ-invariant of $H^1_{\mathrm{Gr}}(O_{K_\infty}[1/S], A)^\vee$ is zero.*

Proof. In fact, in Corollary 2.14 $A(-1)^{\Gamma_{v,nr}}$ is p-divisible because $\Gamma_{v,nr}$ has profinite order prime to p. Hence this corollary follows at once from Corollary 2.14 and our assumption that $H^1_{\mathrm{Gr}}(O_{K_\infty}, A)^\vee$ contains no nontrivial finite Λ-submodule and the μ-invariant is zero. □

We go back to the setting of Lemma 2.12.

Lemma 2.16 (Vanishing lemma for H^1_{Gr})**.** *Let L/K be a finite extension such that L, $K \in \mathcal{K}$, and S be a finite subset of $\mathcal{P}$ such that S contains all ramifying primes in L/K. Then, putting $G = \mathrm{Gal}(L_\infty/K_\infty)$, we have*

$$H^1(G, H^1_{\mathrm{Gr}}(O_{L_\infty}[1/S], A)) = 0.$$

Proof. For a prime v of L_∞, we denote by $L_{\infty,v,nr}$ the maximal unramified extension of $L_{\infty,v}$, and put $\Gamma_{v,nr} = \mathrm{Gal}(L_{\infty,v,nr}/L_{\infty,v})$. Suppose at first that v is not lying over p. As we have seen in (5), $H^1_{\mathrm{Gr}}(L_{\infty,v}, A) = 0$. Suppose next that v is a prime of L_∞ lying over p. Since the cohomological dimension of $\Gamma_{v,nr}$ is 1, $H^1(L_{\infty,v}, A) \longrightarrow H^1(L_{\infty,v,nr}, A)^{\Gamma_{v,nr}}$ is surjective. We also have the surjectivity of $H^1(L_{\infty,v,nr}, A) \longrightarrow H^1(L_{\infty,v,nr}, A/F^+A)$ from $\mathrm{cd}_p(G_{L_{\infty,v,nr}}) = 1$, and the surjectivity of $H^1(L_{\infty,v,nr}, A)^{\Gamma_{v,nr}} \longrightarrow H^1(L_{\infty,v,nr}, A/F^+A)^{\Gamma_{v,nr}}$ from $H^1(\Gamma_{v,nr}, H^1(L_{\infty,v,nr}, F^+A)) = 0$ which follows from $H^2(L_{\infty,v}, F^+A) = 0$. Therefore, $H^1(L_{\infty,v}, A) \longrightarrow H^1(L_{\infty,v,nr}, A/F^+A)^{\Gamma_{v,nr}}$ is surjective, and

$$H^1(L_{\infty,v}, A)/H^1_{\mathrm{Gr}}(L_{\infty,v}, A) \xrightarrow{\simeq} H^1(L_{\infty,v,nr}, A/F^+A)^{\Gamma_{v,nr}}$$

is an isomorphism.

Put $S' = P_{\mathrm{bad}} \cup \{p\}$ and $S'' = S \cup S'$. Since all primes above S' are unramified in L/K, the above isomorphism implies the isomorphism

$$\bigoplus_{v \in S'_{K_\infty}} H^1(K_{\infty,v}, A)/H^1_{\mathrm{Gr}}(K_{\infty,v}, A) \xrightarrow{\simeq} \left(\bigoplus_{w \in S'_{L_\infty}} H^1(L_{\infty,w}, A)/H^1_{\mathrm{Gr}}(L_{\infty,w}, A) \right)^G. \tag{7}$$

We consider an exact sequence which is obtained from the surjectivity lemma (Lemma 2.13);

$$0 \longrightarrow H^1_{\mathrm{Gr}}(O_{L_\infty}[1/S], A) \longrightarrow H^1_{\mathrm{et}}(O_{L_\infty}[1/S''], A) \longrightarrow \bigoplus_{w \in S'} H^1(L_{\infty,w}, A)/H^1_{\mathrm{Gr}}(L_{\infty,w}, A)) \longrightarrow 0 \tag{8}$$

(note that $H^1_{\mathrm{Gr}}(O_{L_\infty}[1/S''], A) = H^1_{\mathrm{et}}(O_{L_\infty}[1/S''], A)$). The isomorphism (7) together with the surjectivity lemma (Lemma 2.13) for K_∞ implies that

$$H^1_{\mathrm{et}}(O_{L_\infty}[1/S''], A)^G \longrightarrow \left(\bigoplus_{w \in S'} H^1(L_{\infty,w}, A)/H^1_{\mathrm{Gr}}(L_{\infty,w}, A) \right)^G \tag{9}$$

is surjective. On the other hand, since we assumed $H^1_{\mathrm{Gr}}(O_{K_\infty}, A)^\vee$ is Λ-torsion, we know by Greenberg [6, Prop. 3,4] (cp. also [6, p.121]) that $H^2_{\mathrm{et}}(O_{K_\infty}[1/S''], A) = 0$. Using our assumption $H^0(L_\infty, A) = 0$ and the Serre–Hochschild spectral sequence, we have $H^1(G, H^1_{\mathrm{et}}(O_{L_\infty}[1/S''], A)) = 0$. Taking the cohomology of the exact sequence (8), we get

$$H^1(G, H^1_{\mathrm{Gr}}(O_{L_\infty}[1/S], A)) = 0$$

from the surjectivity of (9) and $H^1(G, H^1_{\mathrm{et}}(O_{L_\infty}[1/S''], A)) = 0$. □

Proposition 2.17. *Let L/K be a finite extension of fields in $\mathcal{K}$. We assume that S is the subset of $\mathcal{P}$ consisting of primes that are ramified in L_∞/K_∞. Put $e_v = [L_{\infty,w} : K_{\infty,v}]$ for $v \in S_{K_\infty}$ where w is a prime of L_∞ above v. Then we have an exact sequence*

$$0 \longrightarrow H^1_{\mathrm{Gr}}(O_{K_\infty}, A) \longrightarrow H^1_{\mathrm{Gr}}(O_{L_\infty}, A)^G \longrightarrow \bigoplus_{v \in S_{K_\infty}} A(-1)^{\Gamma_{v,nr}}[e_v] \longrightarrow 0$$

and

$$H^1(G, H^1_{\mathrm{Gr}}(O_{L_\infty}, A)) = 0.$$

Proof. Corollary 2.14 implies that there is a commutative diagram of exact sequences

$$\begin{array}{ccccccc}
0 & \longrightarrow & H^1_{\mathrm{Gr}}(O_{K_\infty}, A) & \longrightarrow & H^1_{\mathrm{Gr}}(O_{K_\infty}[1/S], A) & \longrightarrow & \displaystyle\bigoplus_{v \in S_{K_\infty}} A(-1)^{\Gamma_{v,nr}} \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & H^1_{\mathrm{Gr}}(O_{L_\infty}, A)^G & \longrightarrow & H^1_{\mathrm{Gr}}(O_{L_\infty}[1/S], A)^G & \longrightarrow & \left(\displaystyle\bigoplus_{w \in S_{L_\infty}} A(-1)^{\Gamma_{w,nr}}\right)^G.
\end{array}$$

The second vertical arrow is bijective by the Galois descent lemma (Lemma 2.12). Concerning the third vertical arrow, we know that $\Gamma_{v,nr} = \Gamma_{w,nr}$, $A(-1)^{\Gamma_{v,nr}} = A(-1)^{\Gamma_{w,nr}}$ is divisible, and G trivially acts on it. Since $L_{\infty,w}/K_{\infty,v}$ is totally ramified and the corestriction map $H^1(L_{\infty,w}, A) \longrightarrow H^1(K_{\infty,v}, A)$ is bijective, the above map $A(-1)^{\Gamma_{v,nr}} \longrightarrow A(-1)^{\Gamma_{w,nr}}$ is the multiplication by e_v. Therefore, the third horizontal arrow in the lower exact sequence is surjective. We obtain the first claim of Proposition 2.17 by the snake lemma from this commutative diagram. The second claim is obtained by taking the cohomology of the above exact sequence for L_∞ and by using the vanishing lemma for H^1_{Gr} (Lemma 2.16). □

Proposition 2.18. *Suppose that K is in $\mathcal{K}$, and S is a finite subset of $\mathcal{P}$ such that S contains all ramifying primes in $K/\mathbf{Q}$. Put $G = \mathrm{Gal}(K_\infty/\mathbf{Q}_\infty) = \mathrm{Gal}(K/\mathbf{Q})$. Then both $H^1_{\mathrm{Gr}}(O_{K_\infty}[1/S], A)$ and $H^1_{\mathrm{Gr}}(O_{K_\infty}[1/S], A)^\vee$ are cohomologically trivial as G-modules.*

In the elliptic curve case, this was proved in Greenberg [8, Thm. 1].

Proof. By Corollary 2.15, $H^1_{\mathrm{Gr}}(O_{\mathbf{Q}_\infty}[1/S], A)$ is divisible. Therefore, the corestriction map $H^1_{\mathrm{Gr}}(O_{K_\infty}[1/S], A) \longrightarrow H^1_{\mathrm{Gr}}(O_{\mathbf{Q}_\infty}[1/S], A)$ is surjective. By the Galois descent lemma (Lemma 2.12), this implies that $\hat{H}^0(G, H^1_{\mathrm{Gr}}(O_{K_\infty}[1/S], A)) = 0$. Using this together with the vanishing lemma for H^1_{Gr} (Lemma 2.16), we know that $H^1_{\mathrm{Gr}}(O_{K_\infty}[1/S], A)$ is cohomologically trivial by Serre [32, Chap. IX Théorème 8].

For a discrete G-module M such that the Pontrjagin dual $M^\vee$ is a finitely generated $\mathbf{Z}_p$-module, if M is cohomologically trivial, we know that $M^\vee$ is also cohomologically trivial, using the same theorem in Serre [32], because

$\hat{H}^{-1}(G, M^\vee) = \hat{H}^0(G, M)^\vee = 0$ and $\hat{H}^0(G, M^\vee) = \hat{H}^{-1}(G, M)^\vee = 0$. Therefore, we also get the conclusion for $H^1_{\mathrm{Gr}}(O_{K_\infty}[1/S], A)^\vee$. □

Corollary 2.19. *Assume that $K \in \mathcal{K}$ and S is a finite subset of $\mathcal{P}$ which contains all ramifying primes in $K/\mathbf{Q}$. As a $\Lambda_{K_\infty} = O[[\mathrm{Gal}(K_\infty/\mathbf{Q})]]$-module, $H^1_{\mathrm{Gr}}(O_{K_\infty}[1/S], A)^\vee$ is of projective dimension at most 1.*

Proof. Since $H^1_{\mathrm{Gr}}(O_{K_\infty}[1/S], A)^\vee$ is a free O-module of finite rank under our assumptions, the projective dimension of $H^1_{\mathrm{Gr}}(O_{K_\infty}[1/S], A)^\vee$ as a $\Lambda = O[[\mathrm{Gal}(K_\infty/K)]]$-module is at most 1. Therefore, the cohomological triviality of $H^1_{\mathrm{Gr}}(O_{K_\infty}[1/S], A)^\vee$ as a G-module implies that the projective dimension of $H^1_{\mathrm{Gr}}(O_{K_\infty}[1/S], A)^\vee$ as a Λ_{K_∞}-module is at most 1 by Popescu [25, Prop. 2.3]. □

Corollary 2.19 implies that the initial Fitting ideal $\mathrm{Fitt}_{0,\Lambda_{K_\infty}}(H^1_{\mathrm{Gr}}(O_{K_\infty}[1/S], A)^\vee)$ is a *principal ideal*. We will describe a generator of this ideal in the next section.

3. Initial Fitting ideals

In Sections 3–7, we assume all the assumptions in Subsection 2.1.

3.1. **Modified p-adic L-functions.** First of all, we consider a slightly modified p-adic L-function. For an algebraic extension $F/\mathbf{Q}$, we denote by $\mathcal{R}(F/\mathbf{Q})$ the set of all finite primes of $\mathbf{Q}$ ramifying in $F/\mathbf{Q}$. For a finite set S of finite primes of $\mathbf{Q}$ and a Dirichlet character ψ, we denote by $L_S(V, \psi)$ the L-function obtained by removing the Euler factors of primes in S. Note that the p-adic L-function θ_{K_∞} interpolates the values $L_{\mathcal{R}(K_\infty/\mathbf{Q})}(V, \psi)$ for a Dirichlet character ψ of $\mathrm{Gal}(K_n/\mathbf{Q})$ for some n.

We will introduce a modified p-adic L-function $\xi_{K_\infty,S} \in \Lambda_{K_\infty}$. This $\xi_{K_\infty,S}$ is related to Ψ_S in Greither [9, Prop. 8] in the classical setting, namely in the case $V = \mathbf{Q}_p(\chi)$. We will first construct from $\{\theta_{K_\infty}\}$ a family $\{\xi_{K_\infty}\}$ with $\xi_{K_\infty} \in \Lambda_{K_\infty}$ for any $K \in \mathcal{K}$, satisfying the following properties.

(III-1)′ Let $V^* = V^\vee(1)$ be the Kummer dual of V. For $\ell \in \mathcal{P}$, we put $P'_\ell(x) = \det(1 - \mathrm{Frob}_\ell\, x|_{V^*})$. For any K, $L \in \mathcal{K}$ such that $K \subset L$, we consider the natural map $c_{L_\infty/K_\infty} : \Lambda_{L_\infty} \longrightarrow \Lambda_{K_\infty}$ as in (III) in Subsection 2.1. Then these elements satisfy

$$c_{L_\infty/K_\infty}(\xi_{L_\infty}) = \Bigg(\prod_{\ell \in \mathcal{R}(L/K)} P'_\ell(\mathrm{Frob}^{-1}_{\ell,K_\infty}) \Bigg) \xi_{K_\infty}.$$

(III-2)′ If ψ is a faithful character of $\mathrm{Gal}(K/\mathbf{Q})$ for some $K \in \mathcal{K}$, we have

$$\mathrm{char}_{\Lambda_\psi}((\mathrm{Sel}(K_\infty, A)^\vee)_\psi) = (\psi(\xi_{K_\infty}))$$

as ideals of Λ_ψ.

For any n which is prime to p and whose prime divisors are good primes, we denote by $\mathbf{Q}(n) \in \mathcal{K}$ the maximal p-subextension of $\mathbf{Q}$ in $\mathbf{Q}(\mu_n)$. Put $n_\ell = \mathrm{ord}_p(\ell - 1)$ and $d_n = \prod_{\ell|n} p^{n_\ell}$. We have $[\mathbf{Q}(n) : \mathbf{Q}] = d_n$.

We will first construct $\xi_{\mathbf{Q}(n)_\infty}$ from $\theta_{\mathbf{Q}(n)_\infty}$. We have

$$P_\ell(x) \equiv P'_\ell(x) \bmod \ell - 1.$$

Using this congruence, we obtain the existence of $\xi_{\mathbf{Q}(n)_\infty}$ from the following lemma.

Lemma 3.2. *Let $\mathcal{N}$ be the set of squarefree products of primes in $\mathcal{P}$. Suppose that $\{\lambda_n\}_{n\in\mathcal{N}}$ is a family such that $\lambda_n \in \Lambda_{\mathbf{Q}(n)_\infty}$. For $n \in \mathcal{N}$ and $\ell \in \mathcal{P}$, we are also given $m_{\ell,n}$, $m'_{\ell,n}$, $u_{\ell,n} \in \Lambda_{\mathbf{Q}(n)_\infty}$, which are compatible under the restriction maps, namely which satisfy $c_{\mathbf{Q}(n)_\infty/\mathbf{Q}(n')_\infty}(m_{\ell,n}) = m_{\ell,n'}$, $c_{\mathbf{Q}(n)_\infty/\mathbf{Q}(n')_\infty}(m'_{\ell,n}) = m'_{\ell,n'}$, $c_{\mathbf{Q}(n)_\infty/\mathbf{Q}(n')_\infty}(u_{\ell,n}) = u_{\ell,n'}$ for all n, n' with $n'|n$. We assume that $u_{\ell,n}$ is a unit for all $\ell \in \mathcal{P}$ and $n \in \mathcal{N}$, and that $c_{\mathbf{Q}(n\ell)_\infty/\mathbf{Q}(n)_\infty}(\lambda_{n\ell}) = m_{\ell,n}\lambda_n$ and $u_{\ell,n}m_{\ell,n} \equiv m'_{\ell,n} \bmod p^{n_\ell}$ for all $n \in \mathcal{N}$ and $\ell \in \mathcal{P}$ such that $n\ell \in \mathcal{N}$. Then there is a family $\{\mu_n\}_{n\in\mathcal{N}}$ with $\mu_n \in \Lambda_{\mathbf{Q}(n)_\infty}$ such that*

(i) $c_{\mathbf{Q}(n\ell)_\infty/\mathbf{Q}(n)_\infty}(\mu_{n\ell}) = m'_{\ell,n}\mu_n$ *for all $n \in \mathcal{N}$ and $\ell \in \mathcal{P}$ such that $n\ell \in \mathcal{N}$,*

(ii) for any $n \in \mathcal{N}$ and for any Dirichlet character ψ of conductor np^s with some $s \in \mathbf{Z}_{\geq 0}$, $(\psi(\lambda_n)) = (\psi(\mu_n))$ holds as ideals of Λ_ψ, and

(iii) μ_n is congruent to $u\lambda_n$ modulo I_n, where $u = \prod_{\ell|n} u_{\ell,n}$ and I_n is the ideal of $\Lambda_{\mathbf{Q}(n)_\infty}$ generated by all $\nu_{\mathbf{Q}(n)/\mathbf{Q}(d)}(\lambda_d)$ with $d|n$ and $d \neq n$ (for any divisor d of n, we denote by $\nu_{\mathbf{Q}(n)_\infty/\mathbf{Q}(d)_\infty}$ the norm (corestriction) map $\nu_{\mathbf{Q}(n)_\infty/\mathbf{Q}(d)_\infty} : \Lambda_{\mathbf{Q}(d)_\infty} \longrightarrow \Lambda_{\mathbf{Q}(n)_\infty}$ which is defined by $\sigma \mapsto \sum \tau$ where for $\sigma \in \mathrm{Gal}(\mathbf{Q}(d)_\infty/\mathbf{Q})$, τ runs over elements of $\mathrm{Gal}(\mathbf{Q}(n)_\infty/\mathbf{Q})$ such that the restriction of τ to $\mathbf{Q}(d)_\infty$ is σ.)

Proof. For any $\ell \in \mathcal{P}$, we define $\epsilon_{\ell,n} = (m'_{\ell,n} - u_{\ell,n}m_{\ell,n})/p^{n_\ell} \in \Lambda_{\mathbf{Q}(n)_\infty}$. Suppose that $n \in \mathcal{N}$ and d is a divisor of n. We put

$$\alpha_{d,n} = \Big(\prod_{\ell|\frac{n}{d}} \epsilon_{\ell,d}\Big)\Big(\prod_{\ell|d} u_{\ell,d}\Big)\lambda_d \in \Lambda_{\mathbf{Q}(d)_\infty}.$$

In particular, $\alpha_{n,n} = (\prod_{\ell|n} u_{\ell,n})\lambda_n$. We put

$$\mu_n = \sum_{d|n} \nu_{\mathbf{Q}(n)_\infty/\mathbf{Q}(d)_\infty}(\alpha_{d,n}).$$

We simply write $c_{m,n}$ for $c_{\mathbf{Q}(m)_\infty/\mathbf{Q}(n)_\infty}$ and $\nu_{m,n}$ for $\nu_{\mathbf{Q}(m)_\infty/\mathbf{Q}(n)_\infty}$. Then we have

$$\begin{aligned} c_{n\ell,n}(\mu_{n\ell}) &= c_{n\ell,n}\Big(\sum_{d|n} \nu_{n\ell,d}(\alpha_{d,n\ell}) + \sum_{d|n} \nu_{n\ell,d\ell}(\alpha_{d\ell,n\ell})\Big) \\ &= p^{n_\ell}\sum_{d|n} \nu_{n,d}(\epsilon_{\ell,d}\alpha_{d,n}) + \sum_{d|n} \nu_{n,d}(c_{d\ell,d}(\alpha_{d\ell,n\ell})) \\ &= \sum_{d|n} \nu_{n,d}((m'_{\ell,d} - u_{\ell,d}m_{\ell,d})\alpha_{d,n}) + \sum_{d|n} \nu_{n,d}(u_{\ell,d}m_{\ell,d}\alpha_{d,n}) \end{aligned}$$

$$= \sum_{d|n} \nu_{n,d}(m'_{\ell,d}\alpha_{d,n})$$
$$= m'_{\ell,n}\mu_n.$$

If ψ is of conductor np^s, we have $\psi(\mu_n) = \psi(\alpha_{n,n}) = \psi(u)\psi(\lambda_n)$ where $u = \prod_{\ell|n} u_{\ell,n}$. It is clear that μ_n is congruent to $u\lambda_n$ modulo I_n. This completes the proof of Lemma 3.2. □

For general $K \in \mathcal{K}$ whose conductor is n, we define $\xi_{K_\infty} = c_{\mathbf{Q}(n)_\infty/K_\infty}(\xi_{\mathbf{Q}(n)_\infty})$. Then these elements satisfy the conditions (III-1)′ and (III-2)′.

For a finite set $S \subset \mathcal{P}$, we define $\xi_{K_\infty,S}$ by

$$\xi_{K_\infty,S} = \xi_{K_\infty} \prod_{\ell \in S\setminus(S\cap\mathcal{R}(K/\mathbf{Q}))} P'_\ell(\mathrm{Frob}_{\ell,K_\infty}^{-1}) \in \Lambda_{K_\infty}.$$

Note that $\xi_{K_\infty} = \xi_{K_\infty,\mathcal{R}(K/\mathbf{Q})}$. When we consider K, $L \in \mathcal{K}$ such that $K \subset L$, we have

$$c_{L_\infty/K_\infty}(\xi_{L_\infty,S}) = \left(\prod_{\ell\in\mathcal{R}(L/K),\ell\notin S} P'_\ell(\mathrm{Frob}_{\ell,K_\infty}^{-1})\right)\xi_{K_\infty,S}.$$

3.3. **Initial Fitting ideals of certain cohomology groups.** In this subsection, we first prove

Theorem 3.4. *We assume all the assumptions in Subsection 2.1. Suppose that $K \in \mathcal{K}$ and S is a subset of primes which contains all ramifying primes in $K/\mathbf{Q}$. Then the projective dimension of $H^1_{\mathrm{Gr}}(O_{K_\infty}[1/S], A)^\vee$ as a Λ_{K_∞}-module is at most* 1*, and we have*

$$\mathrm{Fitt}_{0,\Lambda_{K_\infty}}(H^1_{\mathrm{Gr}}(O_{K_\infty}[1/S], A)^\vee) = (\xi_{K_\infty,S}).$$

Proof. We already proved the statement concerning projective dimension in Corollary 2.19. Let $\psi : \mathrm{Gal}(K/\mathbf{Q}) \longrightarrow \overline{\mathbf{Q}}_p^\times$ be a character of $\mathrm{Gal}(K/\mathbf{Q})$, and O_ψ, Λ_ψ be as in (III) in Subsection 2.1 (we consider any character ψ of $\mathrm{Gal}(K/\mathbf{Q})$ and do not assume that ψ is faithful). Since the projective dimension of $H^1_{\mathrm{Gr}}(O_{K_\infty}[1/S], A)^\vee$ is at most 1, $\mathrm{Fitt}_{0,\Lambda_{K_\infty}}(H^1_{\mathrm{Gr}}(O_{K_\infty}[1/S], A)^\vee)$ is principal. Therefore, by [14, Cor. 4.1], in order to prove Theorem 3.4, we have only to show

$$\mathrm{Fitt}_{0,\Lambda_\psi}(H^1_{\mathrm{Gr}}(O_{K_\infty}[1/S], A)^\vee \otimes_{O[\mathrm{Gal}(K/\mathbf{Q})]} O_\psi) = (\psi(\xi_{K_\infty,S}))$$

for all characters ψ of $\mathrm{Gal}(K/\mathbf{Q})$.

Let M be the field corresponding to the kernel of $\psi : G_{\mathbf{Q}} \longrightarrow \overline{\mathbf{Q}}^\times$. We know $M \in \mathcal{K}$. For any discrete $O[\mathrm{Gal}(K/\mathbf{Q})]$-module P, we know

$$P^\vee \otimes_{O[\mathrm{Gal}(K/\mathbf{Q})]} O_\psi = (P^{\mathrm{Gal}(K/M)})^\vee \otimes_{O[\mathrm{Gal}(M/\mathbf{Q})]} O_\psi.$$

Hence it follows from the Galois descent lemma (Lemma 2.12) that

$$H^1_{\mathrm{Gr}}(O_{K_\infty}[1/S], A)^\vee \otimes_{O[\mathrm{Gal}(K/\mathbf{Q})]} O_\psi = H^1_{\mathrm{Gr}}(O_{M_\infty}[1/S], A)^\vee \otimes_{O[\mathrm{Gal}(M/\mathbf{Q})]} O_\psi.$$

Suppose that M' is the subfield of M such that $[M : M'] = p$ (note that $M/\mathbf{Q}$ is a cyclic extension). We write $N_0 = N_{\mathrm{Gal}(M/M')} = \sum_{\sigma\in\mathrm{Gal}(M/M')} \sigma$. We

have $O_\psi = O[\mathrm{Gal}(M/\mathbf{Q})]/N_0$. For any $O[\mathrm{Gal}(M/\mathbf{Q})]$-module X, we define $X^\psi = \mathrm{Ker}(N_0 : X \longrightarrow X)$, and $X_\psi = X/N_0X = X \otimes_{O[\mathrm{Gal}(M/\mathbf{Q})]} O_\psi$. From the exact sequence in Corollary 2.14, we get an exact sequence

$$0 \longrightarrow H^1_{\mathrm{Gr}}(O_{M_\infty}, A)^\psi \longrightarrow H^1_{\mathrm{Gr}}(O_{M_\infty}[1/S], A)^\psi \longrightarrow \left(\bigoplus_{v \in S_{M_\infty}} A(-1)^{\Gamma_{v,nr}} \right)^\psi.$$

Since $\mathrm{Ext}^1_{O[\mathrm{Gal}(M/\mathbf{Q})]}(O_\psi, H^1_{\mathrm{Gr}}(O_{M_\infty}, A)) = H^2(\mathrm{Gal}(M/\mathbf{Q}), H^1_{\mathrm{Gr}}(O_{M_\infty}, A))$ is finite by Proposition 2.17, the cokernel of the last map in the above exact sequence is finite.

Let $\mathcal{R}(M/\mathbf{Q})$ be the set of prime numbers which are ramified in M, and $S' = S \setminus \mathcal{R}(M/\mathbf{Q})$. We have

$$\left(\left(\bigoplus_{v \in S_{M_\infty}} A(-1)^{\Gamma_{v,nr}} \right)^\psi \right)^\vee = \bigoplus_{\ell \in S'} (\Lambda_\psi/(\mathrm{Frob}_{\ell,M_\infty} - 1)) \otimes T^*_{\Gamma_{\ell,nr}} \oplus (\text{finite})$$

where for a prime v above ℓ we wrote $\Gamma_{\ell,nr}$ for $\Gamma_{v,nr}$, which is independent of the choice of v. Let $P'_\ell(x)$ be the polynomial defined in (III-1)$'$. For $\ell \in S'$, we have

$$\begin{aligned} \mathrm{char}_{\Lambda_\psi}((\Lambda_\psi/(\mathrm{Frob}_{\ell,M_\infty} - 1)) \otimes T^*_{\Gamma_{\ell,nr}}) &= (\det((x - \mathrm{Frob}_{\ell,M_\infty})_{|V^*})_{|x=\mathrm{Frob}_{\ell,M_\infty}}) \\ &= (P'_\ell(\mathrm{Frob}^{-1}_{\ell,M_\infty})) \end{aligned}$$

in Λ_ψ. Therefore, by the main conjecture (III-2)$'$ and the above exact sequence, we have

$$\begin{aligned} \mathrm{char}_{\Lambda_\psi}((H^1_{\mathrm{Gr}}(O_{M_\infty}[1/S], A)^\vee)_\psi) &= \left(\psi \left(\xi_{M_\infty} \prod_{\ell \in S'} P'_\ell\big(\mathrm{Frob}^{-1}_{\ell,M_\infty}\big) \right) \right) \\ &= \left(\psi \left(\xi_{K_\infty} \prod_{\ell \in S \setminus \mathcal{R}(K/\mathbf{Q})} P'_\ell\big(\mathrm{Frob}^{-1}_{\ell,K_\infty}\big) \right) \right) \\ &= (\psi(\xi_{K_\infty,S})) \end{aligned}$$

where we used (III-1)$'$ to get the second equality.

Next, we will prove that $(H^1_{\mathrm{Gr}}(O_{M_\infty}[1/S], A)^\vee)_\psi$ contains no nontrivial finite submodule. Since $H^1(\mathrm{Gal}(M/M'), H^1_{\mathrm{Gr}}(O_{M_\infty}[1/S], A)) = 0$ by the vanishing lemma for H^1_{Gr} (Lemma 2.16), $\sigma - 1 : H^1_{\mathrm{Gr}}(O_{M_\infty}[1/S], A) \longrightarrow H^1_{\mathrm{Gr}}(O_{M_\infty}[1/S], A)^\psi$ is surjective where σ is a generator of $\mathrm{Gal}(M/M')$. Therefore, taking the dual, we know that there is an injective homomorphism from $(H^1_{\mathrm{Gr}}(O_{M_\infty}[1/S], A)^\vee)_\psi$ to $H^1_{\mathrm{Gr}}(O_{M_\infty}[1/S], A)^\vee$ which contains no nontrivial finite submodule by Corollary 2.15. Hence we have shown that $(H^1_{\mathrm{Gr}}(O_{M_\infty}[1/S], A)^\vee)_\psi$ contains no nontrivial finite submodule.

This fact together with the equality of the characteristic ideal above implies that

$$\mathrm{Fitt}_{0,\Lambda_\psi}((H^1_{\mathrm{Gr}}(O_{M_\infty}[1/S], A)^\vee)_\psi) = (\psi(\xi_{K_\infty,S})).$$

This completes the proof of Theorem 3.4. □

Corollary 3.5.

$$\xi_{K_\infty} \in \mathrm{Fitt}_{0,\Lambda_{K_\infty}}(H^1_{\mathrm{Gr}}(O_{K_\infty}, A)^\vee) = \mathrm{Fitt}_{0,\Lambda_{K_\infty}}(\mathrm{Sel}(K_\infty, A)^\vee)$$

Proof. Take $S = \mathcal{R}(K/\mathbf{Q})$ to be the set of prime numbers ramifying in K. This corollary follows from the surjectivity of

$$H^1_{\mathrm{Gr}}(O_{K_\infty}[1/S], A)^\vee \longrightarrow H^1_{\mathrm{Gr}}(O_{K_\infty}, A)^\vee$$

and $\xi_{K_\infty} = \xi_{K_\infty,S}$. □

Remark 3.6. If we assume only one half of the Main Conjecture (MC) in Subsection 2.1, that is, the inclusion $\mathrm{char}_{\Lambda_\psi}((\mathrm{Sel}(K_\infty, A)^\vee)_\psi) \supset (\psi(\theta_{K_\infty}))$ for any ψ, then we obtain $\xi_{K_{\infty,S}} \in \mathrm{Fitt}_{0,\Lambda_{K_\infty}}(H^1_{\mathrm{Gr}}(O_{K_\infty}[1/S], A)^\vee)$ by the same method as the proof of Theorem 3.4 using [14, Lemma 4.1]. Therefore, this "half" of (MC) implies Corollary 3.5. Note that this half of (MC) is a theorem of Kato [11] when V is the p-adic representation attached to an elliptic modular form.

4. Higher Fitting ideals

By the same method as in [14], [15], [16], we obtain information on the higher Fitting ideals.

4.1. **Preliminaries.** Let R be a commutative ring which is flat over $\mathbf{Z}_p$. We first fix positive integers $N > 0$ and $s > 0$. In the formal power series ring $R[[T]]$ in one variable, we consider an ideal $(p^N, T^{s+1}) = p^N R[[T]] + T^{s+1} R[[T]]$ and take the smallest positive integer $n(N, s)$ such that

$$(1+T)^{p^{n(N,s)}} - 1 \in (p^N, T^{s+1}).$$

For example, $n(N, 1) = \cdots = n(N, p-1) = N$ and $n(N, p) = N + 1$.

We consider a finite abelian p-group G such that G can be written as $G \simeq \mathbf{Z}/p^{n_1}\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/p^{n_r}\mathbf{Z}$ for some $r \in \mathbf{Z}_{>0}$ and that $n_1, \ldots, n_r \geq n(N, s)$. We take generators $\sigma_1, \ldots, \sigma_r$ of G, and identify the group ring $R[G]$ with

$$R[[S_1, \ldots, S_r]]/((1+S_1)^{p^{n_1}} - 1, \ldots, (1+S_r)^{p^{n_r}} - 1)$$

by $\sigma_j \leftrightarrow 1 + S_j$ $(1 \leq j \leq r)$. Note that by the definition of $n(N, s)$ there is a surjective ring homomorphism

$$R[G] \longrightarrow R/p^N[[S_1, \ldots, S_r]]/(S_1^{s+1}, \ldots, S_r^{s+1}).$$

For an element $f \in R[G]$ and $i \in \mathbf{Z}_{\geq 0}$, we define the ideal $I_{i,s}(f)$ of R/p^N as follows. Using the above identification, we write $f = \sum_{i_1,\ldots,i_r \geq 0} a_{i_1 \ldots i_r} S_1^{i_1} \ldots S_r^{i_r} \bmod \mathcal{I}$ where $a_{i_1 \ldots i_r} \in R$ and $\mathcal{I} = ((1+S_1)^{p^{n_1}} - 1, \ldots, (1+S_r)^{p^{n_r}} - 1)$. For $i \in \mathbf{Z}_{\geq 0}$, we define $I_{i,s}(f)$ to be the ideal of R/p^N generated by

$$\{a_{i_1 \ldots i_r} \bmod p^N \mid 0 \leq i_1, \ldots, i_r \leq s \text{ and } i_1 + \cdots + i_r \leq i\}.$$

This ideal does not depend on the choice of the generators $\sigma_1, \ldots, \sigma_r$ (see [16, Sec. 8], [15, Sec. 3]).

