TOKYO J. MATH.
VOL. 34, NO. 2, 2011

On Stronger Versions of Brumer's Conjecture

Masato KURIHARA

Keio University

Abstract. Let k be a totally real number field and L a CM-field such that L/k is finite and abelian. In this paper, we study a stronger version of Brumer's conjecture that the Stickelberger element times the annihilator of the group of roots of unity in L is in the Fitting ideal of the ideal class group of L, and also study the dual version. We mainly study the Teichmüller character component, and determine the Fitting ideal