Lemma 4.2. *Let R, G be as above. Suppose that M, M' are finitely generated $R[G]$-modules, G acts on M' trivially, and that there is a surjective homomorphism $M \longrightarrow M'$. For any $f \in \mathrm{Fitt}_{0,R[G]}(M)$ and for any $i \geq 0$, we have $I_{i,s}(f) \subset \mathrm{Fitt}_{i,R/p^N}(M'/p^N)$.*

Proof. This can be proved by the same method as [16, Thm. 9.11]. We have a surjective homomorphism $M_G \longrightarrow M'$, so it is enough to prove $I_{i,s}(f) \subset \mathrm{Fitt}_{i,R/p^N}(M_G)$. By the definition of $n(N,s)$, we have an isomorphism

$$R/p^N[G]/(S_1^{s+1},\dots,S_r^{s+1}) \simeq R/p^N[[S_1,\dots,S_r]]/(S_1^{s+1},\dots,S_r^{s+1}).$$

We put $R' = R/p^N[[S_1,\dots,S_r]]/(S_1^{s+1},\dots,S_r^{s+1})$. If M is generated by n elements, we know

$$\mathrm{Fitt}_{0,R[G]}(M_G) = \sum_{i=0}^{n} \mathrm{Fitt}_{i,R}(M_G)(S_1,\dots,S_r)^i,$$

so we have $\mathrm{Fitt}_{0,R'}(M_G \otimes_{R[G]} R') = \sum_{i=0}^{n} \mathrm{Fitt}_{i,R/p^N}(M_G)(S_1,\dots,S_r)^i$ in R'. Therefore, $f \in \mathrm{Fitt}_{0,R[G]}(M)$ implies $I_{i,s}(f) \subset \mathrm{Fitt}_{i,R/p^N}(M_G)$. □

We also use a slight modification. We define $n(N,s)'$ to be the smallest positive integer such that

$$\frac{1}{T}\Big((1+T)^{p^{n(N,s)'}} - 1\Big) \in (p^N, T^{s+1}).$$

For example, $n(N,1)' = \cdots = n(N,p-2)' = N$ and $n(N,p-1)' = N+1$. We consider a finite abelian p-group G such that G can be written as $G \simeq \mathbf{Z}/p^{n_1}\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/p^{n_r}\mathbf{Z}$ for some $r \in \mathbf{Z}_{>0}$ and that $n_1,\dots,n_r \geq n(N,s)'$. We define $I_{i,s}(f)$ as above. Since $n(N,s)' \geq n(N,s)$, we can apply Lemma 4.2 to this G. Note that $I_{i,s}(f)$ is determined by $f \bmod \Big(\frac{1}{S_1}\big((1+S_1)^{p^{n_1}}-1\big),\dots,\frac{1}{S_r}\big((1+S_r)^{p^{n_r}}-1\big)\Big)$ in this case.

4.3. **Higher Stickelberger ideals.** We will define ideals $\Theta_{i,s}$ and Θ_i. Suppose that N, $s \in \mathbf{Z}_{>0}$, and $i \in \mathbf{Z}_{\geq 0}$. Put $\Lambda = \Lambda_{\mathbf{Q}_\infty} = O[[\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})]]$. For a squarefree positive integer n whose prime divisors are all in $\mathcal{P}$, we let $\mathbf{Q}(n) \in \mathcal{K}$ be the subfield of $\mathbf{Q}(\mu_n)$ defined in Subsection 3.1, and put $\mathcal{G}_n = \mathrm{Gal}(\mathbf{Q}(n)/\mathbf{Q})$. We have $\mathcal{G}_n = \prod_{\ell|n} \mathcal{G}_\ell$. For $K = \mathbf{Q}(n)$, using the canonical decomposition $\mathrm{Gal}(K_\infty/\mathbf{Q}) = \mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q}) \times \mathrm{Gal}(K/\mathbf{Q})$, we identify Λ_{K_∞} with $\Lambda[\mathcal{G}_n]$. Suppose that $n = \ell_1 \cdots \ell_r$. Taking a generator of $\mathcal{G}_{\ell_j}$ for each ℓ_j, we identify $\Lambda[\mathcal{G}_n]$ with $\Lambda[S_1,\dots,S_r]/I$ where $I = \big((1+S_1)^{p^{n_1}}-1,\dots,(1+S_r)^{p^{n_r}}-1\big)$ with $n_j = \mathrm{ord}_p(\ell_j - 1)$.

We use the positive integer $n(N,s)'$ which was defined in the previous subsection. We define a set

$$\mathcal{K}_s = \{K \in \mathcal{K} \mid K = \mathbf{Q}(n) \text{ for some } n \text{ whose all prime divisors } \ell \text{ satisfy } n_\ell = \mathrm{ord}_p(\ell-1) \geq n(N,s)'\} \cup \{\mathbf{Q}\}.$$

Suppose that a family $g = (g_{K_\infty})_{K \in \mathcal{K}_s}$ with $g_{K_\infty} \in \Lambda_{K_\infty}$ is given (we will take $g_{K_\infty} = \theta_{K_\infty}$, ξ_{K_∞} later). We apply the argument in the previous subsection, and consider the ideal $I_{i,s}(g_{K_\infty}) \subset \Lambda/p^N$ for $g_{K_\infty} \in \Lambda_{K_\infty} = \Lambda[\mathrm{Gal}(K/\mathbf{Q})]$. As we mentioned in the previous subsection, the ideal $I_{i,s}(g_{K_\infty})$ does not depend on the choice of the generators of the Galois group $\mathrm{Gal}(K/\mathbf{Q})$. We define $\Theta_{i,s}^{(N)}(g)$ to be the ideal of Λ/p^N generated by

$$\bigcup_{K \in \mathcal{K}_s} I_{i,s}(g_{K_\infty}),$$

and $\Theta_i^{(N)}(g)$ to be the ideal generated by $\bigcup_{s>0} \Theta_{i,s}^{(N)}(g)$. We define $\Theta_{i,s}(g) = \varprojlim_N \Theta_{i,s}^{(N)}(g) \subset \Lambda$ and $\Theta_i(g) = \varprojlim_N \Theta_i^{(N)}(g) \subset \Lambda$.

We consider $\theta = (\theta_{K_\infty})$ and $\xi = (\xi_{K_\infty})$ in Subsection 3.1.

Lemma 4.4. *For $K \in \mathcal{K}_s$, we have $I_{i,s}(\theta_{K_\infty}) = I_{i,s}(\xi_{K_\infty})$.*

Proof. Suppose that $K = \mathbf{Q}(n)$ and $n = \ell_1 \cdots \ell_r$. Put $N_j = \sum_{\sigma \in \mathcal{G}_{\ell_j}} \sigma$ and define I to be the ideal of Λ_{K_∞} generated by all N_j with $1 \leq j \leq r$. By the construction of ξ_{K_∞} and Lemma 3.2 (iii), we have $\theta_{K_\infty} \equiv \xi_{K_\infty} \bmod I$.

Let σ_j be a generator of $\mathcal{G}_{\ell_j}$ and $S_j = \sigma_j - 1$. By the definition of $n(N,s)'$, $N_j = 0$ in $\Lambda_{K_\infty}/(p^N, S_j^{s+1})$. This implies that $I_{i,s}(\theta_{K_\infty}) = I_{i,s}(\xi_{K_\infty})$. □

This lemma implies that $\Theta_{i,s}^{(N)}(\theta) = \Theta_{i,s}^{(N)}(\xi)$, $\Theta_{i,s}(\theta) = \Theta_{i,s}(\xi)$, and $\Theta_i(\theta) = \Theta_i(\xi)$. (In this sense, $\Theta_i(\theta)$ does not depend on the normalization of the p-adic L-functions.) We simply write $\Theta_{i,s}^{(N)}$, $\Theta_i^{(N)}$, $\Theta_{i,s}$, Θ_i for $\Theta_{i,s}^{(N)}(\theta)$, $\Theta_i^{(N)}(\theta)$, $\Theta_{i,s}(\theta)$, $\Theta_i(\theta)$.

We obtain the following corollary from Theorem 3.4 (from Corollary 3.5).

Corollary 4.5. *For any $K \in \mathcal{K}_s$ and any $i \geq 0$, we have*

$$I_{i,s}(\xi_{K_\infty}) \subset \mathrm{Fitt}_{i,\Lambda/p^N}(\mathrm{Sel}(\mathbf{Q}_\infty, A)^\vee \otimes \mathbf{Z}/p^N).$$

Hence we obtain $\Theta_{i,s}^{(N)} \subset \mathrm{Fitt}_{i,\Lambda/p^N}(\mathrm{Sel}(\mathbf{Q}_\infty, A)^\vee \otimes \mathbf{Z}/p^N)$ and

$$\Theta_{i,s} \subset \Theta_i \subset \mathrm{Fitt}_{i,\Lambda}(\mathrm{Sel}(\mathbf{Q}_\infty, A)^\vee).$$

Proof. First of all, since we assumed $H^0(\mathbf{Q}, A) = 0$, we also have $H^0(\mathbf{Q}_\infty, A) = 0$, and $\mathrm{Sel}(\mathbf{Q}_\infty, A) \longrightarrow \mathrm{Sel}(K_\infty, A)$ is injective. Applying Lemma 4.2 and Corollary 3.5 to our case, we obtain the first assertion. This implies $\Theta_{i,s}^{(N)}(\xi) \subset \mathrm{Fitt}_{i,\Lambda/p^N}(\mathrm{Sel}(\mathbf{Q}_\infty, A)^\vee \otimes \mathbf{Z}/p^N)$. Hence, taking the limit, we obtain the final assertion. □

5. Selmer groups and Galois groups

5.1. **More assumptions.** From this section on, we further assume

(IV-1) Both $H^0(\mathbf{Q}_{\ell,\infty}, A)$ and $H^0(\mathbf{Q}_{\ell,\infty}, A^*)$ are divisible for $\ell \in P_{\mathrm{bad}}$,

(IV-2) $H^0(\mathbf{Q}_p, A/F^+A) = H^0(\mathbf{Q}_p, A^*/F^+(A^*)) = 0$,

(IV-3) $D_{\mathrm{cris}}(V)^{\varphi=1} = D_{\mathrm{cris}}(V)^{\varphi=p^{-1}} = 0$.

For an odd Dirichlet character χ of order prime to p such that $\chi \neq \omega$, these conditions are satisfied for $V = \mathbf{Q}_p(\chi)$ if $\chi(p) \neq 1$. When $V = V_p(E)$ is the Tate module of an elliptic curve over $\mathbf{Q}$ with good ordinary reduction at p, (IV-1) is equivalent to $p \nmid \mathrm{Tam}(E)$, (IV-2) is equivalent to $E(\mathbf{F}_p)[p] = 0$ (see Greenberg [7, Sec. 2 and 3]), and (IV-3) is satisfied.

Recall that we defined $\mathcal{K}$ in Subsection 2.1 by

$$\mathcal{K} = \{K \mid K/\mathbf{Q} \text{ is a finite abelian } p\text{-extension in which } P_{\mathrm{bad}} \cup \{p\} \text{ is unramified}\}.$$

We also define a set $\mathcal{K}_{(p)}$ which contains $\mathcal{K}$ by

$$\begin{aligned}\mathcal{K}_{(p)} &= \{K \mid K/\mathbf{Q} \text{ is a finite abelian } p\text{-extension in which } P_{\mathrm{bad}} \text{ is unramified}\} \\ &= \{K \mid K \subset F_n \text{ for some } F \in \mathcal{K} \text{ and some } n \in \mathbf{Z}_{\geq 0}\}\end{aligned} \tag{10}$$

where F_n is the n-th layer of the cyclotomic $\mathbf{Z}_p$-extension F_∞/F.

Lemma 5.2. *Suppose that K is in $\mathcal{K}_{(p)}$. Under the assumptions (IV-1), (IV-2), (IV-3), we have*

(1) $H^1_f(K_v, A) = H^1_{\mathrm{Gr}}(K_v, A)$ and $H^1_f(K_v, A^*) = H^1_{\mathrm{Gr}}(K_v, A^*)$ for any finite prime v of K,

(2) $H^1_f(O_K[1/S], A) = H^1_{\mathrm{Gr}}(O_K[1/S], A)$ and $H^1_f(O_K[1/S], A^*) = H^1_{\mathrm{Gr}}(O_K[1/S], A^*)$ for any finite set S of finite primes of $\mathbf{Q}$,

(3) $H^1_f(O_K[1/S], T/p^N) = H^1_{\mathrm{Gr}}(O_K[1/S], T/p^N)$ and $H^1_f(O_K[1/S], T^*/p^N) = H^1_{\mathrm{Gr}}(O_K[1/S], T^*/p^N)$ for any positive integer $N > 0$ and any finite set S of finite primes of $\mathbf{Q}$.

Proof. It is enough to prove (1). We prove $H^1_f(K_v, A) = H^1_{\mathrm{Gr}}(K_v, A)$. Put $k = K_v$. Suppose at first that v is a prime above p. Since $k/\mathbf{Q}_p$ is an abelian p-extension, we have $H^2(k, F^+T) = H^0(k, A^*/F^+(A^*)) = 0$ by (IV-2), which implies $H^1(k, F^+A)_{\mathrm{div}} = H^1(k, F^+A)$. We know $H^1_g(k, V) = \mathrm{Ker}(H^1(k, V) \longrightarrow H^1(k_{nr}, V/F^+V))$ by Flach. Since $H^1(k, V/F^+V) \longrightarrow H^1(k_{nr}, V/F^+V)$ is injective by (IV-2) and $D_{\mathrm{cris}}(V)^{\varphi=p^{-1}} = 0$ in (IV-3) implies $H^1_f(k, V) = H^1_g(k, V)$, we have $H^1_f(k, V) = H^1_g(k, V) = H^1(k, F^+V)$. Therefore, $H^1_f(k, A) = H^1(k, F^+A)_{\mathrm{div}} = H^1(k, F^+A)$. Let $k_{\infty,nr,p}/k_\infty$ be the unramified $\mathbf{Z}_p$-extension. Since $H^0(k_{\infty,nr,p}, A/F^+A) = 0$ by (IV-2), the natural map $H^1(k, A/F^+A) \longrightarrow H^1(k_{\infty,nr,p}, A/F^+A)$ is injective. Therefore, we get $H^1_{\mathrm{Gr}}(k, A) = H^1(k, F^+A) = H^1_f(k, A)$.

Next, we suppose that v is a prime such that $v \in P_{\mathrm{bad}}$. Since $K/\mathbf{Q}$ is unramified at v, we have $k_\infty = \mathbf{Q}_{\ell,\infty}$ and $H^0(k_\infty, A)$ is divisible by (IV-1). Thus, $H^1_{\mathrm{Gr}}(k, A) = H^1(k_\infty/k, H^0(k_\infty, A))$ is also divisible. Therefore, we get $H^1_f(k, A) = H^1_{\mathrm{Gr}}(k, A)_{\mathrm{div}} = H^1_{\mathrm{Gr}}(k, A)$ by Rubin [28, Lemma 1.3.5(i)].

If v is a good prime, we always have $H^1_f(k, A) = H^1_{\mathrm{Gr}}(k, A)$. Therefore, we get $H^1_f(K_v, A) = H^1_{\mathrm{Gr}}(K_v, A)$ for any v. We can prove $H^1_f(K_v, A^*) = H^1_{\mathrm{Gr}}(K_v, A^*)$ by the same method. □

5.3. **mod p^N Selmer groups.** From now on, we use H^1_f instead of H^1_{Gr} under the assumptions of the previous subsection. Note that $H^1_f(k, T/p^N)$ and $H^1_f(k, T^*/p^N)$ are orthogonal complements of each other for a local field k.

For a number field K and a finite set S of primes, we define $H^1_f(O_K, T/p^N)_{S,0}$ to be the kernel of $H^1_f(O_K, T/p^N) \longrightarrow \bigoplus_{v\in S} H^1(K_v, T/p^N)$. By the global duality theorem (see Mazur and Rubin [19, Thm. 2.3.4]), we obtain the following.

Proposition 5.4. *Suppose that S, S' are finite sets of primes of K such that $S' \subset S$. Then we have an exact sequence*

$$\begin{aligned} 0 &\longrightarrow H^1_f(O_K, T^*/p^N)_{S',0} \longrightarrow H^1_f(O_K[1/S], T^*/p^N) \\ &\longrightarrow \bigoplus_{v\in S'} H^1(K_v, T^*/p^N) \oplus \bigoplus_{v\in S\setminus S'} H^1(K_v, T^*/p^N)/H^1_f(K_v, T^*/p^N) \\ &\longrightarrow H^1_f(O_K[1/S'], T/p^N)^\vee \longrightarrow (H^1_f(O_K, T/p^N)_{S,0})^\vee \longrightarrow 0. \end{aligned}$$

Corollary 5.5. *Suppose further that $S \setminus S'$ consists of good primes. Then we have an exact sequence*

$$\begin{aligned} 0 &\longrightarrow H^1_f(O_K, T^*/p^N)_{S',0} \longrightarrow H^1_f(O_K[1/S], T^*/p^N) \\ &\longrightarrow \bigoplus_{v\in S'} H^1(K_v, T^*/p^N) \oplus \bigoplus_{v\in S\setminus S'} H^0(\kappa(v), T^*/p^N(-1)) \\ &\longrightarrow H^1_f(O_K[1/S'], T/p^N)^\vee \longrightarrow (H^1_f(O_K, T/p^N)_{S,0})^\vee \longrightarrow 0 \end{aligned}$$

where $\kappa(v)$ is the residue field of v.

Proof. In fact, we know

$$\begin{aligned} H^1(K_v, T^*/p^N)/H^1_f(K_v, T^*/p^N) &= H^0(K_{v,nr}/K_v, T^*/p^N(-1)) \\ &= H^0(\kappa(v), T^*/p^N(-1)) \end{aligned}$$

for $v \in S \setminus S'$. □

Taking $S' = \varnothing$, we have

Corollary 5.6. *Suppose that S is a finite set of good primes. We have an exact sequence*

$$\begin{aligned} 0 &\longrightarrow H^1_f(O_K, T^*/p^N) \longrightarrow H^1_f(O_K[1/S], T^*/p^N) \\ &\xrightarrow{\partial} \bigoplus_{v\in S} H^0(\kappa(v), T^*/p^N(-1)) \xrightarrow{r_S} H^1_f(O_K, T/p^N)^\vee \\ &\longrightarrow (H^1_f(O_K, T/p^N)_{S,0})^\vee \longrightarrow 0. \end{aligned}$$

Remark 5.7. The above exact sequence can be regarded as a modification of the localization sequence in etale cohomology (we can regard $H^1_f(O_K, T/p^N)^\vee$ as $H^2_f(O_K, T^*/p^N)$).

5.8. **The homomorphism r_S.** We put $d = \dim_{\mathcal{F}_\wp} V$. Let $\mathbf{Q}(T)$ be the field corresponding to the kernel of $\rho : G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{Aut}(T) \simeq \mathrm{GL}_d(O)$. Suppose that $\mathbf{Q}_\infty/\mathbf{Q}$ is the cyclotomic $\mathbf{Z}_p$-extension. For simplicity, we assume the following conditions.

(V-1) The image of $\rho_{|G_{\mathbf{Q}_\infty}} : G_{\mathbf{Q}_\infty} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}_\infty) \longrightarrow \mathrm{Aut}(T) \simeq \mathrm{GL}_d(O)$ contains $\mathrm{SL}_d(O)$.

(V-2) There is an $a \in O$ such that $a \neq 1$, $a^r = 1$ for some integer $r > 1$ and $aI \in \mathrm{Image}(\rho : G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{Aut}(T) \simeq \mathrm{GL}_d(O))$ where I is the identity matrix.

Let $W = \{aI \in \mathrm{GL}_d(O) \mid a \in O \text{ and } a^r = 1 \text{ for some } r \in \mathbf{Z}_{>0}\}$ which we regard as a subgroup of $\mathrm{Aut}(T)$. We denote by Δ the subgroup of $\mathrm{Gal}(\mathbf{Q}(T)/\mathbf{Q})$ which is the inverse image of W under $\rho : \mathrm{Gal}(\mathbf{Q}(T)/\mathbf{Q}) \longrightarrow \mathrm{Aut}(T) = \mathrm{GL}_d(O)$. The condition (V-2) means that $\Delta \neq 1$. Since we are assuming that $O/\mathbf{Z}_p$ is unramified, the orders of both W and Δ are prime to p. We note that (V-2) implies $H^0(\mathbf{Q}_\infty, A) = 0$, namely (I). If $d \geq 2$, (V-1) implies (I) and $(\mathrm{I})^*$.

Put $\mathfrak{f} = [\mathcal{F}_\wp : \mathbf{Q}_p]$. If d is not prime to $p^{\mathfrak{f}} - 1$, (V-1) implies (V-2). In fact, if d' is the greatest common divisor of d and $p^{\mathfrak{f}} - 1$, we can take an element $a \in O$ whose order is d'. Since aI is in $\mathrm{SL}_d(O)$, aI is in the image of ρ by (V-1). For example, if $d = 2$, (V-1) implies (V-2) because we are assuming that p is odd.

In this section, we fix a basis $e_1, \ldots, e_d$ of T as an O-module and an isomorphism $\mathrm{Aut}(T) \simeq \mathrm{GL}_d(O)$ by using the basis. We also fix a positive integer $N > 0$. For any O/p^N-module M, we identify the Pontrjagin dual $M^\vee = \mathrm{Hom}(M, \mathbf{Q}/\mathbf{Z}) = \mathrm{Hom}(M, \mathbf{Z}/p^N)$ with $\mathrm{Hom}_O(M, O/p^N)$. Let t be the O-homomorphism defined by $t(e_i) = 0$ $(i = 1, \ldots, d-1)$ and $t(e_d) = 1$. We regard t as an element of the Pontrjagin dual $(T/p^N)^\vee = \mathrm{Hom}_O(T, O/p^N)$.

Put

$$\sigma = \begin{pmatrix} 1 & 1 & 0 & \ldots & & 0 \\ 0 & 1 & 1 & \ldots & & \\ . & & & . & & 0 \\ . & & & . & & 1 \\ 0 & & & \ldots & 0 & 1 \end{pmatrix} \in \mathrm{SL}_d(O/p^N) \subset \mathrm{Aut}(T/p^N), \tag{11}$$

which is a standard unipotent Jordan block. We denote by H the subgroup generated by σ (if $d = 1$, we put $\sigma = 1$ and $H = 1$). We put $\mathcal{T} = (T/p^N)_H$ which is the H-coinvariants of T/p^N. This $\mathcal{T}$ is an O-module and is isomorphic to O/p^N as an O-module. By definition, t can be regarded as an element in the Pontrjagin dual $\mathcal{T}^\vee$, and $\mathcal{T}^\vee$ is generated by t. We note that $\mathcal{T}^\vee$ is isomorphic to $H^0(H, (T/p^N)^\vee) = H^0(H, T^*/p^N(-1))$, so t can be regarded as a generator of $H^0(H, T^*/p^N(-1))$.

Suppose that ℓ is in $\mathcal{P} = P \setminus (P_{\mathrm{bad}} \cup \{p\})$. Since ℓ is a good prime, $G_{\mathbf{F}_\ell} = \mathrm{Gal}(\overline{\mathbf{F}}_\ell/\mathbf{F}_\ell)$ acts on T. We define

$$\mathcal{P}_0 = \{\ell \in \mathcal{P} \mid \ell \equiv 1 \pmod{p^N} \text{ and } H^0(\mathbf{F}_\ell, T^*/p^N(-1)) \text{ contains a free } O/p^N\text{-submodule of rank } 1\},$$

$$\mathcal{P}_1 = \{\ell \in \mathcal{P} \mid \ell \equiv 1 \pmod{p^N} \text{ and } H^0(\mathbf{F}_\ell, T^*/p^N(-1)) \simeq H^1(\mathbf{F}_\ell, T^*/p^N(-1)) \simeq O/p^N\},$$

and

$$\mathcal{P}_0' = \{\ell \in \mathcal{P} \mid \ell \equiv 1 \pmod{p^N} \text{ and } G_{\mathbf{F}_\ell} \text{ acts on } T/p^N \text{ trivially}\}.$$

Clearly, $\mathcal{P}_1 \subset \mathcal{P}_0$ and $\mathcal{P}_0' \subset \mathcal{P}_0$. By definition, we have

$$\mathcal{P}_0' \cap \mathcal{P}_1 = \varnothing \text{ if } d > 1.$$

For any prime $\ell \in \mathcal{P}_0$, we fix a prime $\ell_{\overline{\mathbf{Q}}}$ of an algebraic closure $\overline{\mathbf{Q}}$ above ℓ. For any algebraic number field F, we denote the prime of F below $\ell_{\overline{\mathbf{Q}}}$ by ℓ_F, so when we consider finite extensions F_1/k, F_2/k such that $F_1 \subset F_2$, the primes ℓ_{F_2}, ℓ_{F_1} satisfy $\ell_{F_2}|\ell_{F_1}$.

Let $\mathbf{Q}(T/p^N)$ be the field corresponding to the kernel of $\rho \bmod p^N$: $G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{Aut}(T/p^N) \simeq \mathrm{GL}_d(O/p^N)$. We put $L = \mathbf{Q}(T/p^N)$. By the definition of $\mathcal{P}_0'$, we have

$$\mathcal{P}_0' = \{\ell \in \mathcal{P} \mid \ell \equiv 1 \pmod{p^N} \text{ and } \rho(\mathrm{Frob}_{\ell_L, K_\infty}) \bmod p^N = 1\}.$$

We define

$$\mathcal{P}_{1,\sigma} = \{\ell \in \mathcal{P} \mid \ell \equiv 1 \pmod{p^N} \text{ and } \rho(\mathrm{Frob}_{\ell_L}) \bmod p^N = \sigma\}$$

where $\sigma \in \mathrm{GL}_d(O/p^N)$ was defined in (11). When $\rho(\mathrm{Frob}_\ell) \bmod p^N$ is a conjugate of σ in $\mathrm{GL}_d(O/p^N)$, we always take ℓ_L such that $\rho(\mathrm{Frob}_{\ell_L}) \bmod p^N = \sigma$.

Suppose that ℓ is in $\mathcal{P}_{1,\sigma}$. We denote by $e_1^\vee, \dots, e_d^\vee$ the dual basis of $T^*/p^N(-1) = (T/p^N)^\vee$, corresponding to the basis $e_1, \dots, e_d$ we took for T/p^N. By definition, $t = e_d^\vee$. The action of Frob_{ℓ_L} on $(T/p^N)^\vee = T^*/p^N(-1)$ with respect to the basis $e_1^\vee, \dots, e_d^\vee$ is given by

$$\begin{pmatrix} 1 & & & & \dots & 0 \\ 1 & 1 & & & & \vdots \\ & 1 & \ddots & & & \\ \vdots & & \ddots & 1 & & \\ 0 & \dots & & 1 & 1 \end{pmatrix}.$$

Therefore, $t = e_d^\vee$ is in $H^0(\mathbf{F}_\ell, T^*/p^N(-1))$ and we have $H^0(\mathbf{F}_\ell, T^*/p^N(-1)) \simeq (O/p^N)t$. We also get $H^1(\mathbf{F}_\ell, T^*/p^N(-1)) \simeq ((T/p^N)^\vee)/(\mathrm{Frob}_{\ell_L} - 1) \simeq (O/p^N)$. This shows that $\mathcal{P}_{1,\sigma} \subset \mathcal{P}_1$.

For any number field K of finite degree, we define $\mathcal{P}(K)$, $\mathcal{P}_0(K)$, and $\mathcal{P}_1(K)$ by

$$\mathcal{P}(K) = \{\ell \in \mathcal{P} \mid \ell \text{ splits completely in } K\},$$
$$\mathcal{P}_0(K) = \{\ell \in \mathcal{P}_0 \mid \ell \text{ splits completely in } K\},$$
$$\mathcal{P}_1(K) = \{\ell \in \mathcal{P}_1 \mid \ell \text{ splits completely in } K\}.$$

We define $\mathcal{P}_{1,\sigma}(K)$, $\mathcal{P}_0'(K)$ similarly. By the Chebotarev density theorem, $\mathcal{P}_0'(K)$ is infinite. We next consider $\mathcal{P}_{1,\sigma}(K)$.

Let $\mathcal{K}_{(p)}$ be the set of fields defined in (10).

Lemma 5.9. *Suppose that K is in $\mathcal{K}_{(p)}$. The image of $\rho_{|G_{K_\infty}} : G_{K_\infty} = \mathrm{Gal}(\overline{\mathbf{Q}}/K_\infty) \longrightarrow \mathrm{Aut}(T)$ coincides with the image of $\rho_{|G_{\mathbf{Q}_\infty}} : G_{\mathbf{Q}_\infty} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}_\infty) \longrightarrow \mathrm{Aut}(T)$. In particular, the image of $\rho_{|G_{K_\infty}}$ contains $\mathrm{SL}_d(O)$.*

Proof. Let $\mathbf{Q}(T)$ be the field corresponding to the kernel of $\rho : G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{Aut}(T) \simeq \mathrm{GL}_d(O)$. It is enough to prove

$$\mathbf{Q}(T)\mathbf{Q}_\infty \cap K_\infty = \mathbf{Q}_\infty$$

for $K \in \mathcal{K}_{(p)}$. Suppose that F is a subfield of $\mathbf{Q}(T)\mathbf{Q}_\infty \cap K_\infty$ such that $1 < [F : \mathbf{Q}] < \infty$. Since F is in $\mathcal{K}_{(p)}$ and $F \neq \mathbf{Q}$, some prime in $P \setminus P_{\mathrm{bad}}$ is ramified in F. Since F is also in $\mathbf{Q}(T)\mathbf{Q}_\infty$, F is unramified outside $P_{\mathrm{bad}} \cup \{p\}$. It follows that p has to be the only prime which is ramified in F. This shows that $F \subset \mathbf{Q}_\infty$ because $F/\mathbf{Q}$ is an abelian p-extension. Therefore, we obtain $\mathbf{Q}(T)\mathbf{Q}_\infty \cap K_\infty = \mathbf{Q}_\infty$. □

Using the basis $e_1, \ldots, e_d$, we consider $\rho_{|_{G_{K,p^N}}} = \rho_{|_{G_K}} \bmod p^N$: $G_K \longrightarrow \mathrm{Aut}(T/p^N) = \mathrm{GL}_d(O/p^N)$. Put $L = K\mathbf{Q}(T/p^N)$ which corresponds to the kernel of $\rho_{|_{G_{K,p^N}}}$. By Lemma 5.9 and the Chebotarev density theorem, we can take infinitely many $\ell \in \mathcal{P}(K)$ such that $\ell \equiv 1 \bmod p^N$ and

$$\rho_{|_{G_{K,p^N}}}(\mathrm{Frob}_{\ell_L}) = \sigma = \begin{pmatrix} 1 & & & \ldots & 0 \\ 1 & 1 & & & \vdots \\ & 1 & \ddots & & \\ \vdots & & \ddots & 1 & \\ 0 & \ldots & & 1 & 1 \end{pmatrix} \text{ in } \mathrm{Aut}(T/p^N).$$

Therefore, $\mathcal{P}_{1,\sigma}(K)$ is an infinite set. Since $\mathcal{P}_{1,\sigma}(K) \subset \mathcal{P}_1(K)$, we know that $\mathcal{P}_1(K)$ is also infinite.

For any number field K, we define $S_{\ell,K}$ to be the set of primes of K above ℓ, and put

$$\mathcal{H}^2_\ell(K) = \bigoplus_{v \in S_{\ell,K}} H^0(\kappa(v), T^*/p^N(-1)) \tag{12}$$

where $\kappa(v)$ is the residue field of $v \in S_{\ell,K}$. We define $t_{\ell,K}$ to be the element in $\mathcal{H}^2_\ell(K)$ whose ℓ_K-component is t and the other components are 0.

We obtain the following lemma easily.

Lemma 5.10. *If ℓ is in $\mathcal{P}_{1,\sigma}(K)$, $\mathcal{H}^2_\ell(K)$ is a free $O/p^n[\mathrm{Gal}(K/\mathbf{Q})]$-module of rank 1 generated by $t_{\ell,K}$.*

Suppose that S' is a finite set of primes of $\mathbf{Q}$. For any prime ℓ which is in $\mathcal{P}$ and which is not in S', we consider a natural homomorphism

$$H^1_f(O_K[1/S'], T/p^N) \longrightarrow \bigoplus_{v\in S_{\ell,K}} H^1_f(K_v, T/p^N).$$

Since the Pontrjagin dual of $H^1_f(K_v, T/p^N)$ is $H^1(K_v, T^*/p^N)/H^1_f(K_v, T^*/p^N)$ $= H^0(\kappa(v), T^*/p^N(-1))$ as we saw in the proof of Corollary 5.5, taking the dual of the above homomorphism, we have a homomorphism

$$r_\ell : \mathcal{H}^2_\ell(K) \longrightarrow H^1_f(O_K[1/S'], T/p^N)^\vee, \tag{13}$$

which we denote by r_ℓ. For any finite subset S of $\mathcal{P}$ such that $S \cap S' = \varnothing$, we define

$$r_S : \bigoplus_{\ell\in S} \mathcal{H}^2_\ell(K) \longrightarrow H^1_f(O_K[1/S'], T/p^N)^\vee \tag{14}$$

by the direct sum of all r_ℓ with $\ell \in S$. Note that the map r_S appears in the exact sequence in Corollary 5.6.

5.11. **The surjectivity of r_S.** In this subsection, we assume $K \in \mathcal{K}_{(p)}$ where $\mathcal{K}_{(p)}$ was defined in (10). We will study the homomorphism r_S defined in the previous subsection and will define $\eta^\vee$ which is a homomorphism from a certain Galois group to $H^1(O_K[1/S'], T/p^N)^\vee$ (see below). We consider $\rho_{|_{G_{K,p^N}}} : \mathrm{Gal}(\overline{\mathbf{Q}}/K) \longrightarrow \mathrm{Aut}(T/p^N) \simeq \mathrm{GL}_d(O/p^N)$, and define L to be the field corresponding to the kernel of $\rho_{|_{G_{K,p^N}}}$. The Galois group $\mathrm{Gal}(L/K)$ can be regarded as a subgroup of $\mathrm{GL}_d(O/p^N)$. Let W be the group defined after (V-2). We denote by W_N the image of W in $\mathrm{GL}_d(O/p^N)$ under the natural map $\mathrm{GL}_d(O) \longrightarrow \mathrm{GL}_d(O/p^N)$, and by Δ_N the inverse image of W_N under $\rho_{|_{G_{K,p^N}}}$. Then W_N is isomorphic to W and $\Delta_N \subset \mathrm{Gal}(L/K)$ is isomorphic to Δ which was defined after (V-2). We identify Δ_N with Δ, and regard Δ as a subgroup of $\mathrm{Gal}(L/K)$.

Lemma 5.12. $H^1(\mathrm{Gal}(L/K), T/p^N) = 0$.

Proof. We put $G = \mathrm{Gal}(L/K)$. By (V-2), there is $s \in \Delta$ such that $s \neq 1$. We write $\rho(s) = aI$ with $a \neq 1$. Then $a - 1$ is invertible, so $s - 1$ is invertible on T/p^N. Hence we have $(T/p^N)^\Delta = 0$. Since the order of Δ is prime to p, $H^1(\Delta, T/p^N) = 0$. Note that Δ is in the center of G, so a normal subgroup. From the exact sequence

$$0 \longrightarrow H^1(G/\Delta, (T/p^N)^\Delta) \longrightarrow H^1(G, T/p^N) \longrightarrow H^1(\Delta, T/p^N),$$

we obtain $H^1(G, T/p^N) = 0$. □

Lemma 5.13. *We take a basis $e_1, \dots, e_d$ and consider a quotient $\mathcal{T}$ of T/p^N as in Subsection 5.8. We denote the composition of the natural maps $H^1(K, T/p^N) \longrightarrow H^1(L, T/p^N)$ and $H^1(L, T/p^N) \longrightarrow H^1(L, \mathcal{T})$ by*

$$\eta : H^1(K, T/p^N) \longrightarrow H^1(L, \mathcal{T}).$$

Then η is injective.

Proof. We regard $e_1, \dots, e_d$ as a basis of T/p^N. Then $e_1, \dots, e_{d-1}$ are in the kernel of $T/p^N \longrightarrow \mathcal{T}$, and the image of e_d generates $\mathcal{T}$. Suppose that $x \in H^1(K, T/p^N)$ satisfies $\eta(x) = 0$. Let $\tilde{\eta} : H^1(K, T/p^N) \longrightarrow H^1(L, T/p^N)$ be the natural map. Identifying $H^1(L, T/p^N)$ with $H^1(L, O/p^N) \otimes_O T/p^N$, we can write $\tilde{\eta}(x) = \sum_{i=1}^{d} x_i e_i$ where $x_1, \dots, x_d$ are elements in $H^1(L, O/p^N)$. By our assumption, $x_d = 0$. For any i such that $1 \leq i \leq d-1$, there is an element $\tau \in \mathrm{SL}_d(O)$ such that $\tau e_i = e_i + e_d$, and $\tau e_j = e_j$ for all $j \neq i$. Since $\mathrm{Gal}(L/K)$ acts on $\tilde{\eta}(x)$ trivially and τ is in the image of ρ, $\tau\tilde{\eta}(x) = \tilde{\eta}(x)$. This together with $x_d = 0$ implies that $x_i = 0$. Therefore, $\tilde{\eta}(x) = 0$. Since $H^1(\mathrm{Gal}(L/K), T/p^N) = 0$ by Lemma 5.12, $\tilde{\eta}$ is injective, which implies $x = 0$. □

Suppose that S' is a finite set of primes of $\mathbf{Q}$ containing $P_{\mathrm{bad}} \cup \{p\}$. We write $H^1(O_K[1/S'], T/p^N)$ for $H^1_f(O_K[1/S'], T/p^N) = H^1_{\mathrm{et}}(O_K[1/S'], T/p^N)$.

Lemma 5.14. *Suppose that S' is a finite set of primes of $\mathbf{Q}$ containing $P_{\mathrm{bad}} \cup \{p\}$. For any element $x \in H^1(O_K[1/S'], T/p^N)^\vee$, there exist infinitely many $\ell \in \mathcal{P}'_0(K)$ such that $\ell \notin S'$ and $r_\ell(t_{\ell,K}) = x$ where*

$$r_\ell : \mathcal{H}^2_\ell(K) \longrightarrow H^1(O_K[1/S'], T/p^N)^\vee$$

is the homomorphism defined in (13).

Proof. Let $L^{ab}_{S'}$ be the maximal unramified abelian extension of L outside S'. Since

$$H^1(O_K[1/S'], T/p^N) \longrightarrow H^1(O_L[1/S'], \mathcal{T}) = H^1(O_L[1/S'], \mathbf{Z}/p^N) \otimes \mathcal{T}$$

is injective by Lemma 5.13, taking the dual, we have a surjective homomorphism

$$\eta^\vee : \mathrm{Gal}(L^{ab}_{S'}/L) \otimes \mathcal{T}^\vee \longrightarrow H^1(O_K[1/S'], T/p^N)^\vee.$$

Therefore, by the Chebotarev density theorem, we can take infinitely many $\ell \in \mathcal{P}'_0(L)$ such that $\ell \notin S'$ and $\eta^\vee(\mathrm{Frob}_{\ell_L} \otimes t) = x$.

Since $\ell \in \mathcal{P}'_0(K)$, we have

$$\mathcal{H}^2_\ell(K) = \bigoplus_{v \in S_{\ell,K}} T^*/p^N(-1) = \bigoplus_{v \in S_{\ell,K}} (T/p^N)^\vee.$$

Consider a diagram

$$\begin{array}{ccc} \mathcal{H}^2_\ell(K) & \xrightarrow{r_\ell} & H^1(O_K[1/S'], T/p^N)^\vee \\ \uparrow{\scriptstyle \eta'} & & \uparrow{\scriptstyle \eta^\vee} \\ \bigoplus_{v\in S_{\ell,L}} \mathcal{T}^\vee & \xrightarrow{r_{\ell,L}} & \mathrm{Gal}(L^{ab}_{S'}/L)\otimes \mathcal{T}^\vee \end{array}$$

where the left arrow η' is the natural map induced by the natural injective homomorphism $\mathcal{T}^\vee \longrightarrow (T/p^N)^\vee$, and the bottom arrow $r_{\ell,L}$ is characterized by $r_{\ell,L}(t_v) = \mathrm{Frob}_v \otimes t$ where t_v is the element whose v-component is t and the other components are zero. This diagram is commutative because $r_{\ell,L}$ is also obtained as the dual of $H^1(O_L[1/S'], \mathcal{T}) \longrightarrow \bigoplus_{v\in S_{\ell,L}} H^1_f(L_v, \mathcal{T})$.

Therefore, it follows from $(\eta^\vee \circ r_{\ell,L})(t_{\ell_L}) = \eta^\vee(\mathrm{Frob}_{\ell_L} \otimes t) = x$ and $\eta'(t_{\ell_L}) = t_{\ell,K}$ that $r_\ell(t_{\ell,K}) = x$. □

Next, we consider r_ℓ for $\ell \in \mathcal{P}_{1,\sigma}$. As in Subsection 5.8, we denote by H the subgroup of $\mathrm{Gal}(L/K)$ generated by σ. Let L' be the subfield of L corresponding to H, so L/L' is a cyclic extension of degree at least p^N.

Corollary 5.15. *The natural map $H^1(K, T/p^N) \longrightarrow H^1(L', \mathcal{T})$ is injective.*

Proof. This follows at once from Lemma 5.13. □

Suppose that S' is a finite set as above. By Corollary 5.15, the natural map

$$H^1(O_K[1/S'], T/p^N) \longrightarrow H^1(O_{L'}[1/S'], \mathcal{T}) = H^1(O_{L'}[1/S'], \mathbf{Z}/p^N) \otimes \mathcal{T}$$

is injective. Let M be the maximal unramified abelian extension of L' outside S' such that $p^N \,\mathrm{Gal}(M/L') = 0$. Recall that L/L' is a cyclic extension of degree at least p^N, so there is a unique intermediate field $L'_{(N)}$ such that $[L'_{(N)} : L'] = p^N$. We know $L'_{(N)} \subset M$. Since $\mathrm{Gal}(L'_{(N)}/L') \simeq \mathbf{Z}/p^N$ and $\mathrm{Gal}(M/L')$ is a $\mathbf{Z}/p^N$-module, M has a subfield M' such that $\mathrm{Gal}(M/L') = \mathrm{Gal}(M/L'_{(N)}) \times \mathrm{Gal}(M/M')$ and $\mathrm{Gal}(M/M') = \mathrm{Gal}(L'_{(N)}/L')$. The above injective homomorphism can be written as

$$H^1(O_K[1/S'], T/p^N) \longrightarrow H^1(\mathrm{Gal}(M/L'), \mathbf{Z}/p^N) \otimes \mathcal{T}.$$

Since $H^1(O_K[1/S'], T/p^N) \longrightarrow H^1(O_{L'_{(N)}}[1/S'], \mathbf{Z}/p^N) \otimes \mathcal{T}$ is also injective by Lemma 5.13 and the kernel of $H^1(O_{L'}[1/S'], \mathcal{T}) \longrightarrow H^1(O_{L'_{(N)}}[1/S'], \mathcal{T})$ is $H^1(\mathrm{Gal}(L'_{(N)}/L'), \mathcal{T})$, the composition

$$\begin{aligned} H^1(O_K[1/S'], T/p^N) &\longrightarrow H^1(\mathrm{Gal}(M/L'), \mathbf{Z}/p^N) \otimes \mathcal{T} \\ &\longrightarrow H^1(\mathrm{Gal}(M'/L'), \mathbf{Z}/p^N) \otimes \mathcal{T} \end{aligned}$$

is injective. Taking the dual, we obtain a surjective homomorphism

$$\eta^\vee : \mathrm{Gal}(M'/L') \otimes \mathcal{T}^\vee \longrightarrow H^1(O_K[1/S'], T/p^N)^\vee,$$

for which we also use the notation $\eta^\vee$.

Proposition 5.16. *Suppose that S' is a finite set of primes of $\mathbf{Q}$ containing $P_{\mathrm{bad}} \cup \{p\}$, and that K'/K is an extension such that $K' \in \mathcal{K}_{(p)}$. For any element $x \in H^1(O_K[1/S'], T/p^N)^\vee$, there exist infinitely many $\ell \in \mathcal{P}_{1,\sigma}(K')$ such that $\ell \notin S'$ and $r_\ell(t_{\ell,K}) = x$ where*

$$r_\ell : \mathcal{H}^2_\ell(K) \longrightarrow H^1(O_K[1/S'], T/p^N)^\vee$$

is the homomorphism defined in (13)*. In particular, we can take a suitable finite set $S \subset \mathcal{P}_{1,\sigma}(K')$ such that $S \cap S' = \varnothing$ and*

$$\bigoplus_{\ell \in S} \mathcal{H}^2_\ell(K) \xrightarrow{r_S} H^1(O_K[1/S'], T/p^N)^\vee$$

is surjective where r_S was defined in (14)*.*

Proof. The second statement follows from the first statement and the fact that $H^1(O_K[1/S'], T/p^N)^\vee$ is finite. So it suffices to prove the first statement.

Next, since $H^0(K', T/p^N) = 0$, the natural map $H^1(O_K[1/S'], T/p^N) \longrightarrow H^1(O_{K'}[1/S'], T/p^N)$ is injective. So the dual of this homomorphism is surjective. Therefore, we can take $x' \in H^1(O_{K'}[1/S'], T/p^N)^\vee$ whose image in $H^1(O_K[1/S'], T/p^N)^\vee$ is x. Using x' instead of x, we may assume $K' = K$.

Since $\eta^\vee$ is surjective, we can take $y \in \mathrm{Gal}(M'/L')$ such that $\eta^\vee(y \otimes t) = x$. Note that L/L' and M'/L' are linearly disjoint. Therefore, by the Chebotarev density theorem we can take infinitely many $\ell \in \mathcal{P} \setminus (\mathcal{P} \cap S')$ which split completely in L' and which satisfy $\mathrm{Frob}_{\ell_{L'}} = y$ in $\mathrm{Gal}(M'/L')$ and $\mathrm{Frob}_{\ell_{L'}} = \sigma$ in $\mathrm{Gal}(L/L')$. Then ℓ is in $\mathcal{P}_{1,\sigma}(K)$.

We know $\mathcal{H}^2_\ell(K) = \bigoplus_{v \in S_{\ell,K}} \mathcal{T}^\vee$. By the same argument as the proof of Lemma 5.14, we consider a commutative diagram

$$\begin{array}{ccc} \mathcal{H}^2_\ell(K) & \xrightarrow{r_\ell} & H^1(O_K[1/S], T/p^N)^\vee \\ \uparrow{\scriptstyle \eta'} & & \uparrow{\scriptstyle \eta^\vee} \\ \displaystyle\bigoplus_{v \in S_{\ell,L}} \mathcal{T}^\vee & \xrightarrow{r_{\ell,L'}} & \mathrm{Gal}(M'/L') \otimes \mathcal{T}^\vee \end{array}$$

Let $t_{\ell_{L'}}$ be the element in $\bigoplus_{v \in S_{\ell,L'}} \mathcal{T}^\vee$, whose $\ell_{L'}$-component is t and the other components are zero. Since $(\eta^\vee \circ r_{\ell,L'})(t_{\ell_{L'}}) = \eta^\vee(\mathrm{Frob}_{\ell_{L'}} \otimes t) = \eta^\vee(y \otimes t) = x$ and $\eta'(t_{\ell_{L'}}) = t_{\ell,K}$, we have $r_\ell(t_{\ell,K}) = x$. □

Remark 5.17. Let K'/K be an extension of fields in $\mathcal{K}_{(p)}$. As in the statement of Proposition 5.16, we can prove in Lemma 5.14 the existence of infinitely many $\ell \in \mathcal{P}'_0(K')$ such that $\ell \notin S'$ and $r_\ell(t_{\ell,K}) = x$, by the same method as the proof of Proposition 5.16.

6. Euler systems of Gauss sum type

In Sections 6–9, we generalize the results in [16]. A key point is the definition of the Euler system and the Kolyvagin system in this section and the next section.

6.1. **Control theorems.** Let K be a number field of finite degree and K_∞/K be the cyclotomic $\mathbf{Z}_p$-extension. We put $\Gamma = \mathrm{Gal}(K_\infty/K)$, and suppose that S is a finite set of primes of K. We put $S' = S \cup P_{\mathrm{bad}} \cup \{p\}$. We have a commutative diagram of exact sequences

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^1_{\mathrm{Gr}}(O_K[1/S], A) & \longrightarrow & H^1_{et}(O_K[1/S'], A) & \longrightarrow & \bigoplus_{v\in(S'\setminus S)_K} M_{K,v} \\ & & \downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_2} & & \downarrow{\scriptstyle \alpha_3} \\ 0 & \longrightarrow & H^1_{\mathrm{Gr}}(O_{K_\infty}[1/S], A)^\Gamma & \longrightarrow & H^1_{et}(O_{K_\infty}[1/S'], A)^\Gamma & \longrightarrow & \Big(\bigoplus_{w\in(S'\setminus S)_{K_\infty}} M_{K_\infty,w}\Big)^\Gamma \end{array}$$

where $M_{K,v} = H^1(K_v, A)/H^1_{\mathrm{Gr}}(K_v, A)$, $M_{K_\infty,w} = H^1(K_{\infty,w}, A)/H^1_{\mathrm{Gr}}(K_{\infty,w}, A)$, and $(S' \setminus S)_{K_\infty}$ is the set of primes of K_∞ above $S' \setminus S$. If we assume $H^0(K, A) = 0$, α_2 is bijective. By definition, α_3 is injective. Therefore, we have

Lemma 6.2. *Suppose that $H^0(K, A) = 0$. Then for any finite set S of prime numbers, we have an isomorphism*

$$H^1_{\mathrm{Gr}}(O_K[1/S], A) \xrightarrow{\simeq} H^1_{\mathrm{Gr}}(O_{K_\infty}[1/S], A)^\Gamma.$$

By definition, for a prime v of K, $H^1_{\mathrm{Gr}}(K_v, T/p^N)$ is the inverse image of $H^1_{\mathrm{Gr}}(K_{\infty,w}, A)$ under the natural map $H^1(K_v, T/p^N) \longrightarrow H^1(K_{\infty,w}, A)$ for any prime w of K_∞ above v. Therefore, by the same argument as Lemma 6.2, we obtain

Lemma 6.3. *Suppose that $H^0(K, A) = 0$. Then for any finite set S of prime numbers and for any $N > 0$, we have an isomorphism*

$$H^1_{\mathrm{Gr}}(O_K[1/S], T/p^N) \xrightarrow{\simeq} H^1_{\mathrm{Gr}}(O_{K_\infty}[1/S], T/p^N)^\Gamma.$$

Corollary 6.4. *Under the assumptions (I), (I)*, (IV-1), (IV-2), (IV-3), we have an isomorphism*

$$H^1_f(O_K[1/S], M) \xrightarrow{\simeq} H^1_f(O_{K_\infty}[1/S], M)^\Gamma$$

where $M = A$, A^*, T/p^N, T^*/p^N for any $K \in \mathcal{K}_{(p)}$ and for any $N > 0$.

Proof. This follows from Lemmas 6.2, 6.3 and 5.2. □

Let $\mathbf{Q}_n$ be the intermediate field of $\mathbf{Q}_\infty/\mathbf{Q}$ such that $[\mathbf{Q}_n : \mathbf{Q}] = p^n$. We put $R_n = \mathbf{Z}_p[\mathrm{Gal}(\mathbf{Q}_n)/\mathbf{Q})]$. We considered the higher Stickelberger ideal $\Theta_i^{(N)}$ in Corollary 4.5. We define the ideal $\Theta_i^{(N)}(\mathbf{Q}_n)$ of R_n/p^N by the image of $\Theta_i^{(N)}$ under the natural map $\Lambda/p^N \longrightarrow R_n/p^N$.

Corollary 6.5. *Under the assumptions in Subsection 2.1, we have*

$$\Theta_i^{(N)}(\mathbf{Q}_n) \subset \mathrm{Fitt}_{i,R_n/p^N}(H^1_{\mathrm{Gr}}(O_{\mathbf{Q}_n}, T/p^N)^\vee) \subset \mathrm{Fitt}_{i,R_n/p^N}(H^1_f(O_{\mathbf{Q}_n}, T/p^N)^\vee)$$

for all $i \geq 0$.

Proof. By definition, we have $\mathrm{Sel}(\mathbf{Q}_\infty, A)^\vee \otimes \mathbf{Z}/p^N = H^1_{\mathrm{Gr}}(O_{\mathbf{Q}_\infty}, T/p^N)^\vee$. Therefore, Corollary 6.5 follows from Lemma 6.3 and Corollary 4.5. □

6.6. **An annihilation result.** Let $\mathcal{K}_{(p)}$ be the set defined in (10). Suppose that K is in $\mathcal{K}_{(p)}$, and $\theta_{K_\infty} \in \Lambda_{K_\infty}$ is the p-adic L-function. For $K \in \mathcal{K}_{(p)}$, we define $\theta_K \in O[\mathrm{Gal}(K/\mathbf{Q})]$ as the image of θ_{K_∞}. This definition of θ_K is not natural for $K \in \mathcal{K}$ (where $\mathcal{K}$ was defined in Subsection 2.1), but for simplicity we adopt this definition even for $K \in \mathcal{K}$.

Theorem 6.7. *For any* $K \in \mathcal{K}_{(p)}$, θ_K *annihilates* $H^1_{\mathrm{Gr}}(O_K, A)^\vee$, *namely we have* $\theta_K H^1_{\mathrm{Gr}}(O_K, A)^\vee = 0$.

Proof. We may assume $K = \mathbf{Q}(n)_m$ for some squarefree product n of primes in $\mathcal{P}$ and for some $m \in \mathbf{Z}_{\geq 0}$. Let $\xi_K \in O[\mathrm{Gal}(K/\mathbf{Q})]$ be the image of ξ_{K_∞}. By Corollary 3.5 and Lemma 6.2, we get

$$\xi_K \in \mathrm{Fitt}_{0,O[\mathrm{Gal}(K/\mathbf{Q})]}(H^1_{\mathrm{Gr}}(O_K, A)^\vee).$$

By the proof of Lemma 3.2, ξ_K can be written as

$$\xi_K = \theta_K + \sum_{d|n,\ d\neq n} c_d \nu_{K/\mathbf{Q}(d)_m}(\theta_{\mathbf{Q}(d)_m})$$

for some $c_d \in O[\mathrm{Gal}(K/\mathbf{Q})]$. By induction on $[K : \mathbf{Q}]$, for any subfield F of K with $F \neq K$, we have $\theta_F H^1_{\mathrm{Gr}}(O_F, A)^\vee = 0$. This implies that $\nu_{K/F}(\theta_F)$ annihilates $H^1_{\mathrm{Gr}}(O_K, A)^\vee$. Therefore, $\xi_K H^1_{\mathrm{Gr}}(O_K, A)^\vee = 0$ implies $\theta_K H^1_{\mathrm{Gr}}(O_K, A)^\vee = 0$. □

6.8. **A preliminary lemma.** Suppose that K is in $\mathcal{K}_{(p)}$. It follows from Lemma 2.8 that the corestriction map $H^1_f(O_{K_m}, T^*/p^N) \longrightarrow H^1_f(O_K, T^*/p^N)$ becomes the zero map if m is sufficiently large (where K_m is the intermediate field of K_∞/K such that $[K_m : K] = p^m$). We take the minimal $m > 0$ satisfying this property, and put $K_{[1]} = K_m$. We define inductively $K_{[n]}$ by $K_{[n]} = (K_{[n-1]})_{[1]}$ where we applied the above definition to $K_{[n-1]}$ instead of K.

Let S be a finite subset of $\mathcal{P}$. The following lemma is easy to prove, but is useful.

Lemma 6.9. *Let* g, g' *be elements in* $H^1_f(O_K[1/S], T^*/p^N)$. *Suppose that* $g = \mathrm{Cor}(g_1)$, $g' = \mathrm{Cor}(g_1')$ *for some* g_1, $g_1' \in H^1_f(O_{K_{[1]}}[1/S], T^*/p^N)$ *where* $\mathrm{Cor} : H^1_f(O_{K_{[1]}}[1/S], T^*/p^N) \longrightarrow H^1_f(O_K[1/S], T^*/p^N)$ *is the corestriction map. Let* $\partial : H^1_f(O_{K_{[1]}}[1/S], T^*/p^N) \longrightarrow \bigoplus_{\ell\in S} \mathcal{H}^2_\ell(K_{[1]})$ *be the natural map in Corollary 5.6 for* $K_{[1]}$. *If* $\partial(g_1) = \partial(g_1')$, *then we have* $g = g'$.

Proof. In fact, $g_1 - g_1'$ is in the kernel of ∂. Hence it is in $H^1_f(O_{K_{[1]}}, T^*/p^N)$. Therefore, $g - g' = \mathrm{Cor}(g_1 - g_1') = 0$. □

6.10. **Construction of Euler systems of Gauss sum type.** Let $\mathcal{K}$ and $\mathcal{K}_{(p)}$ be the sets of fields as in Subsection 5.1. For any $K \in \mathcal{K}_{(p)}$, we consider the sets $\mathcal{P}_1(K) \subset \mathcal{P}_0(K)$ of primes, which are defined in Subsection 5.8. In Section 6–8, for each $\ell \in \mathcal{P}_0$, we take $t \in H^0(\mathbf{F}_\ell, T^*/p^N(-1))$ such that t generates a free O/p^N-submodule of rank 1 and fix it. We denote by $t_{\ell,K}$ the element in $\mathcal{H}^2_\ell(K)$ whose ℓ_K-component is t and the other components are 0.

Suppose that ℓ is in $\mathcal{P}_0(K_{[1]})$. By Theorem 6.7, $\theta_{K_{[1]}}$ annihilates $H^1_{\mathrm{Gr}}(O_{K_{[1]}}, A)^\vee$, and hence $H^1_f(O_{K_{[1]}}, T/p^N)^\vee$. It follows from Corollary 5.6 that

$$H^1_f(O_{K_{[1]}}[1/\ell], T^*/p^N) \xrightarrow{\partial} \mathcal{H}^2_\ell(K_{[1]}) \longrightarrow H^1_f(O_{K_{[1]}}, T/p^N)^\vee$$

is exact (where $\mathcal{H}^2_\ell(K_{[1]})$ was defined in (12)). Hence $\theta_{K_{[1]}} H^1_f(O_{K_{[1]}}, T/p^N)^\vee = 0$ implies that there is an element $g \in H^1_f(O_{K_{[1]}}[1/\ell], T^*/p^N)$ such that $\partial(g) = \theta_{K_{[1]}} t_{\ell,K_{[1]}}$. We define $g_\ell^{(K)}$ by

$$g_\ell^{(K)} = \mathrm{Cor}_{K_{[1]}/K}(g) \in H^1_f(O_K[1/\ell], T^*/p^N).$$

By Lemma 6.9, this element does not depend on the choice of g, and satisfies

$$\partial(g_\ell^{(K)}) = \theta_K t_{\ell,K}.$$

Suppose that $K, L \in \mathcal{K}_{(p)}$ such that $K \subset L$. Suppose also that $\ell \in \mathcal{P}_0(L_{[1]})$, hence $g_\ell^{(L)}$ is defined. Note that this implies $\ell \in \mathcal{P}_0(K_{[1]})$, so $g_\ell^{(K)}$ is also defined. In this situation, it is easy to check

Lemma 6.11. *Suppose that $\ell \in \mathcal{P}_0(L_{[1]})$. Let $\mathrm{Cor}_{L/K} : H^1_f(O_L[1/\ell], T^*/p^N) \longrightarrow H^1_f(O_K[1/\ell], T^*/p^N)$ be the corestriction homomorphism, and $S = \mathcal{R}(L_\infty/K_\infty)$ be the set of primes in $\mathcal{P}$ which are ramified in L_∞ and unramified in K_∞. Then we have*

$$\mathrm{Cor}_{L/K}(g_\ell^{(L)}) = \Big(\prod_{\ell \in S} P_\ell(\mathrm{Frob}_{\ell,K_\infty}^{-1}) \Big) g_\ell^{(K)}.$$

Proof. Let $g' \in H^1_f(O_{L_{[1]}}[1/\ell], T^*/p^N)$ be an element such that $\partial(g') = \theta_{L_{[1]}} t_{\ell,L_{[1]}}$, and $g \in H^1_f(O_{K_{[1]}}[1/\ell], T^*/p^N)$ be an element such that $\partial(g) = \theta_{K_{[1]}} t_{\ell,K_{[1]}}$. Put $g'' = \mathrm{Cor}_{L_{[1]}/K_{[1]}}(g') \in H^1_f(O_{K_{[1]}}[1/\ell], T^*/p^N)$. Since $c_{L_{[1]}/K_{[1]}}(\theta_{L_{[1]}}) = \Big(\prod_{\ell \in S} P_\ell\big(\mathrm{Frob}_{\ell,K_{[1],\infty}}^{-1}\big) \Big) \theta_{K_{[1]}}$ by (3) where $c_{L_{[1]}/K_{[1]}}$ is the restriction map of group rings, we have

$$\partial(g'') = \Big(\prod_{\ell \in S} P_\ell\big(\mathrm{Frob}_{\ell,K_{[1],\infty}}^{-1}\big) \Big) \theta_{K_{[1]}} t_{\ell,K_{[1]}} = \partial\Big(\Big(\prod_{\ell \in S} P_\ell\big(\mathrm{Frob}_{\ell,K_{[1],\infty}}^{-1}\big) \Big) g \Big).$$

Note that $\mathrm{Cor}_{L_{[1]}/L}(g') = g_\ell^{(L)}$ and $\mathrm{Cor}_{K_{[1]}/K}(g) = g_\ell^{(K)}$ by definition. Since $\mathrm{Cor}_{K_{[1]}/K}(g'') = \mathrm{Cor}_{L/K}(g_\ell^{(L)})$, the above equation implies

$$\mathrm{Cor}_{L/K}(g_\ell^{(L)}) = \Big(\prod_{\ell \in S} P_\ell\big(\mathrm{Frob}_{\ell,K_\infty}^{-1}\big) \Big) g_\ell^{(K)}$$

by Lemma 6.9. □

This lemma shows that $(g_\ell^{(K)})$ forms an Euler system. But this Euler system relation holds only for subfields K of L. Let K_∞/K be the cyclotomic $\mathbf{Z}_p$-extension, and K_n the intermediate field of degree p^n. We cannot define $(g_\ell^{(K_n)})_{n\geq 0}$ for all $n \geq 0$ because ℓ cannot split completely in all K_n. Our $(g_\ell^{(K)})$ is a finite Euler system in the terminology of Mazur and Rubin [19].

7. Kolyvagin systems of Gauss sum type

7.1. **Two homomorphisms ∂_ℓ and ϕ_ℓ.** We first define two important homomorphisms which play a central role in the theory of Kolyvagin systems.

We fix a primitive p^n-th root of unity $\zeta_{p^n} \in \overline{\mathbf{Q}}$ for every $n > 0$ such that $(\zeta_{p^n}) \in \varprojlim \mu_{p^n} = \mathbf{Z}_p(1)$. Recall that for any prime $\ell \in \mathcal{P}_0$, we fix a prime $\ell_{\overline{\mathbf{Q}}}$. We regard ζ_{p^n} as an element of $\overline{\mathbf{Q}}_\ell$, using the prime $\ell_{\overline{\mathbf{Q}}}$. Let $\mathbf{Q}(\ell)$ be the subfield of $\mathbf{Q}(\mu_\ell)$ of degree p^{n_ℓ} where $n_\ell = \mathrm{ord}_p(\ell - 1)$. We denote by $\mathcal{G}_\ell$ the Galois group $\mathrm{Gal}(\mathbf{Q}(\ell)/\mathbf{Q})$. We identify $\mathcal{G}_\ell$ with the decomposition group $\mathcal{D}_\ell$ of $\mathcal{G}_\ell$ at ℓ. Since $\mu_{p^{n_\ell}}$ is contained in $\mathbf{Q}_\ell$, we have an isomorphism $\mathcal{G}_\ell = \mathcal{D}_\ell \simeq \mu_{p^{n_\ell}}$ by Kummer theory. We denote by σ_ℓ the element of $\mathcal{G}_\ell$ that corresponds to $\zeta_{p^{n_\ell}}$.

Suppose that $\ell \in \mathcal{P}$ and $k = \mathbf{Q}_\ell$. We denote by

$$\partial_\ell : H^1(k, T^*/p^N) \longrightarrow H^0(\mathbf{F}_\ell, T^*/p^N(-1))$$

the homomorphism induced by $H^1(k, T^*/p^N) \to H^1(k, T^*/p^N)/H^1_f(k, T^*/p^N) \simeq H^0(\mathbf{F}_\ell, T^*/p^N(-1))$. We note that when $T = \mathbf{Z}_p$, $\partial_\ell : H^1(k, \mathbf{Z}/p^N(1)) = k^\times \otimes \mathbf{Z}/p^N \longrightarrow \mathbf{Z}/p^N$ is the divisor map, so the above map ∂_ℓ is the analog of the divisor map. For any $K \in \mathcal{K}_{(p)}$, we consider the map

$$\begin{aligned}\partial_\ell : H^1(K, T^*/p^N) &\longrightarrow \bigoplus_{v\in S_{\ell,K}} H^1(K_v, T^*/p^N) \\ &\longrightarrow \bigoplus_{v\in S_{\ell,K}} H^0(\kappa(v), T^*/p^N(-1)) = \mathcal{H}^2_\ell(K)\end{aligned}$$

which we also denote by ∂_ℓ. If ℓ is in $\mathcal{P}_1(K)$, we identify $\mathcal{H}^2_\ell(K)$ with $O/p^N[\mathrm{Gal}(K/\mathbf{Q})]$, using $t_{\ell,K}$ which was defined in Subsection 6.10. Using this identification, we regard ∂_ℓ as

$$\partial_\ell : H^1(K, T^*/p^N) \longrightarrow O/p^N[\mathrm{Gal}(K/\mathbf{Q})].$$

Next, we take $\ell \in \mathcal{P}_1$. Put $k = \mathbf{Q}_\ell$. Since $\ell \equiv 1 \pmod{p^N}$, the absolute Galois group G_k of k acts on μ_{p^N} trivially. The absolute Galois group $G_{\mathbf{F}_\ell}$ of $\mathbf{F}_\ell$ also acts on μ_{p^N} trivially. Therefore, both $H^i(\mathbf{F}_\ell, T^*/p^N)$ and $H^i(\mathbf{F}_\ell, T^*/p^N(-1))$ $(i = 0, 1)$ are free of rank 1 over O/p^N. Also, both $H^i(\mathbf{F}_\ell, T/p^N)$ and $H^i(\mathbf{F}_\ell, T/p^N(-1))$ $(i = 0, 1)$ are free of rank 1 over O/p^N.

We know that $H^1(k, T^*/p^N)$ is a free O/p^N-module of rank 2. In fact, the localization sequence yields an exact sequence

$$0 \longrightarrow H^1(\mathbf{F}_\ell, T^*/p^N) \longrightarrow H^1(k, T^*/p^N) \longrightarrow H^0(\mathbf{F}_\ell, T^*/p^N(-1)) \longrightarrow 0,$$

and $H^1(\mathbf{F}_\ell, T^*/p^N)$ and $H^0(\mathbf{F}_\ell, T^*/p^N(-1))$ are free of rank 1 over O/p^N. The image of $H^1(\mathbf{F}_\ell, T^*/p^N)$ in $H^1(k, T^*/p^N)$ coincides with $H^1_f(k, T^*/p^N)$.

We consider a field $k(\ell)$ which is the subfield of $k(\mu_\ell) = \mathbf{Q}_\ell(\mu_\ell)$ of degree p^{n_ℓ}. The extension $k(\ell)/k$ is a totally ramified extension. We identify $\mathcal{G}_\ell$ with $\mathrm{Gal}(k(\ell)/k)$. We have

$$H^1(k, T^*/p^N) = H^1_f(k, T^*/p^N) \oplus H^1(\mathcal{G}_\ell, H^0(k(\ell), T^*/p^N)). \tag{15}$$

In fact, $H^1(\mathcal{G}_\ell, H^0(k(\ell), T^*/p^N))$ is the kernel of the natural map $H^1(k, T^*/p^N) \longrightarrow H^1(k(\ell), T^*/p^N)$, and is isomorphic to O/p^N. Also, the restriction of this natural map to $H^1_f(k, T^*/p^N)$ is injective. These facts imply the above decomposition. Using the decomposition (15), we obtain a homomorphism

$$\phi'_k : H^1(k, T^*/p^N) \longrightarrow H^1_f(k, T^*/p^N) = H^1(\mathbf{F}_\ell, T^*/p^N).$$

Since $\ell \in \mathcal{P}_1$, by [28, Lemma 4.5.2] there is a unique $Q_\ell(x) \in O/p^N[x]$ such that $P_\ell(x) = (x-1)Q_\ell(x)$ in $O/p^N[x]$. We consider

$$H^1(\mathbf{F}_\ell, T^*/p^N) \xrightarrow{Q_\ell(\mathrm{Frob}_\ell^{-1})} H^0(\mathbf{F}_\ell, T^*/p^N)$$

which is induced by the multiplication by $Q_\ell(\mathrm{Frob}_\ell^{-1})$. We define (see [28, Sec. 4.5])

(16)

$$\phi_k : H^1(k, T^*/p^N) \xrightarrow{\phi'_k} H^1(\mathbf{F}_\ell, T^*/p^N) \xrightarrow{Q_\ell(\mathrm{Frob}_\ell^{-1})} H^0(\mathbf{F}_\ell, T^*/p^N) \longrightarrow O/p^N$$

by the composition of ϕ'_k, $Q_\ell(\mathrm{Frob}_\ell^{-1})$, and $t \otimes \zeta_{p^N} \mapsto 1$. We note that when $T = \mathbf{Z}_p$, $\phi_k : H^1(k, \mathbf{Z}/p^N(1)) = k^\times \otimes \mathbf{Z}/p^N \longrightarrow H^0(\mathbf{F}_\ell, \mathbf{Z}/p^N(1)) = \mu_{p^N} \simeq \mathrm{Gal}(k(\ell)/k) \otimes \mathbf{Z}/p^N$ is the reciprocity map (the tame symbol), so the above map ϕ_k is the analog of the reciprocity map. We know that the kernel of $\phi'_k : H^1(k, T^*/p^N) \longrightarrow H^1(\mathbf{F}_\ell, T^*/p^N)$ is $H^1(\mathcal{G}_\ell, H^0(k(\ell), T/p^N))$ and $Q_\ell(\mathrm{Frob}_\ell^{-1}) : H^1(\mathbf{F}_\ell, T^*/p^N) \longrightarrow H^0(\mathbf{F}_\ell, T^*/p^N)$ is bijective [28, Cor. A.2.7]. Therefore, ϕ_k induces an isomorphism of O/p^N-modules on $H^1_f(k, T^*/p^N)$.

Lemma 7.2. *Let $e_1, \dots, e_d$ be a basis of T. We take $t = e_d^\vee$, and consider σ and $\ell \in \mathcal{P}_{1,\sigma}$ as in Subsection 5.8.*

(1) Let $e_1^\vee, \dots, e_d^\vee$ be the dual basis of $(T/p^N)^\vee$, and put $e_1^* = e_1^\vee \otimes \zeta_{p^N}, \dots, e_d^* = e_d^\vee \otimes \zeta_{p^N} \in T^*/p^N$. Then $H^1(\mathbf{F}_\ell, T^*/p^N) = (T^*/p^N)/(\mathrm{Frob}_\ell - 1)$ is generated by the class of e_1^*, $H^0(\mathbf{F}_\ell, T^*/p^N)$ is generated by e_d^*, and

$$H^1(\mathbf{F}_\ell, T^*/p^N) \xrightarrow{Q_\ell(\mathrm{Frob}_\ell^{-1})} H^0(\mathbf{F}_\ell, T^*/p^N)$$

is the map which sends the class of e_1^* to $-e_d^*$.

(2) Let $\phi_k : H^1(k, T^*/p^N) \longrightarrow O/p^N$ be the map defined above. The restriction of ϕ_k to $H^1_f(k, T^*/p^N) = H^1(\mathbf{F}_\ell, T^*/p^N) = (T^*/p^N)/(\mathrm{Frob}_\ell - 1)$ is induced by $e_1^* \mapsto -1$, $e_2^* \mapsto 0, \dots, e_d^* \mapsto 0$.

Proof. (1) Since Frob_ℓ acts on T^*/p^N by

$$\begin{pmatrix} 1 & & & \dots & 0 \\ 1 & 1 & & & \vdots \\ & 1 & \ddots & & \\ \vdots & & \ddots & 1 & \\ 0 & \dots & & 1 & 1 \end{pmatrix},$$

we have

$$H^1(\mathbf{F}_\ell, T^*/p^N) = (T^*/p^N)/(\mathrm{Frob}_\ell - 1) = (T^*/p^N)/\langle e_2^*, \dots, e_d^* \rangle.$$

Thus, $H^1(\mathbf{F}_\ell, T^*/p^N)$ is a free O/p^N-module of rank 1 generated by the class of e_1^*. We know $P_\ell(x) = (1-x)^d$ and $Q_\ell(x) = -(1-x)^{d-1}$. Hence $Q_\ell(\mathrm{Frob}_\ell^{-1}) = -\mathrm{Frob}_\ell^{1-d}(\mathrm{Frob}_\ell - 1)^{d-1}$ and it maps e_1^* to $-e_d^*$. This proves Proposition 7.2(1).
(2) This follows from (1). □

For a number field K and for $\ell \in \mathcal{P}_1(K)$, we apply the above argument to K_v for v which is above ℓ, and get a homomorphism $\phi_{K_v} : H^1(K_v, T^*/p^N) \longrightarrow H^0(\kappa(v), T^*/p^N)$. We denote by ϕ_ℓ the composition

$$\begin{aligned} \phi_\ell : H^1(K, T^*/p^N) &\longrightarrow \bigoplus_{v|\ell} H^1(K_v, T^*/p^N) \\ &\longrightarrow \bigoplus_{v|\ell} H^0(\kappa(v), T^*/p^N) \simeq O/p^N[\mathrm{Gal}(K/\mathbf{Q})]. \end{aligned} \tag{17}$$

Here, the last isomorphism is defined by $t_{\ell,K} \otimes \zeta_{p^N} \mapsto 1$.

7.3. **A lemma for the construction of Kolyvagin systems.** In this subsection, we prove the following Lemma 7.4 which corresponds to [16, Lemma 5.5].

First of all, we fix the notation related to several homomorphisms. We consider the homomorphism

$$r_S : \bigoplus_{\ell \in S} \mathcal{H}_\ell^2(K) \longrightarrow H_f^1(O_K, T/p^N)^\vee$$

which was defined in (14). Enlarging S to all good primes, we define a homomorphism r_K;

$$r_K : \bigoplus_{\ell \in \mathcal{P}} \mathcal{H}_\ell^2(K) \longrightarrow H_f^1(O_K, T/p^N)^\vee. \tag{18}$$

This homomorphism r_K is surjective by Lemma 5.14 or Proposition 5.16 (note that $H_f^1(O_K[1/S'], T/p^N)^\vee \longrightarrow H_f^1(O_K, T/p^N)^\vee$ is surjective where $S' = P_{\mathrm{bad}} \cup \{p\}$).

Since $\mathcal{H}^2_\ell(K) = \bigoplus_{v\in S_{\ell,K}} H^1(K_v, T^*/p^N)/H^1_f(K_v, T^*/p^N)$, we have a natural homomorphism

$$\partial_K : H^1(K, T^*/p^N) \longrightarrow \bigoplus_{\ell\in\mathcal{P}} \mathcal{H}^2_\ell(K) \tag{19}$$

which we denote by ∂_K. For any submodule M of $H^1(K, T^*/p^N)$, the restriction of ∂_K to M is also denoted by ∂_K. For each $\ell \in \mathcal{P}_0(K)$, we use the element $t_{\ell,K}$ in $\mathcal{H}^2_\ell(K)$ (see the beginning of Subsection 6.10). We also regard $t_{\ell,K}$ as an element of $\bigoplus_{\ell\in\mathcal{P}} \mathcal{H}^2_\ell(K)$ (the element whose ℓ component is $t_{\ell,K}$ and the other components are zero).

By Corollary 5.6, we have an exact sequence

$$\begin{aligned} 0 \longrightarrow H^1_f(O_K, T^*/p^N) &\longrightarrow H^1_f(O_K[1/\mathcal{P}], T^*/p^N) \\ \xrightarrow{\partial_K} \bigoplus_{\ell\in\mathcal{P}} \mathcal{H}^2_\ell(K) &\xrightarrow{r_K} H^1_f(O_K, T/p^N)^\vee \longrightarrow 0. \end{aligned} \tag{20}$$

The next lemma corresponds to [16, Lemma 5.5].

Lemma 7.4. *(1) Suppose that $K \in \mathcal{K}_{(p)}$ where $\mathcal{K}_{(p)}$ is defined in* (10)*. Assume that $\ell_1, \dots, \ell_s$ are s distinct primes in $\mathcal{P}_1(K)$, and for each $i = 1, \dots, s$, $\sigma_i \in O/p^N[\mathrm{Gal}(K/\mathbf{Q})]$ is given. Suppose that ℓ is in $\mathcal{P}_0(K)$ and that K'/K is an extension such that $K' \in \mathcal{K}_{(p)}$. Then there are infinitely many $\ell' \in \mathcal{P}_1(K')$ which satisfy the following properties.*

(i) $r_K(t_{\ell',K}) = r_K(t_{\ell,K})$.

(ii) There is an element $z \in H^1_f(O_K[1/\ell\ell'], T^*/p^N)$ such that $\partial_K(z) = t_{\ell',K} - t_{\ell,K}$ and $\phi_{\ell_i}(z) = \sigma_i$ for each $i = 1, \dots, s$.

(2) Under the same assumption as (1), there are infinitely many $\ell' \in \mathcal{P}'_0(K')$ satisfying (i) and (ii).

Proof. (1) Put $m = \prod_{i=1}^s \ell_i$. By Proposition 5.4, we have an exact sequence

$$\begin{aligned} H^1_f(O_K[1/m\ell\ell'], T^*/p^N) \xrightarrow{\varphi} \bigoplus_{v|m} H^1(K_v, T^*/p^N) \oplus \mathcal{H}^2_\ell(K) \oplus \mathcal{H}^2_{\ell'}(K) \\ \xrightarrow{\psi} H^1_f(O_K[1/m], T/p^N)^\vee. \end{aligned}$$

Recall that the map ϕ_{K_v} defined in (16) induces an isomorphism between $H^1_f(K_v, T^*/p^N)$ and O/p^N as we explained just before Lemma 7.2. Therefore, the maps ϕ_{K_v} for all $v|\ell_i$ induce an isomorphism

$$\phi_{\ell_i,\mathrm{loc}} = ((\phi_{K_v})_{|H^1_f}) : \bigoplus_{v|\ell_i} H^1_f(K_v, T^*/p^N) \xrightarrow{\simeq} \bigoplus_{v|\ell_i} O/p^N \simeq O/p^N[\mathrm{Gal}(K/\mathbf{Q})]$$

where the last isomorphism is defined by taking $(1, 0, \dots, 0) \in \bigoplus_{v|\ell_i} O/p^N$ (the component of $\ell_{i,K}$ is 1 and the other components are 0) to be a basis as an $O/p^N[\mathrm{Gal}(K/\mathbf{Q})]$-module. Recall that ϕ_{ℓ_i} was defined as the composition of the canonical homomorphism $H^1(K, T^*/p^N) \longrightarrow \bigoplus_{v|\ell_i} H^1(K_v, T^*/p^N)$ and (ϕ_{K_v}). We take $x_i = (x_{K_v}) \in \bigoplus_{v|\ell_i} H^1_f(K_v, T^*/p^N)$ such that $\phi_{\ell_i,\mathrm{loc}}(x_i) = \sigma_i$,

and put $x = (x_i) \in \bigoplus_{v|m} H^1(K_v, T^*/p^N)$. Let y be the image of $(x, t_{\ell,K})$ under the map $\bigoplus_{v|m} H^1(K_v, T^*/p^N) \oplus \mathcal{H}^2_\ell(K) \longrightarrow H^1_f(O_K[1/m], T/p^N)^\vee$. Applying Proposition 5.16, there is $\ell' \in \mathcal{P}_1(K')$ such that $r_{\ell',K}(t_{\ell',K}) = y$. (More precisely, there are $\ell' \in \mathcal{P}_1(K')$ and $t_{\ell'} \in H^0(\mathbf{F}_\ell, T^*/p^N(-1))$ such that $r_{\ell',K}((t_{\ell'})_{\ell',K}) = y$. We write $t_{\ell',K}$ for $(t_{\ell'})_{\ell',K}$.)

Suppose that ψ is the map in the above exact sequence. We have $\psi(x, t_{\ell,K}, 0) = \psi(0, 0, t_{\ell',K}) = y$. By the above exact sequence there is $z \in H^1_f(O_K[1/m\ell\ell'], T^*/p^N)$ such that $\varphi(z) = (x, t_{\ell,K}, -t_{\ell',K})$. Since the image x_{K_v} of z in $H^1(K_v, T^*/p^N)$ is in $H^1_f(K_v, T^*/p^N)$ for v dividing m, z is in $H^1_f(O_K[1/\ell\ell'], T^*/p^N)$.

The fact that the image x_{K_v} of z in $H^1(K_v, T^*/p^N)$ is in $H^1_f(K_v, T^*/p^N)$ for v dividing m also implies that $\partial_K(z) = t_{\ell,K} - t_{\ell',K}$. Therefore, we have $r_K(t_{\ell,K} - t_{\ell',K}) = 0$, which implies (i).

By the construction of z and x_i, we have $\phi_{\ell_i}(z) = \sigma_i$, namely we get (ii). This completes the proof of Lemma 7.4(1). We can prove (2) by the same method using Lemma 5.14 and Remark 5.17 instead of Proposition 5.16. □

7.5. **Kolyvagin derivatives.** Suppose that K is in $\mathcal{K}_{(p)}$. For $\ell \in \mathcal{P}_1(K) = \{\ell \in \mathcal{P}_1 \mid \ell \text{ splits completely in } K\}$, we denote by $K(\ell)$ the maximal p-subextension of K in $K(\mu_\ell)$. We recall from Subsection 7.1 that $\mathcal{G}_\ell = \mathrm{Gal}(\mathbf{Q}(\ell)/\mathbf{Q})$. If $\ell \in \mathcal{P}_1(K)$, we have a natural isomorphism $\mathrm{Gal}(K(\ell)/K) = \mathcal{G}_\ell$.

We denote by $\mathcal{N}_1$ (resp. $\mathcal{N}_1(K)$) the set of all squarefree products of primes in $\mathcal{P}_1$ (resp. $\mathcal{P}_1(K)$). By convention 1 is in both $\mathcal{N}_1$ and $\mathcal{N}_1(K)$. For any $m = \ell_1 \cdots \ell_r \in \mathcal{N}_1(K)$, we define $K(m)$ to be the compositum of the fields $K(\ell_1), \ldots, K(\ell_r)$, and $\mathcal{G}_m = \mathcal{G}_{\ell_1} \times \cdots \times \mathcal{G}_{\ell_r}$. By definition, $K(m)$ is in $\mathcal{K}_{(p)}$ and $\mathrm{Gal}(K(m)/K) = \mathcal{G}_m$.

Lemma 7.6. *The natural homomorphism*

$$H^1_f(O_K[1/m\ell], T^*/p^N) \xrightarrow{\simeq} H^1_f(O_{K(m)}[1/m\ell], T^*/p^N)^{\mathcal{G}_m}$$

is bijective.

Proof. Let S' be the union of $P_{\mathrm{bad}} \cup \{p\}$ and the set of prime numbers dividing $m\ell$. By our assumption (I)*, $H^1_{\mathrm{et}}(O_K[1/S'], T^*/p^N) \longrightarrow H^1_{\mathrm{et}}(O_{K(m)}[1/S'], T^*/p^N)^{\mathcal{G}_m}$ is bijective. Let v be a prime of K above $P_{\mathrm{bad}} \cup \{p\}$ and w be a prime of $K(m)$ above v. Using the same method as the proof of Lemma 6.2, in order to prove this lemma, we have only to show the injectivity of

$$H^1(K_v, T^*/p^N)/H^1_f(K_v, T^*/p^N) \longrightarrow H^1(K(m)_w, T^*/p^N)/H^1_f(K(m)_w, T^*/p^N).$$

In general, if k is a local field and k'/k is unramified, the homomorphism

$$H^1(k, T^*/p^N)/H^1_{\mathrm{Gr}}(k, T^*/p^N) \longrightarrow H^1(k', T^*/p^N)/H^1_{\mathrm{Gr}}(k', T^*/p^N)$$

is injective by the definition of H^1_{Gr}. Therefore, the above injectivity follows from Lemma 5.2 and the fact that v is unramified in $K(m)/K$. □

As usual, we use

$$N_\ell = \sum_{i=0}^{p^{n_\ell}-1} \sigma_\ell^i \in \mathbf{Z}[\mathcal{G}_\ell],\ D_\ell = \sum_{i=0}^{p^{n_\ell}-1} i\sigma_\ell^i \in \mathbf{Z}[\mathcal{G}_\ell],$$

$N_m = \Pi_{\ell|m} N_\ell \in \mathbf{Z}[\mathcal{G}_m]$, and $D_m = \Pi_{\ell|m} D_\ell \in \mathbf{Z}[\mathcal{G}_m]$.

For $K \in \mathcal{K}$, $m \in \mathcal{N}_1(K)$, and $\ell \in \mathcal{P}_0(K(m)_{[1]})$, by the standard method we can check that $D_m g_\ell^{K(m)}$ is in $H^1_f(O_{K(m)}[1/m\ell], T^*/p^N)^{\mathcal{G}_m}$. We define

$$\kappa_{m,\ell} = \kappa_{m,\ell}^{(K)} \in H^1_f(O_K[1/m\ell], T^*/p^N)$$

to be the unique element whose image in $H^1_f(O_{K(m)}[1/m\ell], T^*/p^N)$ is $D_m g_\ell^{K(m)}$.

The following lemma is a basic property of $\kappa_{m,\ell}$.

Proposition 7.7. *Suppose that $m \in \mathcal{N}_1(K)$. We take n_0 sufficiently large such that $\mathrm{Gal}(K_\infty/K_{n_0})$ acts trivially on T^*/p^N and that every prime of K_{n_0} dividing m is inert in K_∞/K_{n_0}. We assume that $\ell \in \mathcal{P}_0(K(m)_{[1]})$ and $\ell \in \mathcal{P}_0(K_{n_0+N})$. Then, for any prime r such that $r|m$, we have*

$$\partial_r(\kappa_{m,\ell}) = \phi_r(\kappa_{\frac{m}{r},\ell}).$$

Remark 7.8. The assumption on ℓ in Proposition 7.7 implies that $\ell \in \mathcal{P}_0'(K_{n_0+N})$, especially $\ell \in \mathcal{P}_0'$. Therefore, if ℓ satisfies the conditions of the above lemma and $d > 1$, ℓ is not in $\mathcal{P}_1$. In the next subsection we will construct $\kappa_{m,\ell}$ for $\ell \in \mathcal{P}_1$, and will prove the same property for these $\kappa_{m,\ell}$.

Proof. The method in Rubin [28, Chap. 4] using the universal Euler systems can be applied directly. Note that we are assuming $H^0(K, A^*) = 0$, so the argument in [28] can be used even for "finite Euler systems". The condition $\ell \in \mathcal{P}_0(K_{n_0+N})$ is needed in the argument on page 100 in Rubin [28]. □

We next study $\partial_\ell(\kappa_{m,\ell})$. Suppose that $K \in \mathcal{K}$, and $m = \ell_1 \cdots \ell_r \in \mathcal{N}_1(K)$. Then there is $\delta_m \in O/p^N[\mathrm{Gal}(K/\mathbf{Q})]$ such that $D_m \theta_{K(m)} \equiv \delta_m N_m \bmod p^N$. We also remark that δ_m appears as a coefficient of $\theta_{K(m)}$, namely $\theta_{K(m)}$ can be written as

$$\theta_{K(m)} \equiv (-1)^r \delta_m (\sigma_{\ell_1} - 1) \cdots (\sigma_{\ell_r} - 1) \bmod (p^N, (\sigma_{\ell_1} - 1)^2, \ldots, (\sigma_{\ell_r} - 1)^2) \tag{21}$$

(see [15, Lemma 4.4]). When we clarify the field we are dealing with, we write $\delta_m^{(K)}$ instead of δ_m. The element $\delta_m^{(K)}$ is determined by the above property. The following lemma is easily checked (cp. [16, Sec. 4]).

Lemma 7.9. *Assume that $\ell \in \mathcal{P}_0(K(m)_{[1]})$. Then we have*

$$\partial_\ell(\kappa_{m,\ell}) = \delta_m.$$

7.10. **Construction of a Kolyvagin system.** For a squarefree positive integer m, we define $\epsilon(m)$ to be the number of primes which divide m. Suppose that $m \in \mathcal{N}_1(K_{[\epsilon(m)+1]})$. Our goal in this subsection is to define $\kappa_{m,\ell}$ not only for $\ell \in \mathcal{P}_0(K(m)_{[1]}) \cap \mathcal{P}_0(K_{n_0+N})$ (see Proposition 7.7), but also for $\ell \in \mathcal{P}_1(K_{[\epsilon(m)+1]}) = \mathcal{P}_1(K_{[\epsilon(m\ell)]})$.

Suppose that $m \in \mathcal{N}_1(K)$ and $\ell \in \mathcal{P}_0(K)$ such that ℓ does not divide m. We say that a system $(\alpha_{d,\ell})_{d|m}$ (where d ranges over all divisors of m) is a *weak Kolyvagin system of Gauss sum type* if the following conditions are satisfied for any d dividing m.

(0) $\alpha_{d,\ell}$ is in $H^1_f(O_K[1/d\ell], T^*/p^N)$.
(1) For any prime r dividing d, we have $\partial_r(\alpha_{d,\ell}) = \phi_r(\alpha_{\frac{d}{r},\ell})$.
(2) $\partial_\ell(\alpha_{d,\ell}) = \delta_d$.

When no confusion arises, we say $\alpha_{m,\ell}$ is a weak Kolyvagin system of Gauss sum type instead of saying $(\alpha_{d,\ell})_{d|m}$ is so. For example, $\kappa_{m,\ell}$ is a weak Kolyvagin system of Gauss sum type when m and ℓ satisfy the conditions of Proposition 7.7. Note that we are using the terminology "weak Kolyvagin system" in a different way from Mazur and Rubin [19].

Proposition 7.11. *Suppose that $\alpha_{m,\ell'}$ is a weak Kolyvagin system of Gauss sum type, and that for any prime r dividing m, $\alpha_{\frac{m}{r},r}$ are weak Kolyvagin systems of Gauss sum type. We assume that there are a prime $\ell \in \mathcal{P}_0(K)$ and $b \in H^1_f(O_K[1/\ell\ell'], T^*/p^N)$ such that $\ell \nmid m\ell'$ and $\partial(b) = t_{\ell',K} - t_{\ell,K}$ where ∂ is the map $H^1_f(O_K[1/\ell\ell'], T^*/p^N) \longrightarrow \mathcal{H}^2_\ell(K) \oplus \mathcal{H}^2_{\ell'}(K)$ in Corollary 5.6. Put*

$$\alpha'_{d,\ell} = \alpha_{d,\ell'} - \delta_d b - \sum_{r|d} \phi_r(b)\alpha_{\frac{d}{r},r} \in H^1_f(O_K[1/d\ell\ell'], T^*/p^N).$$

Then $(\alpha'_{d,\ell})_{d|m}$ is a weak Kolyvagin system of Gauss sum type.

Proof. By definition, we compute

$$\partial_{\ell'}(\alpha'_{d,\ell}) = \partial_{\ell'}(\alpha_{d,\ell'}) - \delta_d \partial_{\ell'}(b) = 0,$$

which shows that $\alpha'_{d,\ell}$ satisfies (0). Next, we will show (1). For r dividing d, we have

$$\begin{aligned}\partial_r(\alpha'_{d,\ell}) &= \phi_r\big(\alpha_{\frac{d}{r},\ell'}\big) - \sum_{r'|\frac{d}{r}} \phi_{r'}(b)\phi_r\Big(\alpha_{\frac{d}{rr'},r'}\Big) - \phi_r(b)\delta_{\frac{d}{r}} \\ &= \phi_r(\alpha'_{\frac{d}{r},\ell}).\end{aligned}$$

We also have $\partial_\ell(\alpha'_{d,\ell}) = -\delta_\ell \partial_\ell(b) = \delta_\ell$, which is Property (2). This completes the proof of Proposition 7.11. □

Lemma 7.12. *Suppose that $m \in \mathcal{N}_1(K_{[1]})$, $\ell \in \mathcal{P}_0(K_{[1]})$, and $(\alpha_{d,\ell})_{d|m}$, $(\beta_{d,\ell})_{d|m}$ are weak Kolyvagin systems of Gauss sum type over $K_{[1]}$ such that $\partial_r(\alpha_{d,\ell}) = \partial_r(\beta_{d,\ell})$ for any r dividing $d\ell$ for any $d|m$. Then $(\mathrm{Cor}_{K_{[1]}/K}(\alpha_{d,\ell}))_{d|m}$ and $(\mathrm{Cor}_{K_{[1]}/K}(\beta_{d,\ell}))_{d|m}$ are weak Kolyvagin systems of Gauss sum type over K, and they coincide.*

Proof. It is easy to see that $(\mathrm{Cor}_{K_{[1]}/K}(\alpha_{d,\ell}))_{d|m}$ is a weak Kolyvagin system of Gauss sum type over K since all primes dividing $m\ell$ split completely in $K_{[1]}$. The coincidence between these two systems follows from Lemma 6.9. □

For any $m\ell \in \mathcal{N}_1(K_{[\epsilon(m\ell)]})$, we will define $\kappa_{m,\ell}$ by induction on $\epsilon(m\ell)$. We consider $K_{[\epsilon(m\ell)]}$ and $t_{\ell,K_{[\epsilon(m\ell)]}}$ in $\mathcal{H}^2_\ell(K_{[\epsilon(m\ell)]})$. Let

$$r_{K_{[\epsilon(m\ell)]}} : \bigoplus_{\ell\in\mathcal{P}} \mathcal{H}^2_\ell(K_{[\epsilon(m\ell)]}) \longrightarrow H^1_f(O_{K_{[\epsilon(m\ell)]}}, T/p^N)^\vee$$

be the homomorphism in (18) for $K_{[\epsilon(m\ell)]}$. For m and $K_{[\epsilon(m\ell)]}$, we take n_0 as in Proposition 7.7 and put $K' = K_{[\epsilon(m\ell)]}(m)_{[1]}K_{n_0+N}$ and $S' = P_{\mathrm{bad}} \cup \{p\}$. Since $H^1_{\mathrm{et}}(O_{K_{[\epsilon(m\ell)]}}[1/S'], T/p^N)^\vee \longrightarrow H^1_f(O_{K_{[\epsilon(m\ell)]}}, T/p^N)^\vee$ is surjective, there is $x \in H^1(O_{K_{[\epsilon(m\ell)]}}[1/S'], T/p^N)^\vee$ whose image in $H^1_f(O_{K_{[\epsilon(m\ell)]}}, T/p^N)^\vee$ is $r_{K_{[\epsilon(m\ell)]}}(t_{\ell,K_{[\epsilon(m\ell)]}})$. Using Lemma 5.14 and Remark 5.17 for $K_{[\epsilon(m\ell)]}$, we can take $\ell' \in \mathcal{P}'_0(K')$ such that $r_{K_{[\epsilon(m\ell)]}}(t_{\ell',K_{[\epsilon(m\ell)]}}) = x$, so $r_{K_{[\epsilon(m\ell)]}}(t_{\ell',K_{[\epsilon(m\ell)]}}) = r_{K_{[\epsilon(m\ell)]}}(t_{\ell,K_{[\epsilon(m\ell)]}})$ in $H^1_f(O_{K_{[\epsilon(m\ell)]}}, T/p^N)^\vee$. Since $r_{K_{[\epsilon(m\ell)]}}(t_{\ell',K_{[\epsilon(m\ell)]}} - t_{\ell,K_{[\epsilon(m\ell)]}}) = 0$, by Corollary 5.6 there is an element $b' \in H^1_f(O_{K_{[\epsilon(m\ell)]}}[1/\ell\ell'], T^*/p^N)$ such that

$$\partial_{K_{[\epsilon(m\ell)]}}(b') = t_{\ell',K_{[\epsilon(m\ell)]}} - t_{\ell,K_{[\epsilon(m\ell)]}}.$$

Put $b = \mathrm{Cor}_{K_{[\epsilon(m\ell)]}/K}(b')$. We define $\kappa_{m,\ell} \in H^1_f(O_K[1/m\ell], T^*/p^N)$ by

$$\kappa_{m,\ell} = \kappa_{m,\ell'} - \delta_m b - \sum_{r|m} \phi_r(b)\kappa_{\frac{m}{r},r}. \tag{22}$$

Note that $\kappa_{\frac{m}{r},r}$ is already defined by induction on $\epsilon(m\ell)$. When we need to clarify the field over which $\kappa_{m,\ell}$ is defined, we denote it by $\kappa^{(K)}_{m,\ell}$.

Proposition 7.13. *Suppose that $m\ell \in \mathcal{N}_1(K_{[\epsilon(m\ell)]})$. Then the element $\kappa_{m,\ell}$ defined above does not depend on the choice of ℓ' (hence it does not depend on the choice of b') and is a weak Kolyvagin system of Gauss sum type over K.*

Proof. We prove this proposition by induction on $\epsilon(m)$. We work over $K_{[1]}$ and put $b'_{[1]} = \mathrm{Cor}_{K_{[\epsilon(m\ell)]}/K_{[1]}}(b')$ and

$$(\kappa^{(K_{[1]})}_{m,\ell})' = \kappa^{(K_{[1]})}_{m,\ell'} - \delta^{(K_{[1]})}_m b'_{[1]} - \sum_{r|m} \phi^{(K_{[1]})}_r(b'_{[1]})\kappa^{(K_{[1]})}_{\frac{m}{r},r} \in H^1(K_{[1]}, T^*/p^N). \tag{23}$$

Here, we used a map $\phi^{(K_{[1]})}_r : H^1(K_{[1]}, T^*/p^N) \longrightarrow O/p^N[\mathrm{Gal}(K_{[1]}/\mathbf{Q})]$ which is the map ϕ_r for $K_{[1]}$. Note that $\kappa^{(K_{[1]})}_{m,\ell'}$ was defined and proved to be a weak Kolyvagin system by Proposition 7.7 and Lemma 7.9, and that $\kappa^{(K_{[1]})}_{\frac{m}{r},r}$ has been already proved to be a weak Kolyvagin system and to be independent of the choice of the auxiliary prime by induction on $\epsilon(m)$ because $(K_{[1]})_{[\epsilon(m)]} = K_{[\epsilon(m\ell)]}$. Therefore, by Proposition 7.11 $(\kappa^{(K_{[1]})}_{m,\ell})'$ is a weak Kolyvagin system over $K_{[1]}$.

For r dividing m, we define $(\kappa_{\frac{m}{r},\ell}^{(K_{[1]})})'$ similarly as (23) using ℓ'. Then $(\kappa_{\frac{m}{r},\ell}^{(K_{[1]})})' = \kappa_{\frac{m}{r},\ell}^{(K_{[1]})}$ by definition, and it is independent of the choice of ℓ' by induction on $\epsilon(m)$. Therefore,

$$\partial_r^{(K_{[1]})}((\kappa_{m,\ell}^{(K_{[1]})})') = \phi_r^{(K_{[1]})}((\kappa_{\frac{m}{r},\ell}^{(K_{[1]})})') = \phi_r^{(K_{[1]})}(\kappa_{\frac{m}{r},\ell}^{(K_{[1]})})$$

does not depend on the choice of ℓ'. Since $\partial_\ell^{(K_{[1]})}((\kappa_{m,\ell}^{(K_{[1]})})') = \delta_m^{(K_{[1]})}$, we know that $\partial_{K_{[1]}}((\kappa_{m,\ell}^{(K_{[1]})})')$ does not depend on the choice of ℓ'. Therefore, $\kappa_{m,\ell} = \mathrm{Cor}_{K_{[1]}/K}((\kappa_{m,\ell}^{(K_{[1]})})')$ is a weak Kolyvagin system over K and independent of the choice of ℓ' by Lemma 7.12. □

Proposition 7.14. *We assume either (1) or (2).*

(1) Put $K' = K_{[\epsilon(m\ell)]}(m)_{[1]}K_{n_0+N}$ as above and assume that $m \in \mathcal{N}_1(K_{[\epsilon(m\ell)]})$, and that ℓ, $\ell' \in \mathcal{P}_0'(K')$.

(2) We assume that $m\ell\ell' \in \mathcal{N}_1(K_{[\epsilon(m\ell\ell')]})$.

We also assume that $r_{K_{[\epsilon(m\ell)]}}(t_{\ell',K_{[\epsilon(m\ell)]}}) = r_{K_{[\epsilon(m\ell)]}}(t_{\ell,K_{[\epsilon(m\ell)]}})$, and that $b' \in H_f^1(O_{K_{[\epsilon(m\ell)]}}[1/\ell\ell'], T^*/p^N)$ is an element such that $\partial_{K_{[\epsilon(m\ell)]}}(b') = t_{\ell',K_{[\epsilon(m\ell)]}} - t_{\ell,K_{[\epsilon(m\ell)]}}$. Put $b = \mathrm{Cor}_{K_{[\epsilon(m\ell)]}/K}(b')$.
Then we have

$$\kappa_{m,\ell} = \kappa_{m,\ell'} - \delta_m b - \sum_{r|m} \phi_r(b)\kappa_{\frac{m}{r},r}$$

as weak Kolyvagin systems over K.

Proof. First of all, we claim that $\kappa_{m,\ell}^{K_{[1]}}$, $\kappa_{m,\ell'}^{K_{[1]}}$ are weak Kolyvagin systems over $K_{[1]}$ if either (1) or (2) is satisfied. In fact, if (1) is satisfied, the claim follows from Proposition 7.7 and Lemma 7.9, and if (2) is satisfied, it follows from Proposition 7.13 and $K_{[\epsilon(m\ell\ell')]} = (K_{[1]})_{[\epsilon(m\ell)]}$. Using this claim, we prove the conclusion of Proposition 7.14. We know that $\kappa_{\frac{m}{r},r}^{K_{[1]}}$ is defined over $K_{[1]}$ and is a weak Kolyvagin system over $K_{[1]}$ by Proposition 7.13 because $K_{[\epsilon(m\ell)]} = (K_{[1]})_{[\epsilon(m)]}$. We put

$$\left(\kappa_{m,\ell}^{K_{[1]}}\right)' = \kappa_{m,\ell'}^{K_{[1]}} - \delta_m^{K_{[1]}} b'_{[1]} - \sum_{r|m} \phi_r^{K_{[1]}}(b'_{[1]})\kappa_{\frac{m}{r},r}^{K_{[1]}}$$

where $b'_{[1]} = \mathrm{Cor}_{K_{[\epsilon(m\ell)]}/K_{[1]}}(b')$. By Proposition 7.11, $\left(\kappa_{m,\ell}^{K_{[1]}}\right)'$ is a weak Kolyvagin system over $K_{[1]}$. By induction on $\epsilon(m)$, we have

$$\partial_r^{(K_{[1]})}\left(\left(\kappa_{m,\ell}^{(K_{[1]})}\right)'\right) = \phi_r^{(K_{[1]})}\left(\left(\kappa_{\frac{m}{r},\ell}^{(K_{[1]})}\right)'\right) = \phi_r^{(K_{[1]})}(\kappa_{\frac{m}{r},\ell}^{(K_{[1]})}) = \partial_r^{(K_{[1]})}(\kappa_{m,\ell}^{K_{[1]}})$$

for all r dividing m. Therefore, we have $\partial_{K_{[1]}}\left(\left(\kappa_{m,\ell}^{(K_{[1]})}\right)'\right) = \partial_{K_{[1]}}\left(\kappa_{m,\ell}^{(K_{[1]})}\right)$. This implies that

$$\mathrm{Cor}_{K_{[1]}/K}\left(\left(\kappa_{m,\ell}^{K_{[1]}}\right)'\right) = \mathrm{Cor}_{K_{[1]}/K}\left(\kappa_{m,\ell}^{(K_{[1]})}\right)$$

as weak Kolyvagin systems over K by Lemma 7.12. Computing both sides, we obtain $\kappa_{m,\ell'} - \delta_m b - \sum_{r|m} \phi_r(b)\kappa_{\frac{m}{r},r} = \kappa_{m,\ell}$. □

Suppose that $m \in \mathcal{N}_1(K)$. In [16], if m has a factorization $m = \ell_1 \cdots \ell_r$ such that $\ell_{i+1} \in \mathcal{P}_1(K(\ell_1 \cdots \ell_i))$ for all $i = 1, \ldots, r-1$, we called m *well-ordered*. In this paper, we call m *admissible* if m satisfies the above condition because the word "well-ordered" might perhaps be misunderstood. Note that we do not impose the condition $\ell_1 < \cdots < \ell_r$ in the above definition, and that m is admissible if there is one factorization as above.

The next Proposition can be regarded as a special case of Theorem A4 in Mazur and Rubin [19].

Proposition 7.15. *Suppose that m is admissible. We assume one of the following conditions:*

(i) ℓ satisfies the conditions of Proposition 7.7 (namely, we have $\ell \in \mathcal{P}_0(K(m)_{[1]}K_{n_0+N})$),
(ii) $m\ell \in \mathcal{N}_1(K_{[\epsilon(m\ell)]})$.

Then, for each $r|m$, we have $\phi_r(\kappa_{m,\ell}) = 0$.

Proof. (i) This can be proved by the same method as [16, Prop. 6.3]. The property we used there was, for any $\ell|m$

$$\mathbf{Q}_\ell^\times/(\mathbf{Q}_\ell^\times)^{p^N} = V_1 \oplus V_2$$

where V_1 (resp. V_2) is the kernel of the map $\mathbf{Q}_\ell^\times/(\mathbf{Q}_\ell^\times)^{p^N} \longrightarrow \mathbf{Z}/p^N$ induced by the normalized additive valuation of $\mathbf{Q}_\ell$ (resp. $\mathbf{Q}_\ell^\times/(\mathbf{Q}_\ell^\times)^{p^N} \longrightarrow \mathrm{Gal}(\mathbf{Q}_\ell(\mu_\ell)/\mathbf{Q}_\ell) \otimes \mathbf{Z}/p^N$ induced by the reciprocity map of local class field theory). Instead of the above decomposition, we have the decomposition

$$H^1(\mathbf{Q}_\ell, T^*/p^N) = H^1_f(\mathbf{Q}_\ell, T^*/p^N) \oplus H^1(\mathcal{G}_\ell, H^0(\mathbf{Q}_\ell(\ell), T^*/p^N))$$

in (15), so the same proof works.

(ii) Using Lemma 7.4, we can take ℓ' and b' in the definition of $\kappa_{m,\ell}$ (see (22) before Proposition 7.13) such that $\phi_r^{K_{[\epsilon(m\ell)]}}(b') = 0$ for all r dividing m. Then by Proposition 7.13 we have $\kappa_{m,\ell} = \kappa_{m,\ell'} - \delta_m b$ where $b = \mathrm{Cor}_{K_{[\epsilon(m\ell)]}/K}(b')$. Using Proposition 7.15(i), we obtain

$$\phi_r(\kappa_{m,\ell}) = \phi_r(\kappa_{m,\ell'}) - \delta_m \phi_r(b) = 0 - 0 = 0.$$

□

The next proposition can be proved by the same method as [16, Prop. 6.5].

Proposition 7.16. *Assume that $m\ell \in \mathcal{N}_1(K_{[\epsilon(m\ell)+1]})$ and $m\ell$ is admissible. Then we have $\phi_\ell(\kappa_{m,\ell}) = -\delta_{m\ell}$. (Note that we are not assuming $\ell \in \mathcal{P}_1(K(m))$.)*

Proof. We use the same method as [16, Prop. 6.5]. We take n_0 such that $\mathrm{Gal}(K_\infty/K_{n_0})$ acts trivially on T^*/p^N and that every prime of K_{n_0} dividing $m\ell$ is inert in K_∞/K_{n_0}. We put $K' = K_{[\epsilon(m\ell)+1]}(m\ell)_{[1]}K_{n_0+N}$ and take ℓ'

in $\mathcal{P}_0'(K')$. By Lemma 7.4, we can take another prime $\ell'' \in \mathcal{P}_0'(K')$ and $z' \in H^1_f(O_{K_{[\epsilon(m\ell)+1]}}[1/m\ell\ell'], T^*/p^N)$ such that

$$\partial_{K_{[\epsilon(m\ell)+1]}}(z') = t_{\ell'',K_{[\epsilon(m\ell)+1]}} - t_{\ell',K_{[\epsilon(m\ell)+1]}},$$

$\phi_\ell^{K_{[\epsilon(m\ell)+1]}}(z') = 1$, and $\phi_r^{K_{[\epsilon(m\ell)+1]}}(z') = 0$ for all r which divides m, where for each r dividing $m\ell$,

$$\phi_r^{K_{[\epsilon(m\ell)+1]}} : H^1_f(K_{[\epsilon(m\ell)+1]}, T^*/p^N) \longrightarrow O/p^N[\mathrm{Gal}(K_{[\epsilon(m\ell)+1]}/\mathbf{Q})]$$

is the map ϕ_r for $K_{[\epsilon(m\ell)+1]}$. By Proposition 7.14(1), putting $z = \mathrm{Cor}_{K_{[\epsilon(m\ell)+1]}/K}(z')$, we have

$$\begin{aligned}\kappa_{m\ell,\ell'} &= \kappa_{m\ell,\ell''} - \delta_{m\ell} z - \sum_{r|m\ell} \phi_r(z)\kappa_{\frac{m\ell}{r},r} \\ &= \kappa_{m\ell,\ell''} - \delta_{m\ell} z - \kappa_{m,\ell}.\end{aligned}$$

Since we have $\phi_\ell(\kappa_{m\ell,\ell'}) = \phi_\ell(\kappa_{m\ell,\ell''}) = 0$ by Proposition 7.15, taking ϕ_ℓ of both sides of the above equation, we obtain

$$0 = -\delta_{m\ell}\phi_\ell(z) - \phi_\ell(\kappa_{m,\ell}).$$

Therefore, we get the conclusion of Proposition 7.16 since $\phi_\ell(z) = 1$. □

8. Presentations of Selmer groups

8.1. **Freeness of some cohomology groups.** Let $\mathbf{Q}_\infty/\mathbf{Q}$ be the cyclotomic $\mathbf{Z}_p$-extension, and $\Lambda = O[[\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})]]$. We now have $H^1_f(O_{\mathbf{Q}_\infty}, A) = H^1_{\mathrm{Gr}}(O_{\mathbf{Q}_\infty}, A)$ by Lemma 5.2 under our assumptions. We put

$$X = \mathrm{Sel}(\mathbf{Q}_\infty, A)^\vee = H^1_{\mathrm{Gr}}(O_{\mathbf{Q}_\infty}, A)^\vee = H^1_f(O_{\mathbf{Q}_\infty}, A)^\vee.$$

By Proposition 2.10, X has no nontrivial finite Λ-submodule, namely (II-2) holds. We also have $H^1_{\mathrm{Gr}}(O_{\mathbf{Q}_\infty}, A^*) = H^1_f(O_{\mathbf{Q}_\infty}, A^*)$ by Lemma 5.2. Put

$$X^* = H^1_f(O_{\mathbf{Q}_\infty}, A^*)^\vee.$$

By our assumption (II-1) and Greenberg [6, Thm. 2], X^* is a finitely generated torsion Λ-module. Proposition 2.10 also implies that X^* has no nontrivial finite Λ-submodule, namely (II-2)* holds. Therefore, if λ is the λ-invariant of X, both X and X^* are free O-modules of rank λ (Greenberg [6, Thm. 2]) because we assumed that the μ-invariant of X is zero.

Suppose that $x_1, \ldots, x_a$ are generators of X as a Λ-module. We consider a surjective homomorphism $g : \Lambda^a \longrightarrow X$ such that $e_i \mapsto x_i$ where $(e_i)_{1\le i\le a}$ is the standard basis of Λ^a. Since X has no finite torsion Λ-submodule, X is of projective dimension at most 1 (see for example, Wingberg [36, Prop. 2.1]),so the kernel of $g : \Lambda^a \longrightarrow X$ is a free Λ-module of rank a. We fix some isomorphism $\mathrm{Ker}(g) \simeq \Lambda^a$, and actually treat it as an equality. Then we have an exact sequence

$$0 \longrightarrow \Lambda^a \xrightarrow{f} \Lambda^a \xrightarrow{g} X \longrightarrow 0 \tag{24}$$

where we denoted by f the Λ-homomorphism $\mathrm{Ker}(g) = \Lambda^a \longrightarrow \Lambda^a$. Since X is a free O-module, the above exact sequence yields an exact sequence

$$0 \longrightarrow (\Lambda/p^N)^a \longrightarrow (\Lambda/p^N)^a \longrightarrow X/p^N \longrightarrow 0 \tag{25}$$

for any positive integer N. By our assumption (I), $H^1_f(O_{\mathbf{Q}_\infty}, T/p^N)$ coincides with the kernel of the multiplication by p^N on $H^1_f(O_{\mathbf{Q}_\infty}, A)$. Therefore, $H^1_f(O_{\mathbf{Q}_\infty}, T/p^N)^\vee$ coincides with X/p^N. Note that this group is finite.

Let K_n be the n-th layer of $\mathbf{Q}_\infty/\mathbf{Q}$, $\Gamma_n = \mathrm{Gal}(\mathbf{Q}_\infty/K_n)$ and $R_n = O[\mathrm{Gal}(K_n/\mathbf{Q})]$. We take n sufficiently large such that $H^1_f(O_{K_n}, T/p^N) = H^1_f(O_{K_\infty}, T/p^N)$ and $H^1_f(O_{K_n}, T^*/p^N) = H^1_f(O_{K_\infty}, T^*/p^N)$. We have

$$(X/p^N)_{\Gamma_n} = X/p^N = H^1_f(O_{K_n}, T/p^N)^\vee.$$

Therefore, the above exact sequence yields an exact sequence

$$0 \longrightarrow (X/p^N)^{\Gamma_n} \longrightarrow (R_n/p^N)^a \xrightarrow{f_n} (R_n/p^N)^a \xrightarrow{g_n} H^1_f(O_{K_n}, T/p^N)^\vee \longrightarrow 0$$

where f_n, g_n are induced by f, g.

For $n' > n$, consider the commutative diagram of exact sequences

(26)

$$\begin{array}{ccccccccc}
0 & \to & (X/p^N)^{\Gamma_n} & \longrightarrow & (R_n/p^N)^a & \xrightarrow{f_n} & (R_n/p^N)^a & \xrightarrow{g_n} & H^1_f(O_{K_n}, T/p^N)^\vee \to 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \uparrow \\
0 & \to & (X/p^N)^{\Gamma_{n'}} & \longrightarrow & (R_{n'}/p^N)^a & \xrightarrow{f_{n'}} & (R_{n'}/p^N)^a & \xrightarrow{g_{n'}} & H^1_f(O_{K_{n'}}, T/p^N)^\vee \to 0.
\end{array}$$

The leftmost vertical arrow is induced by the norm map of $\mathrm{Gal}(K_{n'}/K_n)$. Therefore, we can take n' sufficiently large such that $(X/p^N)^{\Gamma_{n'}} \longrightarrow (X/p^N)^{\Gamma_n}$ is the zero map. In the following, we fix such n and n'.

For each prime $\ell \in \mathcal{P}_1(K_{n'})$, we take $t \in H^0(\mathbf{F}_\ell, T^*/p^N(-1))$, which generates a free O/p^N-module of rank 1, and define $t_{\ell,K_{n'}} \in \mathcal{H}^2_\ell(K_{n'})$ as in Subsection 6.10. We consider the homomorphism

$$r_\ell : \mathcal{H}^2_\ell(K_{n'}) \longrightarrow H^1_f(O_{K_{n'}}, T/p^N)^\vee$$

which was defined in (13). Since $H^1(O_{K_{n'}}[1/(P_{\mathrm{bad}} \cup \{p\})], T/p^N)^\vee \longrightarrow H^1_f(O_{K_{n'}}, T/p^N)^\vee$ is surjective, by Proposition 5.16, there exist infinitely many $\ell_i \in \mathcal{P}_1(K_{n'})$ such that $r_{\ell_i}(t_{\ell_i,K_{n'}}) = x_i \bmod (p^N, \Gamma_{n'}) \in H^1_f(O_{K_{n'}}, T/p^N)^\vee$. We define

$$Q_i = \{\ell_i \in \mathcal{P}_1(K_{n'}) \mid r_{\ell_i}(t_{\ell_i,K_{n'}}) = x_i \bmod (p^N, \Gamma_{n'})\} \text{ and } Q = \bigcup_{1 \le i \le a} Q_i. \tag{27}$$

By definition, the sets Q_i are pairwise disjoint. Recall that $\mathcal{H}^2_{\ell_i}(K_{n'})$ is a free $R_{n'}/p^N$-module of rank 1 generated by $t_{\ell_i,K_{n'}}$ for any $\ell_i \in Q_i$ (see Lemma 5.10). Let S be a finite subset of Q such that $S \cap Q_i$ is not empty for

any i. We define an $R_{n'}$-homomorphism

$$\alpha : \bigoplus_{\ell \in S} \mathcal{H}^2_\ell(K_{n'}) \longrightarrow (R_{n'}/p^N)^a$$

by $t_{\ell, K_{n'}} \mapsto e_i$ if $\ell \in Q_i$ where $(e_i)_{1 \le i \le a}$ is the standard basis of $(R_{n'}/p^N)^a$. By our assumption, α is surjective. Consider the commutative diagram of exact sequences

$$\begin{array}{ccccccccc} H^1_f(O_{K_{n'}}[1/S], T^*/p^N) & \longrightarrow & \displaystyle\bigoplus_{\ell \in S} \mathcal{H}^2_\ell(K_{n'}) & \longrightarrow & H^1_f(O_{K_{n'}}, T/p^N)^\vee & \longrightarrow & 0 \\ \downarrow{\scriptstyle \alpha'} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle id} & & \\ 0 \longrightarrow \mathrm{Image}\, f_{n'} & \longrightarrow & (R_{n'}/p^N)^a & \longrightarrow & H^1_f(O_{K_{n'}}, T/p^N)^\vee & \longrightarrow & 0 \end{array}$$

where the upper horizontal sequence is the exact sequence in Corollary 5.6, id is the identity map, and α' is induced by α. By this commutative diagram, for $x \in H^1_f(O_{K_{n'}}[1/S], T^*/p^N)$, there is $y \in (R_{n'}/p^N)^a$ such that $\alpha'(x) = f_{n'}(y)$. Let $y' \in (R_n/p^N)^a$ be the natural projection of y in $(R_n/p^N)^a$. Since the leftmost map is the zero map in the commutative diagram (26), y' does not depend on the choice of y. We define a homomorphism

$$\beta' : H^1_f(O_{K_{n'}}[1/S], T^*/p^N) \longrightarrow (R_n/p^N)^a$$

by $\beta'(x) = y'$.

Since α is surjective, $\alpha' : H^1_f(O_{K_{n'}}[1/S], T^*/p^N) \longrightarrow \mathrm{Image}\, f_{n'}$ is also surjective. Therefore, we know that $\beta' : H^1_f(O_{K_{n'}}[1/S], T^*/p^N) \longrightarrow (R_n/p^N)^a$ is also surjective from the definition.

Proposition 8.2.

(i) The above β' induces a surjective homomorphism

$$\beta : H^1_f(O_{K_n}[1/S], T^*/p^N) \longrightarrow (R_n/p^N)^a$$

such that $\beta' = \beta \circ \mathrm{Cor}$ where

$$\mathrm{Cor} : H^1_f(O_{K_{n'}}[1/S], T^*/p^N) \longrightarrow H^1_f(O_{K_n}[1/S], T^*/p^N)$$

is the corestriction homomorphism.

(ii) $H^1_f(O_{K_n}[1/S], T^*/p^N)$ is a free R_n/p^N-module of rank $\#S$.

Proof. Consider the exact sequence

$$\begin{aligned} (28) \quad 0 \longrightarrow H^1_f(O_{K_{n'}}, T^*/p^N) \longrightarrow H^1_f(O_{K_{n'}}[1/S], T^*/p^N) \longrightarrow \bigoplus_{\ell \in S} \mathcal{H}^2_\ell(K_{n'}) \\ \longrightarrow H^1_f(O_{K_{n'}}, T/p^N)^\vee \longrightarrow 0, \end{aligned}$$

which is obtained from Corollary 5.6. Put $\mathrm{Ker}_{n'} = \mathrm{Ker}(\bigoplus_{\ell \in S} \mathcal{H}^2_\ell(K_{n'}) \longrightarrow H^1_f(O_{K_{n'}}, T/p^N)^\vee)$ and $G = \mathrm{Gal}(K_{n'}/K_n)$. Since $\mathcal{H}^2_\ell(K_{n'})$ is a free $R_{n'}/p^N$-module, we have $\mathcal{H}^2_\ell(K_{n'})^G = N_G \mathcal{H}^2_\ell(K_{n'})$. The fact that N_G is zero on

$H^1_f(O_{K_{n'}}, T/p^N)^\vee = X/p^N$ implies that $(\mathrm{Ker}_{n'})^G = \bigoplus_{\ell\in S} \mathcal{H}^2_\ell(K_{n'})^G$. Therefore, putting $s = \#S$, we get $\#(\mathrm{Ker}_{n'})^G = \#(R_n/p^N)^s$.

Let λ be the λ-invariant of X. As we mentioned above, both X and X^* are free O-modules of rank λ, so we know $X/p^N \simeq X^*/p^N \simeq (O/p^N)^\lambda$. Since n, n' are taken such that $H^1_f(O_{K_\infty}, T^*/p^N) = H^1_f(O_{K_{n'}}, T^*/p^N) = H^1_f(O_{K_n}, T^*/p^N)$, we have $H^1_f(O_{K_{n'}}, T^*/p^N)^G = H^1_f(O_{K_n}, T^*/p^N)$. By Corollary 6.4, we also have

$$H^1_f(O_{K_{n'}}[1/S], T^*/p^N)^G = H^1_f(O_{K_n}[1/S], T^*/p^N).$$

Therefore, using the exact sequence

$$0 \longrightarrow H^1_f(O_{K_{n'}}, T^*/p^N) \longrightarrow H^1_f(O_{K_{n'}}[1/S], T^*/p^N) \longrightarrow \mathrm{Ker}_{n'} \longrightarrow 0$$

and the same exact sequence for n, we have an exact sequence

$$0 \longrightarrow \mathrm{Ker}_n \longrightarrow (\mathrm{Ker}_{n'})^G \longrightarrow H^1_f(O_{K_{n'}}, T^*/p^N)_G \longrightarrow H^1_f(O_{K_{n'}}[1/S], T^*/p^N)_G \longrightarrow \dots.$$

Since $\#(\mathrm{Ker}_{n'})^G = \#(R_n/p^N)^s$, from the exact sequence

$$0 \longrightarrow \mathrm{Ker}_n \longrightarrow \bigoplus_{\ell\in S} \mathcal{H}^2_\ell(K_n) \longrightarrow H^1_f(O_{K_n}, T/p^N)^\vee \longrightarrow 0\ ,$$

we know that

$$\#\,\mathrm{Image}((\mathrm{Ker}_{n'})^G \longrightarrow H^1_f(O_{K_{n'}}, T^*/p^N)_G) = \#H^1_f(O_{K_n}, T/p^N)^\vee = \#(O/p^N)^\lambda.$$

But $\#H^1_f(O_{K_{n'}}, T^*/p^N)_G = \#H^1_f(O_{K_{n'}}, T^*/p^N) = \#X^*/p^N = \#(O/p^N)^\lambda$, so $(\mathrm{Ker}_{n'})^G \longrightarrow H^1_f(O_{K_{n'}}, T^*/p^N)_G$ is surjective and

$$H^1_f(O_{K_{n'}}[1/S], T^*/p^N)_G \xrightarrow{\simeq} (\mathrm{Ker}_{n'})_G$$

is bijective.

We identify $\bigoplus_{\ell\in S} \mathcal{H}^2_\ell(K_{n'})$ with $(R_{n'}/p^N)^s$, then we can take a surjective Λ-homomorphism $f' : \Lambda^s \longrightarrow X$ such that $f' \bmod (p^N, \Gamma_{n'})$ is $\bigoplus_{\ell\in S} \mathcal{H}^2_\ell(K_{n'}) \longrightarrow H^1_f(O_{K_{n'}}, T/p^N)^\vee$. Since X contains no nontrivial finite Λ-submodule, the projective dimension of X as a Λ-module is at most 1, so the kernel of $f' : \Lambda^s \longrightarrow X$ is a free Λ-module of rank s. Namely, we have an exact sequence $0 \longrightarrow \Lambda^s \longrightarrow \Lambda^s \xrightarrow{f'} X \longrightarrow 0$, which yields an exact sequence

$$(R_{n'}/p^N)^s \longrightarrow \bigoplus_{\ell\in S} \mathcal{H}^2_\ell(K_{n'}) \longrightarrow H^1_f(O_{K_{n'}}, T/p^N)^\vee \longrightarrow 0.$$

Therefore, we have a surjective homomorphism $(R_{n'}/p^N)^s \longrightarrow \mathrm{Ker}_{n'}$, which implies that $\mathrm{Ker}_{n'}$ is generated by s elements. Since $H^1_f(O_{K_{n'}}[1/S], T^*/p^N)_G \longrightarrow (\mathrm{Ker}_{n'})_G$ is bijective, $H^1_f(O_{K_{n'}}[1/S], T^*/p^N)$ is

also generated by s elements as an $R_{n'}/p^N$-module. From the exact sequence (28) and $\#H^1_f(O_{K_{n'}}, T^*/p^N) = \#H^1_f(O_{K_n}, T/p^N)^\vee = \#(O/p^N)^\lambda$, we know

$$\#H^1_f(O_{K_{n'}}[1/S], T^*/p^N) = \#\bigoplus_{\ell\in S}\mathcal{H}^2_\ell(K_{n'}) = \#(R_{n'}/p^N)^s.$$

This implies that $H^1_f(O_{K_{n'}}[1/S], T^*/p^N)$ is a free $R_{n'}/p^N$-module of rank s.

In particular, it is a free $O/p^N[G]$-module, so we have $H^i(G, H^1_f(O_{K_{n'}}[1/S], T^*/p^N)) = 0$ for any $i \geq 1$. Since we have $H^1_f(O_{K_{n'}}[1/S], T^*/p^N)^G = H^1_f(O_{K_n}[1/S], T^*/p^N)$ by Corollary 6.4, the corestriction map induces an isomorphism

$$H^1_f(O_{K_{n'}}[1/S], T^*/p^N)_G \xrightarrow{\simeq} H^1_f(O_{K_n}[1/S], T^*/p^N).$$

Since $H^1_f(O_{K_{n'}}[1/S], T^*/p^N)$ is a free $R_{n'}/p^N$-module of rank s, the above isomorphism implies Proposition 8.2(ii). Since β factors through $H^1_f(O_{K_{n'}}[1/S], T^*/p^N)_G$, the above isomorphism also implies Proposition 8.2 (i). □

Let Q be as in (27). Enlarging $S \subset Q$ and taking the direct limit, we obtain a surjective homomorphism

$$\beta : H^1_f(O_{K_n}[1/Q], T^*/p^N) \longrightarrow (R_n/p^N)^a$$

for which we again use the same letter β. For any j such that $1 \leq j \leq a$, we define $\beta_j : H^1_f(O_{K_n}[1/Q], T^*/p^N) \longrightarrow R_n/p^N$ to be the composition of β and the j-th projection.

9. Main Theorem A

9.1. **An extra assumption about non self-duality.** In this section, we make an extra assumption (C) below. In Section 9 we take and fix a basis $e_1, \ldots, e_d$ of T as in Subsection 5.8. Let $\omega : G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathbf{Z}_p^\times$ be the Teichmüller character, and $\rho : G_{\mathbf{Q}} \longrightarrow \mathrm{Aut}(T) \simeq \mathrm{GL}_d(O)$ the representation attached to T.

(C) There are $s \in G_{\mathbf{Q}}$ and $a \in O$ such that $a^r = 1$ for some integer $r > 1$, $\rho(s) = aI$, and $a^2 \neq \omega(s)$.

We use the same notation as in Subsections 5.8 and 5.11. For $K \in \mathcal{K}_{(p)}$, L/K is the Galois extension such that $\rho|_{G_{K,p^N}}$ induces an injective homomorphism from $\mathrm{Gal}(L/K)$ to $\mathrm{GL}_d(O/p^N)$. Let Δ be the subgroup of $\mathrm{Gal}(L/K)$ as in Subsection 5.8, and H the subgroup of $\mathrm{Gal}(L/K)$ defined in Subsection 5.8. We define $\mathcal{T}$ by $\mathcal{T} = (T/p^N)_H$ as in Subsection 5.8. We denote by $\mathcal{T}'$ the O-submodule of T/p^N generated by e_1. Both $\mathcal{T}'$ and $\mathcal{T}$ are isomorphic to O/p^N as O-modules. If $\rho|_{G_{K,p^N}}(s) = aI$, it follows from the definition of Δ that s acts on both $\mathcal{T}'$ and $\mathcal{T}$ by $s(x) = ax$.

In the following, we assume $\mathbf{Q}_{N-1} \subset K$. Then $L(\mu_{p^N}) = L(\mu_p)$. Let L^Δ be the subfield of L such that $\mathrm{Gal}(L/L^\Delta) = \Delta$. Put $\Delta' = \mathrm{Gal}(L(\mu_p)/L^\Delta)$. Then Δ' acts on $(\mathcal{T}')^* = (\mathcal{T}')^\vee(1)$ where (1) is the Tate twist. Note that Δ' is of order prime to p. Consider the following condition.

(C)′ $\mathcal{T}$ is not isomorphic to $(\mathcal{T}')^* = (\mathcal{T}')^\vee(1)$ as a Δ'-module.

We define a character $\chi : \Delta' \longrightarrow \Delta \longrightarrow O^\times$ by $\chi(s) = a$ where $\rho(s) = aI$ for $s \in \Delta$. We denote by χ^* the action of Δ' on $(\mathcal{T}')^* = (\mathcal{T}')^\vee(1)$. So $\chi^* = \chi^{-1}\omega$ where ω is the action of Δ' on μ_p. The condition (C)′ is equivalent to $\chi \neq \chi^*$. Therefore, it is easy to check that the condition (C)′ (for each N) is equivalent to the condition (C).

If $d = 1$, then $L/\mathbf{Q}$ is an abelian extension, and χ, χ^*, ω are Dirichlet characters. Since ω is odd, there is no χ such that $\chi^2 = \omega$, so the condition (C)′ always holds true in the case $d = 1$.

On the other hand, if E is an elliptic curve over $\mathbf{Q}$ and T is the Tate module of E, we know that $(T/p^N)^* = (T/p^N)^\vee(1)$ is canonically isomorphic to T/p^N as a $G_{\mathbf{Q}}$-module by the Weil pairing. We also note that $\mu_p \subset L$, so $\Delta' = \Delta$. By this isomorphism, $(\mathcal{T}')^* = (\mathcal{T}')^\vee(1)$ corresponds to $\mathcal{T}$, so $\mathcal{T}$ and $(\mathcal{T}')^*$ are isomorphic as Δ-modules. This means that (C)′ never holds, and neither does (C).

Let L' be the subfield of L such that $\mathrm{Gal}(L/L') = H$. In Subsection 5.11, for a finite set S' containing $P_{\mathrm{bad}} \cup \{p\}$ we defined a surjective homomorphism

$$\eta^\vee : \mathrm{Gal}(M'/L') \otimes \mathcal{T}^\vee \longrightarrow H^1(O_K[1/S'], T/p^N)^\vee.$$

Let $\chi : \Delta \longrightarrow O^\times$ be the character corresponding to the action on $\mathcal{T}$. For any $\mathbf{Z}_p[\Delta]$-module $\mathfrak{A}$, we denote by $\mathfrak{A}^\chi$ the χ-component of $\mathfrak{A}$, namely $\mathfrak{A}^\chi = \mathfrak{A} \otimes_{\mathbf{Z}_p[\Delta]} O(\chi)$ where $O(\chi)$ is the $\mathbf{Z}_p[\Delta]$-module such that $O(\chi) = O$ as an O-module and Δ acts on $O(\chi)$ via χ. Since Δ is commutative with H, $H \times \Delta$ is a subgroup of $\mathrm{Gal}(L/K)$. Let L'' be the subfield of L such that $\mathrm{Gal}(L/L'') = H \times \Delta$ and $\mathrm{Gal}(L'/L'') = \Delta$. Since the above map $\eta^\vee$ factors through $H^1(O_{L''}[1/S'], T/p^N)^\vee$ on which Δ acts trivially, $\eta^\vee$ induces

$$\eta^\vee : \mathrm{Gal}(M'/L')^\chi \otimes_O \mathcal{T}^\vee \longrightarrow H^1(O_K[1/S'], T/p^N)^\vee, \tag{29}$$

which we also denote by $\eta^\vee$.

We also apply the above argument to $H^1(O_K[1/S'], T^*/p^N)$. Let $\mathfrak{M}$ be the maximal unramified abelian extension of $L'(\mu_p)$ outside S' such that $p^N \,\mathrm{Gal}(\mathfrak{M}/L'(\mu_p)) = 0$. As in Subsection 5.11, we can see that there is a subfield $\mathfrak{M}' \subset \mathfrak{M}$ such that $\mathrm{Gal}(\mathfrak{M}/L'(\mu_p)) = \mathrm{Gal}(\mathfrak{M}'/L'(\mu_p)) \times \mathrm{Gal}(L'_{(N)}(\mu_p)/L'(\mu_p))$. Let χ^* be the character corresponding to the action of Δ' on $(\mathcal{T}')^*$. By the same method as above, we have a surjective homomorphism

$$(\eta^*)^\vee : \mathrm{Gal}(\mathfrak{M}'/L'(\mu_p))^{\chi^*} \otimes_O \mathcal{T}'(-1) \longrightarrow H^1(O_K[1/S'], T^*/p^N)^\vee. \tag{30}$$

Note that since $[L'(\mu_p) : L]$ is prime to p, we have $\mathrm{Gal}(\mathfrak{M}'/L'(\mu_p))^\chi = \mathrm{Gal}(M'/L')^\chi$.

Let $\mathcal{P}_{1,\sigma}$ be the set of primes defined in Subsection 5.8. For any $\ell \in \mathcal{P}_{1,\sigma}$, we take $t = e_d^\vee$ as in Subsection 5.8. For $\ell \in \mathcal{P}_{1,\sigma}(K)$, we define $t_{\ell,K} \in \mathcal{H}^2_\ell(K)$ using this t in this section. Suppose that $\ell \in \mathcal{P}_{1,\sigma}(L'(\mu_p))$ and $\ell \notin S'$. We

consider $\phi_\ell : H^1(K, T^*/p^N) \longrightarrow O/p^N[\mathrm{Gal}(K/\mathbf{Q})]$, which we defined in (17) by using $t_{\ell,K}$. Note that there is a canonical isomorphism

$$\mathrm{Hom}_{O[\mathrm{Gal}(K/\mathbf{Q})]}(\mathfrak{A}, O/p^N[\mathrm{Gal}(K/\mathbf{Q})]) \xrightarrow{\simeq} \mathrm{Hom}_O(\mathfrak{A}, O/p^N) \tag{31}$$

for any $O/p^N[\mathrm{Gal}(K/\mathbf{Q})]$-module $\mathfrak{A}$ (that is, a map $f \in \mathrm{Hom}_{O[\mathrm{Gal}(K/\mathbf{Q})]}(\mathfrak{A}, O/p^N[\mathrm{Gal}(K/\mathbf{Q})])$ such that $f(x) = \sum_{\sigma\in\mathrm{Gal}(K/\mathbf{Q})} f_\sigma(x)\sigma$ corresponds to $x \mapsto f_1(x)$). We denote by

$$\overline{\phi}_\ell : H^1(K, T^*/p^N) \longrightarrow O/p^N$$

the corresponding homomorphism to ϕ_ℓ by the above isomorphism. Explicitly, $\overline{\phi}_\ell$ is the composition of $H^1(K, T^*/p^N) \longrightarrow H^1(K_{\ell_K}, T^*/p^N)$ with $\phi_{K_{\ell_K}} : H^1(K_{\ell_K}, T^*/p^N) \longrightarrow O/p^N$, which was defined in (16).

We denote by $\zeta_{p^N}^{\otimes(-1)}$ a generator of $\mathbf{Z}/p^N(-1) = \mathrm{Hom}(\mu_{p^N}, \mathbf{Z}/p^N)$, which is defined by $\zeta_{p^N} \mapsto 1$. We regard $e_1 \otimes \zeta_{p^N}^{\otimes(-1)}$ as a generator of $\mathcal{T}'(-1)$.

Lemma 9.2. *We denote by* $\mathrm{Frob}_\ell \in \mathrm{Gal}(\mathfrak{M}'/L'(\mu_p))$ *the Frobenius substitution of* $\ell_{L'(\mu_p)}$ *in* $\mathrm{Gal}(\mathfrak{M}'/L'(\mu_p))$. *Then* $(\eta^*)^\vee(\mathrm{Frob}_\ell \otimes e_1 \otimes \zeta_{p^N}^{\otimes(-1)})$ *coincides with* (-1) *times the restriction of* $\overline{\phi}_\ell$ *to* $H^1(O_K[1/S'], T^*/p^N)$.

Proof. Let $e_1^\vee, \dots, e_d^\vee$ be the dual basis of $(T/p^N)^\vee$, and $e_1^* = e_1^\vee \otimes \zeta_{p^N}, \dots, e_d^* = e_d^\vee \otimes \zeta_{p^N} \in T^*/p^N$, which were defined in Lemma 7.2. Note that $(\mathcal{T}')^*$ is generated by e_1^* as an O/p^N-module.

By definition, $(\eta^*)^\vee(\mathrm{Frob}_\ell \otimes e_1 \otimes \zeta_{p^N}^{\otimes(-1)})$ is the composition

$$\begin{aligned} H^1(O_K[1/S'], T^*/p^N) & \\ \longrightarrow H^1(O_{L'(\mu_p)}[1/S'], T^*/p^N) &\longrightarrow H^1(\kappa(\ell_{L'(\mu_p)}), T^*/p^N) \\ \xrightarrow{\simeq} H^1(\kappa(\ell_{L'(\mu_p)}), \mathcal{T}'^*) &= \mathrm{Hom}_{\mathrm{cont}}(G_{\kappa(\ell_{L'(\mu_p)})}, (\mathcal{T}')^*) \\ \xrightarrow{a} (\mathcal{T}')^* &\xrightarrow{b} O/p^N \end{aligned}$$

where the first three arrows are natural maps, a is defined by $f \mapsto f(\mathrm{Frob}_{\ell_{L'(\mu_p)}})$, and b is induced by $e_1^* \mapsto 1$. By Lemma 7.2 (2), the above composition coincides with (-1) times the restriction of $\overline{\phi}_\ell$ to $H^1(O_K[1/S'], T^*/p^N)$.

□

We will prove a modified version of Lemma 7.4, which is an analog of Rubin [26, Thm. 3.1].

Proposition 9.3. *Let* K, K', K'' *be fields in* $\mathcal{K}_{(p)}$ *(*$\mathcal{K}_{(p)}$ *was defined in (10)) such that* $K \subset K' \subset K''$. *Suppose that* $\ell_1, \dots, \ell_s$ *are* s *distinct primes in* $\mathcal{P}_1(K')$. *Suppose that we are given* $\ell \in \mathcal{P}_0(K')$, $\sigma_i \in O/p^N[\mathrm{Gal}(K'/\mathbf{Q})]$ *for each* $i = 1, \dots, s$, *and an* $O/p^N[\mathrm{Gal}(K/\mathbf{Q})]$*-homomorphism*

$$\lambda : W \longrightarrow O/p^N[\mathrm{Gal}(K/\mathbf{Q})]$$

where W is an $O/p^N[\mathrm{Gal}(K/\mathbf{Q})]$-submodule of $H^1_f(O_K[1/S], T^*/p^N)$ for some finite set S of primes. Then there are infinitely many $\ell' \in \mathcal{P}_{1,\sigma}(K'')$ which satisfy the following properties.

(i) $r_{K'}(t_{\ell',K'}) = r_{K'}(t_{\ell,K'})$.

(ii) There is an element $z \in H^1_f(O_{K'}[1/\ell\ell'], T^*/p^N)$ *such that* $\partial_{K'}(z) = t_{\ell',K'} - t_{\ell,K'}$ *and* $\phi^{K'}_{\ell_i}(z) = \sigma_i$ *for each* $i = 1, \dots, s$.

(iii) ℓ' *is not in* S *and the restriction of*

$$\phi^K_{\ell'} : H^1(K, T^*/p^N) \longrightarrow O/p^N[\mathrm{Gal}(K/\mathbf{Q})]$$

to W *is* λ.

Proof. First of all, we may assume $K' = K$. In fact, suppose that this proposition holds in the case $K' = K$. In the general case, let $\nu_{K'/K} : O/p^N[\mathrm{Gal}(K/\mathbf{Q})] \longrightarrow O/p^N[\mathrm{Gal}(K'/\mathbf{Q})]$ be the norm (corestriction) map, and $i_{K'/K} : H^1_f(O_K[1/S], T^*/p^N) \longrightarrow H^1_f(O_{K'}[1/S], T^*/p^N)$ the natural injective homomorphism. We consider $\nu_{K'/K} \circ \lambda : W \longrightarrow O/p^N[\mathrm{Gal}(K'/\mathbf{Q})]$ and apply this proposition. Then there are infinitely many $\ell' \in \mathcal{P}_{1,\sigma}(K'')$ ($\ell' \notin S$) such that the restriction of $\phi^{K'}_{\ell'}$ to $i_{K'/K}(W)$ is $\nu_{K'/K} \circ \lambda$. Since ℓ' splits completely in K', it is easy to check that $\phi^{K'}_{\ell'} \circ i_{K'/K} = \nu_{K'/K} \circ \phi^K_{\ell'}$. Therefore, the restriction of $\phi^K_{\ell'}$ to W is λ, so the general case follows.

In the following, we assume $K' = K$. We apply the argument and the notation before Proposition 9.3. Suppose that $\lambda(x) = \sum_{\sigma \in \mathrm{Gal}(K/\mathbf{Q})} a_\sigma(x)\sigma$. We define $\overline{\lambda} : W \longrightarrow O/p^N$ by $x \mapsto a_1(x)$. We put $S' = S \cup P_{\mathrm{bad}} \cup \{p\}$ and consider a surjective homomorphism $H^1(O_K[1/S'], T^*/p^N)^\vee \longrightarrow W^\vee$. We take an element $\overline{\lambda}' \in H^1(O_K[1/S'], T^*/p^N)^\vee$ whose restriction to W is $\overline{\lambda}$.

Let $\mathfrak{M}'(\chi)$ (resp. $\mathfrak{M}'(\chi^*)$) be the subfield of $\mathfrak{M}'$ such that $\mathrm{Gal}(\mathfrak{M}'(\chi)/L'(\mu_p)) = \mathrm{Gal}(\mathfrak{M}'/L'(\mu_p))^\chi$ (resp. $\mathrm{Gal}(\mathfrak{M}'(\chi^*)/L'(\mu_p)) = \mathrm{Gal}(\mathfrak{M}'/L'(\mu_p))^{\chi^*}$). *By our assumption (C), we have*

$$\mathfrak{M}'(\chi) \cap \mathfrak{M}'(\chi^*) = L'(\mu_p).$$

We use the same notation as in the proof of Lemma 7.4. Let $y \in H^1_f(O_K[1/m], T/p^N)^\vee$ be the element constructed from σ_i and $t_{\ell,K}$ in the proof of Lemma 7.4. We consider the surjective homomorphisms $\eta^\vee$, $(\eta^*)^\vee$ in (29), (30). By the Chebotarev density theorem, we can take $\ell' \in \mathcal{P}_{1,\sigma}(K'')$ such that the Frobenius $\mathrm{Frob}_{\ell'_{L'(\mu_p)}}(\chi) \in \mathrm{Gal}(\mathfrak{M}'(\chi)/L'(\mu_p))$ satisfies $\eta^\vee(\mathrm{Frob}_{\ell'_{L'(\mu_p)}}(\chi) \otimes t) = y$ and that the Frobenius $\mathrm{Frob}_{\ell'_{L'(\mu_p)}}(\chi^*) \in \mathrm{Gal}(\mathfrak{M}'(\chi^*)/L'(\mu_p))$ satisfies $(\eta^*)^\vee(\mathrm{Frob}_{\ell'_{L'(\mu_p)}}(\chi^*) \otimes e_1 \otimes \zeta_{p^N}^{\otimes(-1)}) = -\overline{\lambda}'$. By Lemma 9.2, this implies that the restriction of $\overline{\phi}_{\ell'}$ to W coincides with $\overline{\lambda}$. It follows from the isomorphism (31) that the restriction of $\phi_{\ell'}$ to W coincides with λ. Properties (i) and (ii) were proved in Lemma 7.4.

□

9.4. **The elements $x_{m,\ell}$.** As in [16, Sec. 7], we will introduce a system $x_{m,\ell}$ of elements in $H^1_f(O_{K_n}[1/Q], T^*/p^N)$, which plays the most important role for the proof of Theorem A. The element $x_{m,\ell}$ is defined in (32), and the key property of $x_{m,\ell}$ is Lemma 9.5.

We use the same notation as in Section 8. In particular, K_n is the n-th layer of $\mathbf{Q}_\infty/\mathbf{Q}$. For each j such that $1 \le j \le a$, we take a prime $\ell_j \in Q_j$ such that $\ell_j \in \mathcal{P}_1((K_{n'})_{[a+1]})$. By definition, $r_{\ell_j}(t_{\ell_j,K_{n'}}) = x_j \bmod (p^N, \Gamma_{n'})$. We put $\mathfrak{L} = \Pi_{j=1}^a \ell_j$.

Let $\mathcal{A} \in M_a(\Lambda)$ be the matrix corresponding to the Λ-homomorphism f in (24). We take $\mathcal{A}$ such that $\det \mathcal{A} = \theta_{K_\infty}$. We consider the square matrix $\mathcal{A}_i$ which is the matrix obtained from $\mathcal{A}$ by eliminating the c_1-th row, ..., the c_i-th row and the d_1-th column, ..., the d_i-th column. Our goal is to prove $\det \mathcal{A}_i \in \Theta_i$. We may assume that $\det \mathcal{A}_j \ne 0$ for any j such that $0 \le j \le i$ (see [16, Sec. 10.2]). In the case $i = 1$, we put $m_1 = 1$ and $\ell = \ell_{c_1}$. Suppose $i \ge 2$. Recall that β_j is the composition of the map β with the j-th projection, defined at the end of Section 8. For any j such that $2 \le j \le i$, we define a prime r_j by induction on j. Suppose that $r_2, \dots, r_{j-1}$ were defined. Put $m_{j-1} = r_2 \cdots r_{j-1}$. We consider

$$\beta_{d_{j-1}} : H^1_f(O_{K_n}[1/\mathfrak{L}m_{j-1}], T^*/p^N) \longrightarrow R_n/p^N.$$

Applying Lemma 9.3, by induction on j, we can take a prime $r_j \in \mathcal{P}_{1,\sigma}((K_{n'})_{[a+1]}(\mathfrak{L}m_{j-1}))$ such that

(9.2-I) $r_j \in Q_{c_j}$ and $r_j \ne \ell_{c_j}$,

(9.2-II) there is $b'_{r_j} \in H^1_f(O_{K_{n'}}[1/r_j\ell_{c_j}], T^*/p^N)$ such that $\partial(b'_{r_j}) = t_{r_j,K_{n'}} - t_{\ell_{c_j},K_{n'}}$, $\phi_{r_s}(b'_{r_j}) = 0$ holds for any s such that $2 \le s < j$, and

(9.2-III) $\beta_{d_{j-1}}(x) = \phi_{r_j}(x)$ for all $x \in H^1_f(O_{K_n}[1/\mathfrak{L}m_{j-1}], T^*/p^N)$.

Thus, we have taken r_j and b'_{r_j} for all j such that $2 \le j \le i$. (Note that r_1 is not defined.) We put $m_j = r_2 \cdots r_j$ for all j such that $2 \le j \le i$.

We define $b_{r_j} = \mathrm{Cor}_{K_{n'}/K_n}(b'_{r_j}) \in H^1_f(O_{K_n}[1/Q], T^*/p^N)$ for any j such that $2 \le j \le i$. Let m be a divisor of m_i. We define

$$a_d = \prod_{r|d} \phi_r(b_r) \in R_n/p^N$$

for any divisor d of m (we define $a_1 = 1$), and define

$$x_{m,\ell} = \sum_{d|m} a_d \kappa_{\frac{m}{d},\ell} \in H^1_f(O_{K_n}[1/m\ell], T^*/p^N) \tag{32}$$

for a prime ℓ dividing $\mathfrak{L}$ where the sum is taken over all divisors d of m including 1. We note that for any divisor m of m_i, $m\ell$ is admissible in the sense of Section 7 by our construction of r_j. So we can apply Propositions 7.15, 7.16 to $\kappa_{m,\ell}$. For $m = 1$, we define $x_{1,\ell} = \kappa_{1,\ell}$. The following lemma gives the key property of $x_{m,\ell}$.

Lemma 9.5. *Let ℓ be a prime dividing $\mathfrak{L}$.*

(1) For a prime r which divides m_i, we have $\partial_r(x_{m_i,\ell}) = \phi_r(x_{\frac{m_i}{r},\ell})$.

(2) *For a prime r which divides m_i, we have $\phi_r(x_{m_i,\ell}) = \phi_r(b_r)\phi_r(x_{\frac{m_i}{r},\ell})$.*

(3) *Let j be any integer such that $2 \leq j \leq i$, and $\beta_{d_{j-1}}$ be the map defined above. Then we have*

$$\beta_{d_{j-1}}(x_{m_i,\ell}) = 0.$$

(4) *Let*

$$\alpha : \bigoplus_{\ell' | \mathfrak{L}m_i} \mathcal{H}^2_{\ell'}(K_n) \longrightarrow (R_{n'}/p^N)^a$$

be the map defined in Section 8. The composition of α with the j-th projection induces

$$\alpha_j : \bigoplus_{\ell' | \mathfrak{L}m_i} \mathcal{H}^2_{\ell'}(K_n) \longrightarrow R_n/p^N,$$

which we denote by α_j. Then we have

$$\alpha_j(\partial(x_{m_i,\ell_{c_1}})) = 0$$

for any j such that $j \neq c_1, \ldots, c_i$.

Proof. Properties (1) and (2) can be proved by the same method as [16, Prop. 7.1]. Property (1) follows from Proposition 7.13, and Property (2) follows from Proposition 7.15 by direct computations (see the proof of [16, Prop. 7.1]).

Next, we will prove (4). Since $x_{m_i,\ell_{c_1}}$ is in $H^1_f(O_{K_n}[1/\ell_{c_1} r_2 \cdots r_i], T^*/p^N)$, we obtain (4) from the definition of $x_{m_i,\ell}$, using above Property (9.2-I).

We will prove (3). Let j be an integer such that $2 \leq j \leq i$, and let b'_{r_j} be as above. By the definition of α and (9.2-I), we have $\alpha(\partial(b'_{r_j})) = \alpha(t_{r_j,K_{n'}} - t_{\ell_{c_j},K_{n'}}) = 0$. This implies that $\beta(b_{r_j}) = 0$ by the definition of β. Put

$$x = x_{m_i,\ell} - (\phi_{r_j}(x_{\frac{m_i}{r_j},\ell})b_{r_j} + \cdots + \phi_{r_i}(x_{\frac{m_i}{r_i},\ell})b_{r_i}).$$

It follows from $\beta(b_{r_j}) = \cdots = \beta(b_{r_i}) = 0$ that

$$\beta_{d_{j-1}}(x_{m_i,\ell}) = \beta_{d_{j-1}}(x).$$

By Lemma 9.5(1), for any $r = r_j, \ldots, r_i$, we have $\partial_r(x) = \phi_r(x_{\frac{m_i}{r},\ell}) - \phi_r(x_{\frac{m_i}{r},\ell}) = 0$. This shows that x is in $H^1_f(O_{K_n}[1/m_{j-1}\mathcal{L}], T^*/p^N)$ because $m_i/(r_j \cdots r_i) = m_{j-1}$. Hence, applying above Property (9.2-III), we obtain

$$\beta_{d_{j-1}}(x) = \phi_{r_j}(x).$$

By above Property (9.2-II), we have $\phi_{r_j}(b_{r_{j+1}}) = \cdots = \phi_{r_j}(b_{r_i}) = 0$. Therefore, we obtain

$$\begin{aligned}
\phi_{r_j}(x) &= \phi_{r_j}(x_{m_i,\ell} - \phi_{r_j}(x_{\frac{m_i}{r_j},\ell})b_{r_j}) \\
&= \phi_{r_j}(x_{m_i,\ell}) - \phi_{r_j}(x_{\frac{m_i}{r_j},\ell})\phi_{r_j}(b_{r_j}) \\
&= 0.
\end{aligned}$$

Here, we used Lemma 9.5(2) to get the last equality. Thus, we have obtained $\beta_{d_{j-1}}(x_{m_i,\ell}) = \phi_{r_j}(x) = 0$, which completes the proof of Lemma 9.5. □

9.6. **Proof of Theorem A.** We put $\ell = \ell_{c_1}$. We regard $\mathbf{x} = \beta(x_{m_i,\ell}) \in (R_n/p^N)^a$ and $\mathbf{y} = \alpha(\partial(x_{m_i,\ell})) \in (R_n/p^N)^a$ as column vectors. Recall that $\Lambda = O[[\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})]]$. Let γ_n be a generator of $\Gamma_n = \mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q}_n)$. Since $R_n/p^N = \Lambda/(\gamma_n - 1, p^N)$, we have

$$\mathcal{A}\mathbf{x} \equiv \mathbf{y} \pmod{(\gamma_n - 1, p^N)}.$$

When $i = 1$, since $x_{1,\ell} = g_\ell^{K_n}$, the c_1-th component of $\mathbf{y}$ is θ_{K_n}, and the other components are zero, namely we have $\mathbf{y} = \theta_{K_n}\mathbf{e}_{c_1}$ and

$$\mathcal{A}\mathbf{x} \equiv (\det \mathcal{A})\mathbf{e}_{c_1} \pmod{(\gamma_n - 1, p^N)} \tag{33}$$

because $\det \mathcal{A} = \theta_{K_\infty} \equiv \theta_{K_n} \pmod{(\gamma_n - 1)}$.

Suppose that $i \geq 2$. Let $\mathbf{x}' \in (R_n/p^N)^{a-i+1}$ be the vector obtained from $\mathbf{x}$ by eliminating the d_1-th component, ..., and the d_{i-1}-th component, and $\mathbf{y}' \in (R_K/p^N)^{a-i+1}$ the vector obtained from $\mathbf{y}$ by eliminating the c_1-th component, ..., and the c_{i-1}-th component. It follows from Lemma 9.5(3) that the d_j-th component of $\mathbf{x}$ is zero in R_n/p^N for all j such that $1 \leq j \leq i-1$. Therefore, we have

$$\mathcal{A}_{i-1}\mathbf{x}' \equiv \mathbf{y}' \pmod{(\gamma_n - 1, p^N)}.$$

The c_i-th component of $\mathbf{y}$ is $\phi_{r_i}(x_{\frac{m_i}{r_i},\ell}) = \phi_{r_i}(x_{m_{i-1},\ell})$ by Lemma 9.5(1). Hence, if the c_i'-th component of $\mathbf{y}'$ is the c_i-th component of $\mathbf{y}$, by Lemma 9.5 (4) we have

$$\mathbf{y}' \equiv \phi_{r_i}(x_{m_{i-1},\ell})\mathbf{e}_{c_i'} \pmod{(\gamma_n - 1, p^N)}$$

where $\mathbf{e}_{c_i'}$ denotes the c_i'-th standard basis vector of $(R_n/p^N)^{a-i+1}$.

Let $\mathrm{Adj}(\mathcal{A}_{i-1})$ be the matrix of cofactors (namely, the (s,t) entry of $\mathrm{Adj}(\mathcal{A}_{i-1})$ is $(-1)^{s+t}\det P_{ts}$ where P_{ts} is the matrix obtained by eliminating the t-th row and the s-th column of $\mathcal{A}_{i-1}$). Multiplying both sides of $\mathcal{A}_{i-1}\mathbf{x}' \equiv \phi_{r_i}(x_{m_{i-1},\ell})\mathbf{e}_{c_i'}$ by $\mathrm{Adj}(\mathcal{A}_{i-1})$ on the left, we get

$$(\det \mathcal{A}_{i-1})\mathbf{x}' \equiv \mathrm{Adj}(\mathcal{A}_{i-1})\phi_{r_i}(x_{m_{i-1},\ell})\mathbf{e}_{c_i'}.$$

Suppose that the d_i'-th component of $\mathbf{x}'$ is the d_i-th component of $\mathbf{x}$. Then the above congruence implies

$$(\det \mathcal{A}_{i-1})\beta_{d_i}(x_{m_i,\ell}) \equiv (-1)^{c_i'+d_i'}(\det \mathcal{A}_i)\phi_{r_i}(x_{m_{i-1},\ell}) \pmod{(\gamma_m - 1, p^N)}. \tag{34}$$

We continue this procedure and take r_{i+1} satisfying the above properties. Especially, by Property (9.2-III), we have

$$\beta_{d_i}(x_{m_i,\ell}) = \phi_{r_{i+1}}(x_{m_i,\ell}).$$

Therefore, (34) becomes

$$(\det \mathcal{A}_{i-1})\phi_{r_{i+1}}(x_{m_i,\ell}) \equiv \pm(\det \mathcal{A}_i)\phi_{r_i}(x_{m_{i-1},\ell}) \pmod{(\gamma_m - 1, p^N)}. \tag{35}$$

Here, we wrote $\pm$ because we do not care about the sign.

In the case $i = 1$, multiplying (33) by $\mathrm{Adj}(\mathcal{A})$ and looking at the d_1-th component, we obtain

$$(\det \mathcal{A})\phi_{r_2}(x_{m_1,\ell}) \equiv (-1)^{c_1+d_1}(\det \mathcal{A}_1)(\det \mathcal{A}) \pmod{(\gamma_m - 1, p^N)} \tag{36}$$

by the same method as above.

We take N such that $N \to \infty$ as $n \to \infty$. We can prove that the limit of $\phi_{r_{i+1}}(x_{m_i,\ell})$ exists in Λ, and

$$\lim_{n\to\infty} \phi_{r_{i+1}}(x_{m_i,\ell}) = \pm \det \mathcal{A}_i \in \Lambda \tag{37}$$

by the same method as [16, Sec. 10]. In fact, for $i = 1$ we obtain

$$\lim_{n\to\infty} \phi_{r_2}(x_{m_1,\ell}) = \pm \det \mathcal{A}_1 \in \Lambda$$

from (36). For general $i \geq 1$, using induction on i we conclude (37) from (35).

Therefore, in order to prove Theorem A, it is enough to show

$$\lim_{n\to\infty} \phi_{r_{i+1}}(x_{m_i,\ell}) \in \Theta_i. \tag{38}$$

Let $\Theta^{(N)}_{i,K_n}$ be the image of $\Theta^{(N)}_i$ in R_n/p^N. We have $\varprojlim \Theta^{(N)}_{i,K_n} = \Theta^{(N)}_i$. Hence, in order to prove (38), it suffices to show

$$\phi_{r_{i+1}}(\kappa_{m,\ell}) \in \Theta^{(N)}_{i,K_n} \tag{39}$$

for all divisors m of m_i.

We will prove (39). Applying Proposition 9.3, we can take $\ell' \in Q_{c_1}$ such that

(i) $\ell' \in \mathcal{P}_{1,\sigma}((K_{n'})_{[a+1]}(\mathfrak{L}m_i))$,
(ii) $\ell' \neq \ell = \ell_{c_1}$,
(iii) there is $b' \in H^1_f(O_{(K_{n'})_{[a+1]}}[1/\ell'\ell_{c_j}], T^*/p^N)$ such that $\partial(b') = t_{\ell',(K_{n'})_{[a+1]}} - t_{\ell,(K_{n'})_{[a+1]}}, \phi_{r_s}(b') = 0$ holds for any s such that $2 \leq s \leq i$, and
(iv) $\phi_{r_{i+1}} = \phi_{\ell'}$ on $H^1_f(O_{K_n}[1/\mathfrak{L}m_i], T^*/p^N)$.

Using the above (iv), we have

$$\phi_{r_{i+1}}(\kappa_{m,\ell}) = \phi_{\ell'}(\kappa_{m,\ell}).$$

Put $b = \mathrm{Cor}_{(K_{n'})_{[a+1]}/K_n}(b')$. Since $m\ell\ell' \in \mathcal{N}_1((K_n)_{[a+1]}) \subset \mathcal{N}_1((K_n)_{[\epsilon(m\ell\ell')]})$, we have $\kappa_{m,\ell} = \kappa_{m,\ell'} - \delta_m b$ by Proposition 7.14(2). Since $m\ell$ is admissible and $m\ell \in \mathcal{N}_1((K_n)_{[a+1]}) \subset \mathcal{N}_1((K_n)_{[\epsilon(m\ell)+1]})$, using Proposition 7.16, we compute

$$\begin{aligned}\phi_{r_{i+1}}(\kappa_{m,\ell}) &= \phi_{\ell'}(\kappa_{m,\ell}) = \phi_{\ell'}(\kappa_{m,\ell'} - \delta_m b)\\ &= -\delta_{m\ell'} - \delta_m \phi_{\ell'}(b).\end{aligned}$$

Therefore, we get $\phi_{r_{i+1}}(\kappa_{m,\ell}) \in \Theta^{(N)}_{i,K_n}$ because both $\delta_{m\ell'}$ and δ_m belong to $\Theta^{(N)}_{i,K_n}$. This completes the proof of (39) and that of Theorem A.

10. Main Theorem B

10.1. **An exact sequence and self-duality.** In the previous section, we proved Theorem A where a key role was played by the elements $x_{m,\ell}$. In this section, we study an elliptic curve case for simplicity, where $\kappa_{m,\ell}$ plays a key role instead of $x_{m,\ell}$. Namely, we need not modify the elements $\kappa_{m,\ell}$, and can use them directly.

Let E be an elliptic curve over $\mathbf{Q}$. We denote by $T = T_p(E) = \varprojlim E[p^n]$ the Tate module, and define $V = T \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ and $A = T \otimes_{\mathbf{Z}_p} \mathbf{Q}_p/\mathbf{Z}_p = E[p^\infty]$. For simplicity we fix a basis of T. We take a basis e_1,e_2 of T/p^N such that $\langle e_1, e_2\rangle_{\mathrm{Weil}} = \zeta_{p^N}$ where $\langle e_1, e_2\rangle_{\mathrm{Weil}}$ is the Weil pairing of e_1, $e_2 \in T/p^N = E[p^N]$ and ζ_{p^N} is the primitive p^N-th root of unity we fixed. By the Weil pairing, T is self-dual, namely T^* is isomorphic to T. We defined e_1^*, $e_2^* \in T^*/p^N$ in Lemma 7.2. By our identification of T/p^N with T^*/p^N by the Weil pairing, we know that e_1^* corresponds to $-e_2$ and e_2^* corresponds to e_1.

We use the same notation as Section 8. We fix $N > 0$ and take sufficiently large n and n' as in Section 8. We define K_n to be the n-th layer of $\mathbf{Q}_\infty/\mathbf{Q}$, $\Gamma_n = \mathrm{Gal}(\mathbf{Q}_\infty/K_n)$ and $R_n = \mathbf{Z}_p[\mathrm{Gal}(K_n/\mathbf{Q})]$. We take generators $x_1, \dots, x_a$ of X as in Section 8. We take a to be *minimal*, namely we suppose that X is generated by *exactly* a *elements*. We assume $a > 0$. We consider $\mathcal{P}_{1,\sigma}$ as in Subsection 5.8, then $H^0(\mathbf{F}_\ell, T/p^N(-1)) = t(\mathbf{Z}/p^N)$ where $t = e_2^\vee$ for any $\ell \in \mathcal{P}_{1,\sigma}$. (We may take a basis depending on each $\ell \in \mathcal{P}_1$ for the argument below, so we need not fix our basis e_1, e_2, but for simplicity we fix it.) For each i such that $1 \le i \le a$, we define

$$Q_i = \{\ell_i \in \mathcal{P}_{1,\sigma}(K_{n'}) \mid r_{\ell_i}(t_{\ell_i,K_{n'}}) = x_i \bmod (p^N, \Gamma_{n'})\}. \tag{40}$$

We take $\ell_i \in Q_i$ for each i, and put $S = \{\ell_1, \dots, \ell_a\}$.

By Proposition 8.2(ii), $H^1_f(O_{K_n}[1/S], T/p^N)$ is a free R_n/p^N-module of rank a. By Corollary 5.6 we have an exact sequence

$$\begin{aligned} 0 \longrightarrow H^1_f(O_{K_n}, T/p^N) \longrightarrow H^1_f(O_{K_n}[1/S], T/p^N) \xrightarrow{\partial} \bigoplus_{\ell\in S} \mathcal{H}^2_\ell(K_n) \\ \longrightarrow H^1_f(O_{K_n}, T/p^N)^\vee \longrightarrow 0. \end{aligned} \tag{41}$$

For a prime v above ℓ_i, we consider a map $\phi'_{K_{n,v}} : H^1(K_{n,v}, T/p^N) \longrightarrow H^1(\kappa(v), T/p^N)$ which was defined in Subsection 7.1 where $\kappa(v)$ is the residue field of v, which is $\mathbf{F}_{\ell_i}$ in our case. We put

$$\mathcal{H}^1_{\ell,f}(K_n) = \bigoplus_{v\in S_{\ell,K_n}} H^1(\kappa(v), T/p^N).$$

We define

$$\Phi_S : H^1_f(O_{K_n}[1/S], T/p^N) \longrightarrow \bigoplus_{\ell\in S} \mathcal{H}^1_{\ell,f}(K_n)$$

as the direct sum of the compositions of the natural maps

$$H^1_f(O_{K_n}[1/S], T/p^N) \longrightarrow H^1(K_{n,v}, T/p^N)$$

and $\phi'_{K_{n,v}}$.

Let e_1^*, $e_2^* \in T^*/p^N$ be as above. We regard e_1^* as an element of $H^1(\kappa(v), T/p^N) = H^1(\kappa(v), T^*/p^N)$ as in Lemma 7.2. We denote by t^*_{ℓ,K_n} the element of $\mathcal{H}^1_{\ell,f}(K_n)$ whose ℓ_{K_n}-component is e_1^* and the other components are 0. Note that $\mathcal{H}^1_{\ell,f}(K_n)$ is a free R_n/p^N-module of rank 1, generated by t^*_{ℓ,K_n}.

Lemma 10.2. *Φ_S gives an isomorphism of R_n-modules.*

Proof. Let $\mathfrak{m} = (p, \gamma - 1)$ be the maximal ideal of R_n/p^N where γ is a generator of $\mathrm{Gal}(K_n/\mathbf{Q})$. For an R_n/p^N-module M, we define $M[\mathfrak{m}]$ to be $\{x \in M \mid \mathfrak{m}x = 0\}$. Since X is generated by exactly a elements, $H^1_f(O_{K_n}, T/p^N)^\vee/\mathfrak{m}$ is an $\mathbf{F}_p$-vector space of dimension a by Nakayama's lemma. Therefore, $H^1_f(O_{K_n}, T/p^N)[\mathfrak{m}]$ is also an $\mathbf{F}_p$-vector space of dimension a. Since $H^1_f(O_{K_n}[1/S], T/p^N)$ is a free R_n/p^N-module of rank a by Proposition 8.2(1) and R_n/p^N is a Gorenstein ring, $H^1_f(O_{K_n}[1/S], T/p^N)[\mathfrak{m}]$ is also an $\mathbf{F}_p$-vector space of dimension a. It follows that the injective homomorphism

$$H^1_f(O_{K_n}, T/p^N)[\mathfrak{m}] \longrightarrow H^1_f(O_{K_n}[1/S], T/p^N)[\mathfrak{m}] \tag{42}$$

is bijective.

Since $\bigoplus_{\ell \in S} \mathcal{H}^2_\ell(K_n) \longrightarrow H^1_f(O_{K_n}, T/p^N)^\vee$ is surjective, taking the dual, we know that the natural map

$$H^1_f(O_{K_n}, T/p^N)[\mathfrak{m}] \longrightarrow \bigoplus_{\ell \in S} \mathcal{H}^1_{\ell,f}(K_n)[\mathfrak{m}]$$

is injective. Since both groups have order p^a, this is bijective. Therefore, it follows from the bijectivity of (42) that

$$\Phi_S : H^1_f(O_{K_n}[1/S], T/p^N)[\mathfrak{m}] \longrightarrow \bigoplus_{\ell \in S} \mathcal{H}^1_{\ell,f}(K_n)[\mathfrak{m}]$$

which is induced by Φ_S is bijective. Since both $H^1_f(O_{K_n}[1/S], T/p^N)$ and $\bigoplus_{\ell \in S} \mathcal{H}^1_{\ell,f}(K_n)$ are free R_n/p^N-modules of rank a and R_n is Gorenstein, this implies that $\Phi_S : H^1_f(O_{K_n}[1/S], T/p^N) \longrightarrow \bigoplus_{\ell \in S} \mathcal{H}^1_{\ell,f}(K_n)$ is bijective. This completes the proof of Lemma 10.2. □

We put

$$\mathcal{H}_1 = \bigoplus_{\ell \in S} \mathcal{H}^1_{\ell,f}(K_n), \ \mathcal{H}_2 = \bigoplus_{\ell \in S} \mathcal{H}^2_\ell(K_n).$$

We denote by $\Psi : \mathcal{H}_1 \longrightarrow \mathcal{H}_2$ the composition of Φ_S^{-1} and the natural map $\partial_K : H^1_f(O_{K_n}[1/S], T/p^N) \longrightarrow \mathcal{H}_2$. Then we have an exact sequence

$$0 \longrightarrow H^1_f(O_{K_n}, T/p^N) \longrightarrow \mathcal{H}_1 \xrightarrow{\Psi} \mathcal{H}_2 \longrightarrow H^1_f(O_{K_n}, T/p^N)^\vee \longrightarrow 0 \tag{43}$$

from the exact sequence (41). Note that both $\mathcal{H}_1$ and $\mathcal{H}_2$ are free R_n/p^N-modules of rank a.

By definition $\mathcal{H}_1$ and $\mathcal{H}_2$ are dual each other by the canonical pairing $\cup : \mathcal{H}_1 \times \mathcal{H}_2 \longrightarrow \mathbf{Z}/p^N$ which is induced by the local Tate pairing. We extend this pairing to

$$\cup_{R_n} : \mathcal{H}_1 \times \mathcal{H}_2 \longrightarrow R_n/p^N$$

by $x \cup_{R_n} y = \sum_{\sigma \in G_n} ((\sigma x) \cup y)\sigma^{-1}$ where $G_n = \mathrm{Gal}(K_n/\mathbf{Q})$. Then this is a perfect pairing of R_n-modules. Let $\iota : R_n \longrightarrow R_n$ be the ring homomorphism

induced by $\gamma \mapsto \gamma^{-1}$ where γ is a generator of $\mathrm{Gal}(K_n/\mathbf{Q})$. Then by the definition of $\cup_{R_n}$, we have

$$a(x \cup_{R_n} y) = (ax) \cup_{R_n} y = x \cup_{R_n} (\iota(a)y) \tag{44}$$

for any $a \in R_n$, $x \in \mathcal{H}_1$, and $y \in \mathcal{H}_2$.

As in Subsection 5.8, let $t_{\ell,K_n} \in \mathcal{H}^2_\ell(K_n)$ be the element whose ℓ_{K_n}-component is $t = e_2^\vee$ and the other components are 0. Note that $e_2^\vee = e_1 \otimes \zeta_{p^N}^{\otimes(-1)}$. We regard t_{ℓ,K_n} as an element of $\mathcal{H}_2$. Then $\{t_{\ell,K_n}\}_{\ell\in S}$ is a basis of R_n/p^N-module $\mathcal{H}_2$. We defined $t^*_{\ell,K_n} \in \mathcal{H}^1_{\ell,f}(K_n)$ above. We regard t^*_{ℓ,K_n} as an element of $\mathcal{H}_1$, namely it is the element whose ℓ_{K_n}-component is e_1^* and the other components are 0. For any $\ell \in S$ and a prime v of K_n above ℓ, we have $H^1(\kappa(v), T/p^N) = (T/p^N)_{G_{\kappa(v)}}$ where $G_{\kappa(v)}$ is the absolute Galois group of $\kappa(v)$, so we know that $H^1(\kappa(v), T/p^N) = (T/p^N)/(\mathrm{Frob}_\ell - 1)$ is generated by e_2. Note that $e_1^* = -e_2$ by this identification. We know that $\{t^*_{\ell,K_n}\}_{\ell\in S}$ is a basis of R_n/p^N-module $\mathcal{H}_1$, moreover $\{t^*_{\ell,K_n}\}_{\ell\in S}$ is the dual basis of the pairing $\cup_{R_n}$ in the sense that $t^*_{\ell_i,K_n} \cup_{Rn} t_{\ell_j,K_n} = 1$ if $\ell_i = \ell_j$ and $= 0$ otherwise (where we used $\langle -e_2, e_1\rangle_{\mathrm{Weil}} = \zeta_{p^N}$).

We consider an $a \times a$ matrix

$$M = (m_{ij}) \in M_a(R_n/p^N)$$

which corresponds to Ψ with respect to the basis $\{t_{\ell_i,K_n}\}_{i=1,\dots,a}$ and $\{t^*_{\ell_j,K_n}\}_{j=1,\dots,a}$. Namely, $\Psi(t^*_{\ell_j,K_n}) = \sum_{i=1}^a m_{ij} t_{\ell_i,K_n}$. We define M^* by $M^* = (\iota(m_{ji}))$.

Lemma 10.3. *We have $M^* = -M$. Namely, M is skew-Hermitian.*

Proof. For any i, j such that $1 \le i, j \le a$, we have

$$\begin{aligned} t^*_{\ell_i,K_n} \cup_{R_n} \Psi(t^*_{\ell_j,K_n}) &= t^*_{\ell_i,K_n} \cup_{R_n} (\sum_{k=1}^a m_{kj} t_{\ell_k,K_n}) \\ &= t^*_{\ell_i,K_n} \cup_{R_n} (m_{ij} t_{\ell_i,K_n}) \\ &= \iota(m_{ij}) \end{aligned}$$

by (44).

On the other hand, the Pontrjagin dual of the exact sequence (43) is also the exact sequence (43). Therefore, the diagram

$$\begin{array}{ccccc} \mathcal{H}_1 & \times & \mathcal{H}_2 & \xrightarrow{\cup} & \mathbf{Z}/p^N \\ \downarrow{\scriptstyle \Psi} & & \uparrow{\scriptstyle \Psi} & & \downarrow{\scriptstyle =} \\ \mathcal{H}_2 & \times & \mathcal{H}_1 & \xrightarrow{\cup} & \mathbf{Z}/p^N \end{array}$$

is commutative. This implies that $x \cup_{R_n} \Psi(y) = \Psi(x) \cup_{R_n} y$ for any x, $y \in \mathcal{H}_1$. Hence

$$t^*_{\ell_i,K_n} \cup_{R_n} \Psi(t^*_{\ell_j,K_n}) = \Psi(t^*_{\ell_i,K_n}) \cup_{R_n} t^*_{\ell_j,K_n}$$

$$= \left(\sum_{k=1}^{a} m_{ki} t_{\ell_k, K_n} \right) \cup_{R_n} t^*_{\ell_j, K_n}$$
$$= m_{ji} t_{\ell_j, K_n} \cup_{R_n} t^*_{\ell_j, K_n}$$
$$= -m_{ji} t^*_{\ell_j, K_n} \cup_{R_n} t_{\ell_j, K_n} = -m_{ji}.$$

Combining the above two equations, we get $\iota(m_{ij}) = -m_{ji}$. This completes the proof of Lemma 10.3. □

Remark 10.4. By the exact sequence (43), we know that M is a relation matrix of the Selmer group $H^1_f(O_{K_n}, T/p^N)^\vee$. Taking the projective limit with respect to N and n, we obtain from each M a relation matrix $\mathcal{A}$ of the Selmer group $X = H^1_f(O_{\mathbf{Q}_\infty}, E[p^\infty])^\vee$. Then $\mathcal{A}$ satisfies $\mathcal{A}^* = -\mathcal{A}$, namely $\mathcal{A}$ is skew-Hermitian. Such a matrix is called an organizing matrix by Mazur and Rubin [20].

We can choose a suitable unit $u \in \Lambda^\times$ such that $\theta'_{\mathbf{Q}_\infty} = u\theta_{\mathbf{Q}_\infty}$ satisfies $\iota(\theta'_{\mathbf{Q}_\infty}) = \epsilon\theta'_{\mathbf{Q}_\infty}$ where ϵ is the root number of E. The usual main conjecture asserts that $\mathrm{char}(X) = (\det \mathcal{A})\Lambda = \theta_{\mathbf{Q}_\infty}\Lambda = \theta'_{\mathbf{Q}_\infty}\Lambda$ as ideals of Λ. Put $\Lambda^\pm = \{x \in \Lambda \mid \iota(x) = \pm x\}$. Then we have decomposition $\Lambda = \Lambda^+ \oplus \Lambda^-$. We regard the equality

$$(\det \mathcal{A})\Lambda = \theta'_{\mathbf{Q}_\infty}\Lambda$$

as an equality of Λ^+-modules. Then it gives a refined version of the main conjecture. In fact, the above equality of Λ^+-modules implies $\iota(\det \mathcal{A}) = \det(-\mathcal{A}) = (-1)^a \det \mathcal{A}$. Since we took a to be minimal, we have $a \equiv \mathrm{rank}\,\mathrm{Sel}(\mathbf{Q}, E[p^\infty])^\vee \bmod 2$. Therefore, the above equality implies

$$\epsilon = (-1)^{\mathrm{rank}\,\mathrm{Sel}(\mathbf{Q}, E[p^\infty])^\vee},$$

which is nothing but the parity conjecture for a Selmer group, which was proved in our case by Nekovář [23].

10.5. **A suitable relation matrix of a Selmer group.** In this subsection we begin with the following standard fact on quadratic forms and skew-symmetric forms.

Lemma 10.6.

(1) Let $M \in M_r(\mathbf{Z}/p^N)$ be a symmetric matrix. Then there is an invertible matrix $P \in \mathrm{GL}_r(\mathbf{Z}/p^N)$ such that ${}^tPMP$ is a diagonal matrix where ${}^tP$ is the transpose of P.

(2) Let $M \in M_{2s}(\mathbf{Z}/p^N)$ be a skew-symmetric matrix. Then there is an invertible matrix $P \in \mathrm{GL}_{2s}(\mathbf{Z}/p^N)$ such that

$${}^tPMP = \begin{pmatrix} M_1 & & & 0 \\ & M_2 & & \\ & & \ddots & \\ 0 & & & M_s \end{pmatrix}$$

where $M_i = \begin{pmatrix} 0 & \alpha_i \\ -\alpha_i & 0 \end{pmatrix}$ *for some* $\alpha_i \in \mathbf{Z}/p^N$.

Proof. We define a function $\mathrm{ord}_p : \mathbf{Z}/p^N \longrightarrow \{0, 1, \ldots, N-1, \infty\}$ as follows. For $a \in \mathbf{Z}/p^N$ such that $a \neq 0$, if p^i divides a and p^{i+1} does not, we define $\mathrm{ord}_p(a) = i$. For $a = 0$, we define $\mathrm{ord}_p(0) = \infty$.

(1) Let $V = (\mathbf{Z}/p^N)^r$ and $f : V \times V \longrightarrow \mathbf{Z}/p^N$ be the corresponding symmetric form to the matrix M. We take $x \in V$ such that $\mathrm{ord}_p(f(x,x))$ is minimal. Then we can take V' such that $V = \langle x \rangle \oplus V'$ and $f(x,y) = 0$ for all $y \in V'$. By induction on the rank of V, we get the conclusion.

(2) Let $V = (\mathbf{Z}/p^N)^s$ and $f : V \times V \longrightarrow \mathbf{Z}/p^N$ be the corresponding skew-symmetric form to M. We take x, $y \in V$ such that $\mathrm{ord}_p(f(x,y))$ is minimal. Then we can take V' such that $V = \langle x, y \rangle \oplus V'$ and $f(x,z) = f(y,z) = 0$ for all $z \in V'$. By induction on the rank, we get the conclusion. □

Let $\mathrm{Sel}(\mathbf{Q}, E[p^\infty])$ be the Selmer group with respect to $E[p^\infty]$, and consider the Pontrjagin dual $\mathrm{Sel}(\mathbf{Q}, E[p^\infty])^\vee$ and its torsion part $(\mathrm{Sel}(\mathbf{Q}, E[p^\infty])^\vee)_{\mathrm{tors}}$. We take $N \in \mathbf{Z}_{>0}$ such that $N > \mathrm{ord}_p(\#(\mathrm{Sel}(\mathbf{Q}, E[p^\infty])^\vee)_{\mathrm{tors}})$.

Let $M \in M_a(R_n/p^N)$ be the matrix defined before Lemma 10.3. Put $\mathfrak{t} = \gamma - 1$. We identify R_n/p^N with $\mathbf{Z}/p^N[\mathfrak{t}]/(\omega_n(\mathfrak{t}))$ where $\omega_n(\mathfrak{t}) = (1+\mathfrak{t})^{p^n} - 1$. Since M is skew-Hermitian by Lemma 10.3, $M \bmod \mathfrak{t} \in M_a(\mathbf{Z}/p^N)$ is a skew-symmetric matrix. By Corollary 6.4 we have

$$(H^1_f(O_{K_n}, T/p^N)^\vee)_{\mathrm{Gal}(K_n/\mathbf{Q})} = H^1_f(\mathbf{Z}, T/p^N)^\vee = \mathrm{Sel}(\mathbf{Q}, T/p^N)^\vee.$$

This shows that $M \bmod \mathfrak{t}$ is a relation matrix of $\mathrm{Sel}(\mathbf{Q}, T/p^N)^\vee$. By changing the basis suitably (namely changing M to ${}^tPMP$ for some invertible P), we can take M to be

$$M = \begin{pmatrix} C_0 + \mathfrak{t}M_A & \mathfrak{t}M_B \\ \mathfrak{t}M_C & \mathfrak{t}M_D \end{pmatrix} \tag{45}$$

where C_0 is a matrix whose entries are in $\mathbf{Z}/p^N$ such that $\mathrm{ord}_p(\det C_0) = \mathrm{ord}_p(\#(\mathrm{Sel}(\mathbf{Q}, E[p^\infty])^\vee)_{\mathrm{tors}})$, and M_A, M_B, M_C, M_D are matrices whose entries are in R_n/p^N. Since M is skew-Hermitian, C_0 is a skew-symmetric matrix. We write $M_D = C_1 + \mathfrak{t}M'_D$ with $C_1 \in M_a(\mathbf{Z}/p^N)$ and $M'_D \in M_a(R_n/p^N)$. Then, since M is skew-Hermitian, C_1 is a symmetric matrix. Applying Lemma 10.6, by choosing a suitable basis, we can take

$$C_1 = \begin{pmatrix} \beta_1 & & & 0 \\ & \beta_2 & & \\ & & \ddots & \\ 0 & & & \beta_r \end{pmatrix} \text{ and } C_0 = \begin{pmatrix} 0 & \alpha_1 & & & 0 \\ -\alpha_1 & 0 & \ddots & & \\ & \ddots & \ddots & \ddots & \\ & & \ddots & 0 & \alpha_s \\ 0 & & & -\alpha_s & 0 \end{pmatrix} \tag{46}$$

where $\alpha_1, \ldots, \alpha_s$, $\beta_1, \ldots, \beta_r \in \mathbf{Z}/p^N$ for some s, $r \in \mathbf{Z}_{\geq 0}$. Note that $\mathrm{ord}_p(\det C_0) < \infty$ because we took $N > \mathrm{ord}_p(\#(\mathrm{Sel}(\mathbf{Q}, E[p^\infty])^\vee)_{\mathrm{tors}})$. We

take a basis of X such that

$$\mathrm{ord}_p(\alpha_1) \leq \cdots \leq \mathrm{ord}_p(\alpha_s) < \infty.$$

Note that changing the basis corresponds in our case to changing the generators $x_1, \ldots, x_a$ of X to appropriate generators which are linear combinations of $x_1, \ldots, x_a$.

We now have isomorphisms

$$\mathrm{Sel}(\mathbf{Q}, E[p^\infty])^\vee \simeq \bigoplus_{k=1}^{s} (\mathbf{Z}_p/p^{\nu_k})^{\oplus 2} \oplus \mathbf{Z}_p^{\oplus r} \tag{47}$$

and

$$\mathrm{Sel}(\mathbf{Q}, T/p^N)^\vee \simeq \bigoplus_{k=1}^{s} (\mathbf{Z}/p^{\nu_k})^{\oplus 2} \oplus (\mathbf{Z}/p^N)^{\oplus r} \tag{48}$$

where $\nu_k = \mathrm{ord}_p(\alpha_k)$.

10.7. **Higher Stickelberger ideals.** Recall that we defined in Subsection 4.3 the higher Stickelberger ideal $\Theta_i^{(N)} \subset \Lambda/p^N$ (now we are taking $T = T_p(E)$). We define the ideal $\Theta_i^{(N)}(K_n)$ of R_n/p^N to be the image of $\Theta_i^{(N)}$ under the canonical homomorphism $\Lambda/p^N \longrightarrow R_n/p^N$. We also define $\Theta_i(K_n)$ by $\Theta_i(K_n) = \varprojlim_N \Theta_i^{(N)}(K_n) \subset R_n$, in particular,

$$\Theta_i(\mathbf{Q}) = \varprojlim_N \Theta_i^{(N)}(\mathbf{Q}) \subset \mathbf{Z}_p.$$

We denote by $\mathcal{N}^{(N)}$ the set of squarefree products of primes $\ell \in \mathcal{P}$ such that $\ell \equiv 1 \pmod{p^N}$. For $m \in \mathcal{N}^{(N)}$, we consider $\mathbf{Q}(m)_\infty \in \mathcal{K}$ and $\theta_{\mathbf{Q}(m)_\infty} \in \Lambda_{\mathbf{Q}(m)_\infty}$ (see Subsection 3.1 for the definition of $\mathbf{Q}(m)$). Suppose that $m = \prod_{i=1}^{q} \ell_i$. We put $S_i = \sigma_{\ell_i} - 1$ and identify $\Lambda_{\mathbf{Q}(m)_\infty}$ with $\Lambda[S_1, \ldots, S_q]/I$ where I is the ideal generated by all $(1+S_i)^{p^{n_{\ell_i}}} - 1$. Let $\delta_m^{(\mathbf{Q}_\infty)} \in \Lambda/p^N$ be $(-1)^{\epsilon(m)}$ times the coefficient of $\prod_{i=1}^{q} S_i$ in $\theta_{\mathbf{Q}(m)_\infty}$ (cp. (21)). Then by definition, $\delta_m^{(\mathbf{Q}_\infty)} \in \Theta_i^{(N)}$. For a subfield K_n of $\mathbf{Q}_\infty$, we denote by $\delta_m^{(K_n)}$ the image of $\delta_m^{(\mathbf{Q}_\infty)}$ in R_n/p^N. We know

$$\delta_m^{(K_n)} \in \Theta_{\epsilon(m)}^{(N)}(K_n) \tag{49}$$

by definition. Note that if $m \in \mathcal{N}_1(K_n)$, $\delta_m^{(K_n)}$ coincides with the element defined in (21).

We denote by $\Theta_i^{(N,\delta)}(\mathbf{Q})$ the ideal of $\mathbf{Z}/p^N$ generated by $\{\delta_m^{(\mathbf{Q})} \mid \epsilon(m) \leq i$ and $m \in \mathcal{N}^{(N)}\}$. By Corollary 6.5, we have

$$\Theta_i^{(N)}(K_n) \subset \mathrm{Fitt}_{i,R_n/p^N}(H_f^1(O_{K_n}, T/p^N)^\vee). \tag{50}$$

Therefore, for $n = 0$, we have

$$\Theta_i^{(N,\delta)}(\mathbf{Q}) \subset \Theta_i^{(N)}(\mathbf{Q}) \subset \mathrm{Fitt}_{i,\mathbf{Z}/p^N}(\mathrm{Sel}(\mathbf{Q}, T/p^N)^\vee). \tag{51}$$

We put

$$\mathrm{Fitt}_{i,\mathbf{Z}_p}(\mathrm{Sel}(\mathbf{Q},E[p^\infty])^\vee)=p^{n_i}\mathbf{Z}_p$$

where $n_i \in \mathbf{Z}_{\geq 0}\cup\{\infty\}$ (we define $p^\infty = 0$). By the description (47) of $\mathrm{Sel}(\mathbf{Q},E[p^\infty])^\vee$, we have $n_i=\infty$ for i such that $0\leq i\leq r-1$, and

$$n_{r+2i}=2\sum_{k=1}^{s-i}\nu_k \quad \text{for} \quad i=0,\dots,s-1,$$

and $n_i=0$ for all $i\geq a$. By the above inclusion, we have

$$\Theta_i^{(N)}(\mathbf{Q})=\mathrm{Fitt}_{i,\mathbf{Z}_p}(\mathrm{Sel}(\mathbf{Q},T/p^N)^\vee)=0$$

for all i such that $0\leq i\leq r-1$. Therefore, in order to prove Theorem B, it is enough to prove

$$\Theta_{r+2i}^{(N,\delta)}(\mathbf{Q})=p^{e_i}(\mathbf{Z}/p^N) \text{ where } e_i=2\sum_{k=1}^{s-i}\nu_k \tag{52}$$

for all $i=0,\dots,s$ and for all sufficiently large N. In fact, if we prove (52), then by (51) we get

$$\Theta_{r+2i}^{(N,\delta)}(\mathbf{Q})=\Theta_{r+2i}^{(N)}(\mathbf{Q})=\mathrm{Fitt}_{r+2i,\mathbf{Z}_p}(\mathrm{Sel}(\mathbf{Q},T/p^N)^\vee) \tag{53}$$

for all $i=0,\dots,s$.

We assume the main conjecture for (E,p) and the nondegeneracy of the p-adic height pairing. Let $\theta_{\mathbf{Q}_\infty}\in\Lambda$ be the p-adic L-function. Then by Schneider [29, Thm. 5], $\theta_{\mathbf{Q}_\infty}$ can be written as $\theta_{\mathbf{Q}_\infty}=\eta_0\mathfrak{t}^r+\eta'\mathfrak{t}^{r+1}$ where $\eta_0\in\mathbf{Z}_p$, $\eta_0\neq 0$, and $\eta'\in\Lambda$ (see (54)).

In order to prove Theorem B, we may take N and n sufficiently large. From now on, we take N such that $N>2\,\mathrm{ord}_p(\eta_0)$, and take n such that $\omega_n(\mathfrak{t})\in p^N\mathbf{Z}_p[[\mathfrak{t}]]+\mathfrak{t}^{2a}\mathbf{Z}_p[[\mathfrak{t}]]$, namely such that there is a natural surjective homomorphism $R_n\longrightarrow\mathbf{Z}_p[[\mathfrak{t}]]/(p^N,\mathfrak{t}^{2a})$. As we will see in (54), the condition on N implies that $N>\mathrm{ord}_p(\det C_0)$, which we assumed in the previous subsection.

Let $H^1_f(\mathbf{Z},T)$ be the Selmer group of $T=T_p(E)$ over $\mathbf{Q}$. Taking the dual of the natural injective homomorphism $H^1_f(\mathbf{Z},T)\otimes\mathbf{Q}_p/\mathbf{Z}_p\longrightarrow H^1_f(\mathbf{Z},E[p^\infty])$, we consider a surjective homomorphism $X\longrightarrow H^1_f(\mathbf{Z},E[p^\infty])^\vee\longrightarrow(H^1_f(\mathbf{Z},T)\otimes\mathbf{Q}_p/\mathbf{Z}_p)^\vee\longrightarrow\mathrm{Hom}_{\mathbf{Z}_p}(H^1_f(\mathbf{Z},T)',\mathbf{Z}_p)$ where $H^1_f(\mathbf{Z},T)'$ is the quotient of $H^1_f(\mathbf{Z},T)$ by the subgroup of $\mathbf{Z}_p$-torsion elements. Let $x_1,\dots,x_a$ be the generators of X we took. We denote by $x_{i,\mathbf{Q}}$ the image of x_i in $\mathrm{Hom}_{\mathbf{Z}_p}(H^1_f(\mathbf{Z},T)',\mathbf{Z}_p)$. Then $x_{2s+1,\mathbf{Q}},\dots,x_{2s+r,\mathbf{Q}}$ is a basis of the $\mathbf{Z}_p$-module $\mathrm{Hom}_{\mathbf{Z}_p}(H^1_f(\mathbf{Z},T)',\mathbf{Z}_p)$. We denote by $(x_{i,\mathbf{Q}})^\vee$ the dual basis of $H^1_f(\mathbf{Z},T)'$. In Schneider [30, p.335], the p-adic height pairing is defined by using the homomorphism

$$H^1_f(\mathbf{Z},E[p^\infty])\longrightarrow H^1_f(O_{K_\infty},E[p^\infty])^\Gamma\longrightarrow H^1_f(O_{K_\infty},E[p^\infty])_\Gamma\longrightarrow H^1_f(\mathbf{Z},T)^\vee$$

where $\Gamma = \mathrm{Gal}(K_\infty/\mathbf{Q}) = \mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})$. Let C_1 be the matrix in (45). Then C_1 corresponds to the matrix of the p-adic height pairing, which means the following. We write $C_1 = (c_{ij})$. Using the relation matrix M of $H^1_f(O_{K_\infty}, E[p^N])$, we compute the map $(H^1_f(O_{K_\infty}, E[p^\infty])^\vee)^\Gamma \longrightarrow (H^1_f(O_{K_\infty}, E[p^\infty])^\vee)_\Gamma$, then we know that the p-adic height pairing of $(x_{2s+i,\mathbf{Q}})^\vee$ and $(x_{2s+j,\mathbf{Q}})^\vee$ mod p^N coincides with c_{ij}. In particular, $\det C_1$ coincides with the p-adic regulator mod p^N. Therefore, Theorem $2'$ in Schneider [30] implies that

$$\mathrm{ord}_p(\eta_0) = \mathrm{ord}_p(\det C_0 \det C_1). \tag{54}$$

Since we took $N > 2\,\mathrm{ord}_p(\eta_0) \geq \mathrm{ord}_p(\eta_0)$, we have $\det C_1 \neq 0$ in $\mathbf{Z}/p^N$ by (54), so $\beta_i \neq 0$ in $\mathbf{Z}/p^N$ for all i such that $1 \leq i \leq r$.

Note that N also satisfies $N > \mathrm{ord}_p(C_0) = 2\sum_{k=1}^{s} \nu_k$. The following theorem implies (52), so implies Theorem B. Therefore, the rest of our task is to prove

Theorem 10.8. *For any i such that $0 \leq i \leq s$, there is $m \in \mathcal{N}_1(K_n)$ such that $\epsilon(m) = r + 2i$ and*

$$\mathrm{ord}_p(\delta_m^{(\mathbf{Q})}) = 2\sum_{k=1}^{s-i} \nu_k.$$

10.9. **Kolyvagin systems of Gauss sum type.** Recall that we took N such that $N > 2\,\mathrm{ord}_p(\eta_0)$, and took n such that $\omega_n(\mathfrak{t}) \in p^N\mathbf{Z}_p[[\mathfrak{t}]] + \mathfrak{t}^{2a}\mathbf{Z}_p[[\mathfrak{t}]]$. We take generators $x_1, \ldots, x_a$ of X such that the matrices M, C_0, C_1 have the forms as in (45) and (46). For an integer i such that $0 \leq i \leq a-1$, by induction on i we take $\ell_{a-i} \in Q_{a-i}$ such that

$$\ell_{a-i} \in \mathcal{P}_1((K_{n'})_{[a+1]}(m_i))$$

where we define $m_0 = 1$ and $m_i = \ell_a \cdots \ell_{a-i+1}$ for $i > 0$ (note that we are using a different notation from Section 9), and n' is an integer which was used when we defined Q_i in (40). We put $m_a = \ell_1 \cdots \ell_a$. For any positive integer $m\ell$ which divides m_a, $m\ell$ is admissible by this construction.

By Propositions 7.13, 7.15, 7.16 we obtain the following Proposition.

Proposition 10.10. *Assume that $m\ell$ divides $m_a = \ell_1 \cdots \ell_a$. Then the element $\kappa_{m,\ell} \in H^1_f(O_{K_n}[1/S], T/p^N)$ constructed in Section 7 satisfies the following properties;*

(0) $\kappa_{m,\ell} \in H^1_f(O_{K_n}[1/m\ell], T/p^N)$,
(1) $\partial_r(\kappa_{m,\ell}) = \phi_r(\kappa_{\frac{m}{r},\ell})$ *for any prime divisor r of m,*
(2) $\partial_\ell(\kappa_{m,\ell}) = \delta_m$,
(3) $\phi_r(\kappa_{m,\ell}) = 0$ *for any prime divisor r of m,*
(4) $\phi_\ell(\kappa_{m,\ell}) = -\delta_{m\ell}$.

For any i such that $1 \leq i \leq r$, we denote by M_i the matrix which is obtained from M by eliminating the a-th row, ..., the $(a-i+1)$-th row and the a-th column, ..., the $(a-i+1)$-th column. By (45) and (46) we have

$$\det M_i \equiv (\det C_0)\beta_1 \cdots \beta_{r-i}\mathfrak{t}^{r-i} \pmod{\mathfrak{t}^{r-i+1}}. \tag{55}$$

For each $1 \leq i \leq a$, recall that $m_i = \ell_a \cdots \ell_{a-i+1}$, and that $m_0 = 1$. We prove the following proposition at first. We consider $\delta_{m_i} = \delta_{m_i}^{(K_n)} \in R_n/p^N$. When $i = 0$, δ_1 means θ_{K_n} which is the image of $\theta_{\mathbf{Q}_\infty}$ in R_n/p^N.

Proposition 10.11. *For $0 \leq i \leq r$, we have*

$$\delta_{m_i} \equiv d_{m_i} \mathfrak{t}^{r-i} \ (mod\ \mathfrak{t}^{r-i+1})$$

for some $d_{m_i} \in \mathbf{Z}/p^N$ such that

$$\mathrm{ord}_p(d_{m_i}) = \mathrm{ord}_p((\det C_0)\beta_1 \cdots \beta_{r-i}).$$

In particular, we have $\mathrm{ord}_p(\delta_{m_r}^{(\mathbf{Q})}) = \mathrm{ord}_p(\det C_0)$.

Proof. We prove this proposition by induction on i. If $i = 0$, this is nothing but (54). Next, suppose $r > 0$, and assume the above property for i and proceed to $i+1$. We identify $\mathcal{H}_1$ (resp. $\mathcal{H}_2$) with $(R_n/p^N)^a$ using the basis $(t^*_{\ell_j,K_n})_{j=1,\ldots,a}$ (resp. $(t_{\ell_i,K_n})_{i=1,\ldots,a}$), and write elements of $\mathcal{H}_1$ (resp. $\mathcal{H}_2$) as column vectors. We consider

$$\kappa_i = \kappa_{m_i,\ell_{a-i}}.$$

Put $\mathbf{x}_i = \Phi_S(\kappa_i)$ and $\mathbf{y}_i = \partial(\kappa_i)$. By definition we have $M\mathbf{x}_i = \mathbf{y}_i$. It follows from Proposition 10.10(3) that the j-th component of $\mathbf{x}_i$ is zero for all j such that $a - i + 1 \leq j \leq a$. Therefore, if we denote by $\mathbf{x}'_i$, $\mathbf{y}'_i$ the vectors obtained by eliminating the a-th component, ..., the $(a-i+1)$-th component from $\mathbf{x}_i$, $\mathbf{y}_i$, respectively, we have

$$M_i \mathbf{x}'_i = \mathbf{y}'_i.$$

By Proposition 10.10(0), κ_i is in $H^1_f(O_{K_n}[1/m_{i+1}], T/p^N)$, so all j-th components of $\mathbf{y}'_i$ are zero except $j = a - i$. Also, by Proposition 10.10(2), we know that the $(a-i)$-th component of $\mathbf{y}'_i$ is δ_{m_i}. Namely, $\mathbf{y}'_i = \delta_{m_i}\mathbf{e}_{a-i}$ where $\mathbf{e}_{a-i}$ is the vector whose $(a-i)$-th component is 1 and whose other components are zero. Let $\mathrm{Adj}(M_i)$ be the matrix of cofactors as in Subsection 9.6. We have

$$(\det M_i)\mathbf{x}'_i = \mathrm{Adj}(M_i)\delta_{m_i}\mathbf{e}_{a-i}.$$

By Proposition 10.10(4) and Lemma 7.2(2), the $(a-i)$-th component of $\mathbf{x}'_i$ is $\delta_{m_i\ell_{a-i}} = \delta_{m_{i+1}}$. Therefore, looking at the $(a-i)$-th component of the above equation, we have

$$(\det M_i)\delta_{m_{i+1}} = (\det M_{i+1})\delta_{m_i}. \tag{56}$$

We put $\mathcal{R} = \mathbf{Z}_p[[\mathfrak{t}]]/(p^N, \mathfrak{t}^{2a})$. By our choice of n, we have a surjective homomorphism $R_n \longrightarrow \mathcal{R}$, and we can regard (56) as an equation in $\mathcal{R}$.

We claim that the image of $\delta_{m_{i+1}}$ in $\mathcal{R}$ is in $\mathfrak{t}^{r-i-1}\mathcal{R}$. By the description (45) and (46), we have

$$\mathrm{Fitt}_{i+1,\mathcal{R}}(H^1_f(O_{K_n}, T/p^N)^\vee \otimes \mathcal{R}) \subset \mathfrak{t}^{r-i-1}\mathcal{R}.$$

Therefore, by (50) we have $\Theta^{(N)}_{i+1}(K_n) \otimes \mathcal{R} \subset \mathfrak{t}^{r-i-1}\mathcal{R}$. Since we know $\delta_{m_{i+1}}$ is in $\Theta^{(N)}_{i+1}(K_n)$ by (49), the above implies that the image of $\delta_{m_{i+1}}$ in $\mathcal{R}$ is in $\mathfrak{t}^{r-i-1}\mathcal{R}$.

For any element $f(\mathfrak{t}) \in \mathcal{R}$ such that $f(\mathfrak{t}) \equiv c\mathfrak{t}^d \bmod \mathfrak{t}^{d+1}$ with $c \neq 0$ in $\mathbf{Z}/p^N$ and $d < 2r$, we define $v(f(\mathfrak{t})) = \mathrm{ord}_p(c)$ and $d(f(\mathfrak{t})) = d$. We regard $\det M_i$, $\det M_{i+1}$, δ_{m_i}, $\delta_{m_{i+1}}$ as elements in $\mathcal{R}$. By (55) we know $d(\det M_i) = r-i$, and by the hypothesis of induction we have $d(\delta_{m_i}) = r-i$. Also, the hypothesis of induction implies that $v(\det M_i) = v(\delta_{m_i}) < N/2$. Therefore, by (56) we get

$$d((\det M_i)\delta_{m_{i+1}}) = d((\det M_{i+1})\delta_{m_i}) = 2(r-i) - 1 < 2r$$

and $v((\det M_i)\delta_{m_{i+1}}) = v(\det M_{i+1}) + v(\det M_i) < N$. Since we saw that $\mathfrak{t}^{r-i-1}$ divides $\delta_{m_{i+1}}$ above, the above equality implies that

$$d(\delta_{m_{i+1}}) = d(\det M_{i+1}) = r - i - 1$$

and

$$v(\delta_{m_{i+1}}) = v(\det M_{i+1}) = \mathrm{ord}_p((\det C_0)\beta_1 \cdots \beta_{r-i-1}).$$

This shows that Proposition 10.11 holds for $i+1$. Thus, we obtain Proposition 10.11. Concerning the statement on $\delta_{m_i}^{(\mathbf{Q})}$, the image of δ_{m_i} in $\mathbf{Z}/p^N$ is $\delta_{m_i}^{(\mathbf{Q})}$ by definition. When $i = r$, it is also d_{m_r}, so we have $\mathrm{ord}_p(\delta_{m_r}^{(\mathbf{Q})}) = \mathrm{ord}_p(d_{m_r}) = \mathrm{ord}_p(\det C_0)$. □

We next proceed to prove Theorem 10.8. More explicitly, we prove the following, which certainly implies Theorem 10.8.

Theorem 10.12. *For any $i \in \mathbf{Z}$ such that $0 \leq i \leq s$, we have*

$$\mathrm{ord}_p(\delta_{m_{r+2i}}^{(\mathbf{Q})}) = 2\sum_{k=1}^{s-i} \nu_k.$$

Proof. We prove this theorem also by induction on i. If $i = 0$, this follows from Proposition 10.11. We assume the above property for i. We use a slightly different notation. We put $m' = m_r$, $r_1 = \ell_1$, $r_1' = \ell_2$, $r_2 = \ell_3$, $r_2' = \ell_4, \ldots, r_s = \ell_{2s-1}$, $r_s' = \ell_{2s} = \ell_{a-r}$ (note that $a = 2s + r$).

We first consider $m_{r+2i} = m' r_s' r_s \cdots r_{s-i+1}' r_{s-i+1}$ and

$$\kappa_{r+2i} = \kappa_{m_{r+2i}, r_{s-i}'}.$$

Put $\mathbf{x}_{r+2i} = \Phi_S(\kappa_{r+2i})$ and $\mathbf{y}_{r+2i} = \partial(\kappa_{r+2i})$. We have $M\mathbf{x}_{r+2i} = \mathbf{y}_{r+2i}$ by definition. The $(2s-2i-1)$-th component of $\mathbf{x}_{r+2i}$ is $-\phi_{r_{s-i}}(\kappa_{r+2i})$ by Lemma 7.2(2). We denote by $\phi_{r_{s-i}}(\kappa_{r+2i})^{(\mathbf{Q})}$ the image of $\phi_{r_{s-i}}(\kappa_{r+2i})$ in $\mathbf{Z}/p^N$. The $(2s-2i)$-th component of $\mathbf{y}_{r+2i}$ is $\delta_{m_{r+2i}}$ by Proposition 10.10(2). Considering (45), (46), and looking at the $(2s-2i)$-th component of $M\mathbf{x}_{r+2i} = \mathbf{y}_{r+2i}$, we have

$$\alpha_{s-i}\phi_{r_{s-i}}(\kappa_{r+2i})^{(\mathbf{Q})} = \delta_{m_{r+2i}}^{(\mathbf{Q})}. \tag{57}$$

This together with the hypothesis of induction implies that

$$\begin{aligned} \mathrm{ord}_p(\phi_{r_{s-i}}(\kappa_{r+2i})^{(\mathbf{Q})}) &= \mathrm{ord}_p(\delta_{m_{r+2i}}^{(\mathbf{Q})}) - \mathrm{ord}_p(\alpha_{s-i}) \\ &= 2\left(\sum_{k=1}^{s-i} \nu_k\right) - \nu_{s-i} = 2\left(\sum_{k=1}^{s-i-1} \nu_k\right) + \nu_{s-i}. \end{aligned} \tag{58}$$

Next we consider $m_{r+2i}r_{s-i}$ and

$$\kappa'_{r+2i} = \kappa_{m_{r+2i}r_{s-i},r'_{s-i}}.$$

Put $\mathbf{z}_{r+2i} = \Phi_S(\kappa'_{r+2i})$ and $\mathbf{w}_{r+2i} = \partial(\kappa'_{r+2i})$. As above, we have $M\mathbf{z}_{r+2i} = \mathbf{w}_{r+2i}$. By Proposition 10.10(1), the $(2s-2i-1)$-th component of $\mathbf{w}_{r+2i}$ is $\phi_{r_{s-i}}(\kappa_{m_{r+2i},r'_{s-i}}) = \phi_{r_{s-i}}(\kappa_{r+2i})$. By Proposition 10.10(4) and Lemma 7.2(2), the $(2s-2i)$-th component of $\mathbf{z}_{r+2i}$ is $\delta_{m_{r+2i}r_{s-i}r'_{s-i}} = \delta_{m_{r+2(i+1)}}$. Considering (45), (46), and looking at the $(2s-2i-1)$-th component of $M\mathbf{z}_{r+2i} = \mathbf{w}_{r+2i}$, we have

$$\alpha_{s-i}\delta^{(\mathbf{Q})}_{m_{r+2(i+1)}} = \phi_{r_{s-i}}(\kappa_{r+2i})^{(\mathbf{Q})}. \tag{59}$$

Therefore, we have

$$\begin{aligned} \operatorname{ord}_p(\delta^{(\mathbf{Q})}_{m_{r+2(i+1)}}) &= \operatorname{ord}_p(\phi_{r_{s-i}}(\kappa_{r+2i})^{(\mathbf{Q})}) - \operatorname{ord}_p(\alpha_{s-i}) \\ &= \operatorname{ord}_p(\phi_{r_{s-i}}(\kappa_{r+2i})^{(\mathbf{Q})}) - \nu_{s-i}. \end{aligned} \tag{60}$$

Combining (58) and (60), we get

$$\operatorname{ord}_p(\delta^{(\mathbf{Q})}_{m_{r+2(i+1)}}) = 2\Bigg(\sum_{k=1}^{s-i-1}\nu_k\Bigg).$$

Namely, Theorem 10.12 holds for $i+1$. This completes the proof of Theorem 10.12 and that of Theorem B. □

10.13. **Hypotheses of Theorem B.** In this subsection, we give some remarks on the assumptions of Theorem B. In Theorem B we assumed the nondegeneracy of the p-adic height pairing and the main conjecture, but these assumptions can be replaced by the following conditions on the elements δ_m.

We assume as in Theorem B that E is an elliptic curve defined over $\mathbf{Q}$, p is a good ordinary (odd) prime, p does not divide $\operatorname{Tam}(E)$, the action of $G_{\mathbf{Q}}$ on $T_p(E)$ is surjective, the μ-invariant of $(E, \mathbf{Q}_\infty/\mathbf{Q})$ is zero, and $\#E(\mathbf{F}_p) \not\equiv 0 \pmod p$. We do not assume the main conjecture nor the nondegeneracy of the p-adic height pairing in this subsection. We assume that $\operatorname{Sel}(\mathbf{Q}, E[p^\infty])^\vee$ has the structure as in (47) and take a matrix M as in (45) and (46). In particular, we suppose $r = \operatorname{rank}_{\mathbf{Z}_p}\operatorname{Sel}(\mathbf{Q}, E[p^\infty])^\vee$, $2s = \dim_{\mathbf{F}_p}((\operatorname{Sel}(\mathbf{Q}, E[p^\infty])^\vee)_{\mathrm{tors}} \otimes \mathbf{F}_p)$, and $a = r + 2s$. We put $r' = \operatorname{ord}_{\mathfrak{t}}(\theta_{\mathbf{Q}_\infty})$. We take N such that $N > 2\operatorname{ord}_p(\eta_0)$ as in Subsection 10.9, and take n such that $\omega_n(\mathfrak{t}) \in p^N\mathbf{Z}_p[[\mathfrak{t}]] + \mathfrak{t}^{2r'}\mathbf{Z}_p[[\mathfrak{t}]]$.

Proposition 10.14. *We assume the following two conditions.*

- *(i) There are $\ell_{a-i} \in Q_{a-i}$ $(0 \le i \le a-1)$ satisfying the conditions in the beginning of Subsection 10.9 such that $\delta^{(\mathbf{Q})}_{m_a}$ is a unit where m_a is the product of all ℓ_i as in the beginning of Subsection 10.9.*
- *(ii) For any i such that $0 \le i < r$, there is a prime $\ell'_{a-i} \in Q_{a-i} \cap \mathcal{P}_1((K_{n'})_{[2]})$ such that $\mathfrak{t}^{r'-1}$ divides $\delta_{\ell'_{a-i}}$ but $\mathfrak{t}^{r'}$ does not (where $r' = \operatorname{ord}_{\mathfrak{t}}(\theta_{\mathbf{Q}_\infty})$).*

Then the same conclusion as Theorem B holds.

Proof. Suppose that $r > 0$. For any i such that $0 \leq i < r$, we denote by N_i the matrix which is obtained from M by eliminating the $(a-i)$-th row and the $(a-i)$-th column. By the same method as (56), using $g_{\ell'_{a-i}}$ we have

$$(\det M)\delta_{\ell'_{a-i}} = (\det N_i)\theta_{\mathbf{Q}_n}.$$

We use the notation $d(*)$ from the proof of Proposition 10.11. Then $d(\theta_{\mathbf{Q}_n}) = r'$ and by the condition (ii) we know $d(\delta_{\ell'_{a-i}}) = r'-1$. The above equation implies that $d(\det M/\det N_i) = d(\beta_{r-i}\mathfrak{t}) = 1$, so $\beta_{r-i} \neq 0$. Therefore, we obtain the nondegeneracy of the p-adic height pairing.

For i such that $0 \leq i \leq a = r+2s$, we define δ_{m_i} as in Subsection 10.9. For any element $x \in R_n/p^N = \mathbf{Z}/p^N[\mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})]$, we denote by $x^{(\mathbf{Q})} \in \mathbf{Z}/p^N$ the image of x by the natural map $R_n/p^N \longrightarrow \mathbf{Z}/p^N$ defined by $\gamma \mapsto 1$. We consider $\delta^{(\mathbf{Q})}_{m_{r+2i}}$ for i such that $0 \leq i < s$. By the same method as the proof of Theorem 10.12 (see (57) and (59)), we have

$$\alpha_{s-i}\phi_{r_{s-i}}(\kappa_{r+2i})^{(\mathbf{Q})} = \delta^{(\mathbf{Q})}_{m_{r+2i}} \quad \text{and} \quad \alpha_{s-i}\delta^{(\mathbf{Q})}_{m_{r+2(i+1)}} = \phi_{r_{s-i}}(\kappa_{r+2i})^{(\mathbf{Q})},$$

which implies that

$$\alpha^2_{s-i}\delta^{(\mathbf{Q})}_{m_{r+2(i+1)}} = \delta^{(\mathbf{Q})}_{m_{r+2i}}$$

for any i such that $0 \leq i < s$. Therefore, using $\mathrm{ord}_p(\delta^{(\mathbf{Q})}_{m_a}) = 0$ which is the condition (i), we get

$$\mathrm{ord}_p(\delta^{(\mathbf{Q})}_{m_r}) = 2\sum_{i=1}^{s}\mathrm{ord}_p(\alpha_i) = \mathrm{ord}_p((\mathrm{Sel}(\mathbf{Q}, E[p^\infty])^\vee)_{\mathrm{tors}}). \tag{61}$$

Using the notation from the previous subsections, we obtain $d(\delta_{m_r}) = 0$ and $v(\delta_{m_r}) = 2\sum_{i=1}^{s}\mathrm{ord}_p(\alpha_i) = \mathrm{ord}_p((\det M_r)^{(\mathbf{Q})}) = v(\det M_r)$. Next, suppose $r > 0$. For any i such that $0 \leq i \leq r$, we claim that $d(\delta_{m_{r-i}}) = i$ and $v(\delta_{m_{r-i}}) = v(\det M_{r-i})$. We prove this claim by induction on i. If $i = 0$, we have just seen them. Suppose $i > 0$. We have

$$(\det M_{r-i})\delta_{m_{r-i+1}} = (\det M_{r-i+1})\delta_{m_{r-i}}$$

by the same method as (56). Since we showed that $\beta_j \neq 0$ for all j such that $1 \leq j \leq r$, we have $d(\det M_{r-i}) = i$ and $d(\det M_{r-i+1}) = i-1$. Therefore, if we suppose that our claim holds for $i-1$, then our claim holds for i. Thus we have proved our claim.

Note that $\delta_{m_0} = \theta_{\mathbf{Q}_n}$ and $M_0 = M$. Therefore, we obtain $d(\theta_{\mathbf{Q}_n}) = r$ and $v(\theta_{\mathbf{Q}_n}) = v(\det M)$. This means that $r' = r$ and

$$\mathrm{ord}_p((\theta_{\mathbf{Q}_n}/\mathfrak{t}^r)^{(\mathbf{Q})}) = \mathrm{ord}_p((\det M/\mathfrak{t}^r)^{(\mathbf{Q})}). \tag{62}$$

This was the property from the main conjecture, which we needed for the proof of Theorem B. Hence we get the conclusion. □

10.15. **Modular elements and examples.** Let $f(z) = \sum a_n e^{2\pi niz}$ be the modular form corresponding to E. We consider modular symbols $[\frac{a}{m}] = 2\pi i \int_\infty^{a/m} f(z)dz$ and modular elements

$$\tilde{\theta}_{\mathbf{Q}(\mu_m)} = \sum_{\substack{a=1 \\ (a,m)=1}}^{m} \frac{\mathrm{Re}([\frac{a}{m}])}{\Omega_E^+}\tau_a \in \mathbf{Q}[\mathrm{Gal}(\mathbf{Q}(\mu_m)/\mathbf{Q})]$$

of Mazur and Tate [21] where $\tau_a(\zeta) = \zeta^a$ for $\zeta \in \mu_m$, and $\Omega_E^+ = \int_{E(\mathbf{R})} \omega_E$ is the Néron period. Let K be a real abelian field of conductor m. We define $\tilde{\theta}_K$ to be the image of $\tilde{\theta}_{\mathbf{Q}(\mu_m)}$ in $\mathbf{Q}[\mathrm{Gal}(K/\mathbf{Q})]$. For a positive integer n, let $\mathbf{Q}(n)$ be the maximal p-subextension of $\mathbf{Q}$ in $\mathbf{Q}(\mu_n)$ as in Subsection 3.1. Suppose that m is a squarefree positive integer whose prime divisors ℓ satisfy $\ell \in \mathcal{P}$ and $\ell \equiv 1 \pmod p$. We consider $\mathbf{Q}(mp^n)$ for $n > 1$. Since we assumed the Galois representation on $E[p]$ is surjective, we know $\tilde{\theta}_{\mathbf{Q}(mp^n)} \in \mathbf{Z}_p[\mathrm{Gal}(\mathbf{Q}(mp^n)/\mathbf{Q})]$ (see [35]). We put $R_K = \mathbf{Z}_p[\mathrm{Gal}(K/\mathbf{Q})]$. For any integers d, m such that $d|m$, we denote by $\nu_{\mathbf{Q}(m)/\mathbf{Q}(d)}$ the norm (corestriction) map $R_{\mathbf{Q}(d)} \longrightarrow R_{\mathbf{Q}(m)}$ defined by $\sigma \mapsto \sum \tau$ where for $\sigma \in \mathrm{Gal}(\mathbf{Q}(d)/\mathbf{Q})$, τ runs over elements of $\mathrm{Gal}(\mathbf{Q}(m)/\mathbf{Q})$ such that the restriction of τ to $\mathbf{Q}(d)$ is σ. Let $\alpha \in \mathbf{Z}_p^\times$ be the unit root of $x^2 - a_p x + p = 0$ and put

$$\vartheta_{\mathbf{Q}(mp^n)} = \alpha^{-n}(\tilde{\theta}_{\mathbf{Q}(mp^n)} - \alpha^{-1}\nu_{\mathbf{Q}(mp^n)/\mathbf{Q}(mp^{n-1})}(\tilde{\theta}_{\mathbf{Q}(mp^{n-1})}))$$

as usual. Then $\{\vartheta_{\mathbf{Q}(mp^n)}\}$ is a projective system and we obtain an element $\vartheta_{\mathbf{Q}(m)_\infty} \in \Lambda_{\mathbf{Q}(m)_\infty}$. Let $\theta_{\mathbf{Q}(m)_\infty}$ be the p-adic L-function as in Subsection 2.1 (III). The family $\{\vartheta_{\mathbf{Q}(m)_\infty}\}_m$ and the family $\{\theta_{\mathbf{Q}(m)_\infty}\}_m$ differ only in the Euler factors. We can construct $\theta_{\mathbf{Q}(m)_\infty}$ from $\vartheta_{\mathbf{Q}(d)_\infty}$ by Lemma 3.2. Let $I(\mathbf{Q}(m)_\infty)$ be the ideal of $\Lambda_{\mathbf{Q}(m)_\infty}$ generated by $\nu_{\mathbf{Q}(m)_\infty/\mathbf{Q}(d)_\infty}(\Lambda_{\mathbf{Q}(d)_\infty})$ for all divisors d of m such that $d \neq m$. We have

$$\vartheta_{\mathbf{Q}(m)_\infty} \equiv u\theta_{\mathbf{Q}(m)_\infty} \bmod I(\mathbf{Q}(m)_\infty) \tag{63}$$

for some unit $u \in \Lambda_{\mathbf{Q}(m)_\infty}$ by Lemma 3.2. Let $c_{\mathbf{Q}(m)_\infty/\mathbf{Q}} : \Lambda_{\mathbf{Q}(m)_\infty} \longrightarrow R_{\mathbf{Q}(m)}$ be the natural restriction map. Then we know

$$c_{\mathbf{Q}(m)_\infty/\mathbf{Q}}(\vartheta_{\mathbf{Q}(m)_\infty}) = \left(1 - \frac{\tau_p}{\alpha}\right)\left(1 - \frac{\tau_p^{-1}}{\alpha}\right)\tilde{\theta}_{\mathbf{Q}(m)}$$

(see [21, p.717, equ.(1)]). Since we assumed $a_p \not\equiv 1 \pmod p$, we have $\alpha \not\equiv 1 \pmod p$. Therefore,

$$\tilde{\theta}_{\mathbf{Q}(m)} = vc_{\mathbf{Q}(m)_\infty/\mathbf{Q}}(\theta_{\mathbf{Q}(m)_\infty}) \bmod I(\mathbf{Q}(m)) \tag{64}$$

for some unit $v \in R_{\mathbf{Q}(m)}$ where $I(\mathbf{Q}(m))$ is the ideal generated by $\nu_{\mathbf{Q}(m)_\infty/\mathbf{Q}(d)_\infty}(R_{\mathbf{Q}(d)})$ for all divisors d of m such that $d \neq m$.

Let $\mathcal{K}$ be the set of fields defined in Subsection 2.1. As in Subsection 4.3, for an element $x \in R_{\mathbf{Q}(m)}$, the ideal $I_{i,s}(x)$ of $\mathbf{Z}/p^N$ is defined. Then (64) implies that the ideal $\Theta_i^{(N)}(\mathbf{Q}) \subset \mathbf{Z}/p^N$ is generated by $\bigcup_{\mathbf{Q}(m)\in\mathcal{K}_s} I_{i,s}(\tilde{\theta}_{\mathbf{Q}(m)})$ for all $s > 0$.

Let $\mathcal{N}^{(N)}$ be the set of squarefree numbers defined in Subsection 10.7. For $m = \prod_{i=1}^{q} \ell_i \in \mathcal{N}^{(N)}$, we regard $\tilde{\theta}_{\mathbf{Q}(m)}$ as an element of $\mathbf{Z}_p[S_1, \dots, S_q]/I$ where I is the ideal generated by all $(1+S_i)^{p^{n_{\ell_i}}} - 1$ by the identification of $R_{\mathbf{Q}(m)}$ with $\mathbf{Z}_p[S_1, \dots, S_q]/I$. We denote by $\tilde{\delta}_m^{(\mathbf{Q})}$ the coefficient of $\prod_{i=1}^{q} S_i$ in $\tilde{\theta}_{\mathbf{Q}(m)}$ mod p^N. Explicitly, taking a primitive root ξ_ℓ mod ℓ which corresponds to the generator σ_ℓ of $\mathcal{G}_\ell = \mathrm{Gal}(\mathbf{Q}(\ell)/\mathbf{Q})$ we fixed, we can write

$$\tilde{\delta}_m^{(\mathbf{Q})} = \sum_{\substack{a=1 \\ (a,m)=1}}^{m} \frac{\mathrm{Re}([\frac{a}{m}])}{\Omega_E^+} \Big(\prod_{\ell \mid m} \log_{\mathbf{F}_\ell}(a) \Big) \bmod p^N \ \in \ \mathbf{Z}/p^N \tag{65}$$

where $\log_{\mathbf{F}_\ell}(a) \in \mathbf{Z}$ is the integer such that $0 \le \log_{\mathbf{F}_\ell}(a) \le \ell - 2$ and $\xi_\ell^{\log_{\mathbf{F}_\ell}(a)} \equiv a \pmod{\ell}$.

Then we know by (64) that $\Theta_i^{(N,\delta)}(\mathbf{Q})$ is generated by the elements $\tilde{\delta}_m^{(\mathbf{Q})}$;

$$\Theta_i^{(N,\delta)}(\mathbf{Q}) = \langle \{ \tilde{\delta}_m^{(\mathbf{Q})} \mid \epsilon(m) \le i \text{ and } m \in \mathcal{N}^{(N)} \} \rangle.$$

In this way, we can compute $\Theta_i^{(N,\delta)}(\mathbf{Q})$ and $\Theta_i^{(N)}(\mathbf{Q})$ from the modular elements $\tilde{\theta}_{\mathbf{Q}(m)}$.

Next, we prove (2) in Section 1. Let ϵ be the root number of E, and m a squarefree product of primes in $\mathcal{P}$. Suppose that $\tilde{\theta}_{\mathbf{Q}(m)} \equiv \sum_{i_1+\dots+i_r=i} a_{i_1 \dots i_r} S_1^{i_1} \dots S_r^{i_r} \bmod (p^c, \text{degree } i+1)$ for some $c \in \mathbf{Z}_{>0}$. Then, by the functional equation (1.6.2) in Mazur and Tate [21], we have

$$\begin{aligned} \epsilon(-1)^i \sum_{i_1+\dots+i_r=i} & a_{i_1 \dots i_r} S_1^{i_1} \dots S_r^{i_r} \\ & \equiv \sum_{i_1+\dots+i_r=i} a_{i_1 \dots i_r} S_1^{i_1} \dots S_r^{i_r} \bmod (p^c, I, \text{degree } i+1). \end{aligned}$$

Therefore, if $\epsilon \neq (-1)^i$ and $i_1 + \dots + i_r = i$, we have $a_{i_1 \dots i_r} \equiv 0 \pmod{p^c}$. This implies that for all $j \in \mathbf{Z}_{\ge 0}$, $\Theta_{2j}(\mathbf{Q}) = \Theta_{2j+1}(\mathbf{Q})$ if $\epsilon = 1$, and $\Theta_{2j+1}(\mathbf{Q}) = \Theta_{2j+2}(\mathbf{Q})$ if $\epsilon = -1$.

Examples. Let $E = X_0(11)^{(d)}$ be the quadratic twist of $X_0(11)$ by d. We first take $d = -2315$. We know $L(E,1)/\Omega_E^+ = 81$. The minimal Weierstrass model of E is $y^2 + y = x^3 - x^2 - 55378658x + 287323286343$. We take $p = 3$. Then 3 is a good ordinary prime which is not anomalous, 3 does not divide $\mathrm{Tam}(E)$, the action of $G_{\mathbf{Q}}$ on $T_3(E)$ is surjective, and the μ-invariant of $(E, \mathbf{Q}_\infty/\mathbf{Q})$ is zero. By the main conjecture, the 3-component $Ш(E/\mathbf{Q})[3^\infty]$ of the Tate Shafarevich group is finite, and we know $\#Ш(E/\mathbf{Q})[3^\infty] = 81$. But the main conjecture does not tell whether $Ш(E/\mathbf{Q})[3^\infty] \simeq (\mathbf{Z}/3\mathbf{Z})^{\oplus 4}$ or $(\mathbf{Z}/9\mathbf{Z})^{\oplus 2}$.

Let ℓ be a good reduction prime such that $\ell \equiv 1 \pmod{p^N}$, and consider $\tilde{\theta}_{\mathbf{Q}(\ell)} = \sum_{i \ge 0} a_i^{(\ell)} (\sigma_\ell - 1)^i \in \mathbf{Z}_p[\mathrm{Gal}(\mathbf{Q}(\ell)/\mathbf{Q})]$. By the definition of $I_{i,1}(\tilde{\theta}_{\mathbf{Q}(\ell)})$ and what we explained above, we know that $a_i^{(\ell)} \in \Theta_i^{(N)}(\mathbf{Q})$ for

$i = 0,1,\dots,p-2$, and that $a_i^{(\ell)} \in \Theta_i^{(N-1)}(\mathbf{Q})$ for $i = p-1,\dots,p^2-2$. Therefore, by Corollary 6.5, we have

$$a_i^{(\ell)} \in \mathrm{Fitt}_{i,\mathbf{Z}/p^N}(\mathrm{Sel}(\mathbf{Q}, E[p^N])) \text{ for } i = 0,1,\dots,p-2$$

and

$$a_i^{(\ell)} \in \mathrm{Fitt}_{i,\mathbf{Z}/p^{N-1}}(\mathrm{Sel}(\mathbf{Q}, E[p^{N-1}])) \text{ for } i = p-1,\dots,p^2-2.$$

Explicitly, we can compute $a_1^{(\ell)} = \tilde{\delta}_\ell^{(\mathbf{Q})}$ (see (65)),

$$a_2^{(\ell)} = \sum_{a=1}^{\ell-1} \frac{\mathrm{Re}([\frac{a}{\ell}])}{\Omega_E^+} \frac{\log_{\mathbf{F}_\ell}(a)(\log_{\mathbf{F}_\ell}(a)-1)}{2},$$

... etc.

We go back to $E = X_0(11)^{(-2315)}$. Take $\ell = 163$ (so $N = 4$). We take σ_ℓ which corresponds to a primitive root 2 of $(\mathbf{Z}/163)^\times$. Then we compute $a_1^{(163)} = 74925$ and $a_2^{(163)} = 4621766$ which is prime to 3. Therefore, $\mathrm{Fitt}_{2,\mathbf{Z}_3}(Ш(E/\mathbf{Q})[3^\infty]) = \mathbf{Z}_3$, which implies that $Ш(E/\mathbf{Q})[3^\infty] \simeq (\mathbf{Z}/9\mathbf{Z})^{\oplus 2}$.

For $d = -2435, -2627, -2963$, we also have $L(E,1)/\Omega_E^+ = 81$. Take $p = 3$. Then for each d above, we compute $a_2^{(37)} = 54569/2$, $a_2^{(19)} = 5275/2$, $a_2^{(19)} = 2753/2$, respectively, which are all prime to 3. Therefore, we also get

$$Ш(E/\mathbf{Q})[3^\infty] \simeq (\mathbf{Z}/9\mathbf{Z})^{\oplus 2}$$

for these d. The structure of Selmer groups for more examples is studied in [17].

References

[1] S. Bloch and K. Kato, *L*-functions and Tamagawa numbers of motives, in *The Grothendieck Festschrift, Vol. I*, 333–400, Progr. Math., **86**, Birkhäuser, Boston, Boston, MA. MR1086888 (92g:11063)

[2] J. Coates and B. Perrin-Riou, On p-adic L-functions attached to motives over $\mathbf{Q}$, in *Algebraic number theory*, 23–54, Adv. Stud. Pure Math., **17**, Academic Press, Boston, MA, 1989. MR1097608 (92j:11060a)

[3] J. Coates, R. Sujatha and J.-P. Wintenberger, On the Euler-Poincaré characteristics of finite dimensional p-adic Galois representations, Publ. Math. Inst. Hautes Études Sci. No. **93** (2001), 107–143. MR1863736 (2003d:11078)

[4] J. E. Cremona, *Algorithms for modular elliptic curves*, Cambridge Univ. Press, Cambridge, 1992. MR1201151 (93m:11053)

[5] M. Flach, Selmer groups for the symmetric square of an elliptic curve, PhD thesis, St. John's College (1990).

[6] R. Greenberg, Iwasawa theory for p-adic representations, in *Algebraic number theory*, 97–137, Adv. Stud. Pure Math., **17**, Academic Press, Boston, MA, 1989. MR1097613 (92c:11116)

[7] R. Greenberg, Iwasawa theory for elliptic curves, in *Arithmetic theory of elliptic curves (Cetraro, 1997)*, 51–144, Lecture Notes in Math., 1716, Springer, Berlin. MR1754686 (2002a:11056)

[8] R. Greenberg, Iwasawa theory, projective modules, and modular representations, Mem. Amer. Math. Soc. **211** (2011), no. 992. MR2807791

[9] C. Greither, Computing Fitting ideals of Iwasawa modules, Math. Z. **246** (2004), no. 4, 733–767. MR2045837 (2004k:11170)

[10] Y. Hachimori and K. Matsuno, An analogue of Kida's formula for the Selmer groups of elliptic curves, J. Algebraic Geom. **8** (1999), no. 3, 581–601. MR1689359 (2000c:11086)
[11] K. Kato, p-adic Hodge theory and values of zeta functions of modular forms, Astérisque No. **295** (2004), ix, 117–290. MR2104361 (2006b:11051)
[12] V. A. Kolyvagin, Euler systems, in *The Grothendieck Festschrift, Vol. II*, 435–483, Progr. Math., **87**, Birkhäuser, Boston, Boston, MA, 1990. MR1106906 (92g:11109)
[13] Y. Kubo and Y. Taguchi, A generalization of a theorem of Imai and its applications to Iwasawa theory, Math. Z. **275** (2013), no. 3-4, 1181–1195. MR3127053
[14] M. Kurihara, Iwasawa theory and Fitting ideals, J. Reine Angew. Math. **561** (2003), 39–86. MR1998607 (2004h:11087)
[15] M. Kurihara, On the structure of ideal class groups of CM-fields, Doc. Math. **2003**, Extra Vol., 539–563 (electronic). MR2046607 (2005a:11174)
[16] M. Kurihara, Refined Iwasawa theory and Kolyvagin systems of Gauss sum type, Proc. Lond. Math. Soc. (3) **104** (2012), no. 4, 728–769. MR2908781
[17] M. Kurihara, The structure of Selmer groups for elliptic curves and modular symbols. To appear in Iwasawa theory 2012, edited by T. Bouganis and O. Venjakob (2014). `http://www.math.keio.ac.jp/~kurihara/`
[18] K. Matsuno, An analogue of Kida's formula for the p-adic L-functions of modular elliptic curves, J. Number Theory **84** (2000), no. 1, 80–92. MR1782263 (2001g:11085)
[19] B. Mazur and K. Rubin, Kolyvagin systems, Mem. Amer. Math. Soc. **168** (2004), no. 799. MR2031496 (2005b:11179)
[20] B. Mazur and K. Rubin, Organizing the arithmetic of elliptic curves, Adv. Math. **198** (2005), no. 2, 504–546. MR2183387 (2006h:11059)
[21] B. Mazur and J. Tate, Refined conjectures of the "Birch and Swinnerton-Dyer type", Duke Math. J. **54** (1987), no. 2, 711–750. MR0899413 (88k:11039)
[22] J. Nekovář, On the parity of ranks of Selmer groups. II, C. R. Acad. Sci. Paris Sér. I Math. **332** (2001), no. 2, 99–104. MR1813764 (2002e:11060)
[23] J. Nekovář, Selmer complexes, Astérisque No. 310 (2006). MR2333680 (2009c:11176)
[24] D. G. Northcott, *Finite free resolutions*, Cambridge Univ. Press, Cambridge, 1976. MR0460383 (57 #377)
[25] C. D. Popescu, On the Coates-Sinnott conjecture, Math. Nachr. **282** (2009), no. 10, 1370–1390. MR2571700 (2011c:19010)
[26] K. Rubin, The main conjecture, Appendix to S. Lang, *Cyclotomic fields I and II*. Combined second edition. Texts in Mathematics, 121. Springer-Verlag, New York, 1990. MR1029028 (91c:11001)
[27] K. Rubin, Kolyvagin's system of Gauss sums, in *Arithmetic algebraic geometry (Texel, 1989)*, 309–324, Progr. Math., **89**, Birkhäuser, Boston, Boston, MA. MR1085265 (92a:11121)
[28] K. Rubin, *Euler systems*, Annals of Mathematics Studies, **147**, Princeton Univ. Press, Princeton, NJ, 2000. MR1749177 (2001g:11170)
[29] P. Schneider, Iwasawa L-functions of varieties over algebraic number fields. A first approach, Invent. Math. **71** (1983), no. 2, 251–293. MR0689645 (85d:11063)
[30] P. Schneider, p-adic height pairings. II, Invent. Math. **79** (1985), no. 2, 329–374. MR0778132 (86j:11063)
[31] P. Schneider, Motivic Iwasawa theory, in *Algebraic number theory*, 421–456, Adv. Stud. Pure Math., **17**, Academic Press, Boston, MA, 1989. MR1097626 (92g:11064)
[32] J.-P. Serre, *Corps locaux*, deuxième édition, Publications de l'Université de Nancago, No. VIII. Hermann, Paris, 1968. MR0354618 (50 #7096)
[33] J.-P. Serre, *Cohomologie Galoisienne*, Cours au Collège de France, Paris, 1962–1963. Avec des textes inédits de J. Tate et de Jean-Louis Verdier. Quatrième édition. Lecture Notes in Mathematics, Vol. 5. Springer-Verlag, Berlin-New York, 1973. MR0404227 (53 #8030)

[34] C. Skinner and E. Urban, The Iwasawa main conjecture for GL_2, Invent. Math. **195** (2014), no. 1, 1–277.
[35] G. Stevens, Stickelberger elements and modular parametrizations of elliptic curves, Invent. Math. **98** (1989), no. 1, 75–106. MR1010156 (90m:11089)
[36] K. Wingberg, Duality theorems for Γ-extensions of algebraic number fields, Compositio Math. **55** (1985), no. 3, 333–381. MR0799821 (87e:11125)

Received April 21, 2013; accepted July 22, 2013

Masato Kurihara
Department of Mathematics, Keio University
3-14-1 Hiyoshi, Kohoku-ku, Yokohama, 223-8522, Japan
E-mail: kurihara@math.keio.ac.jp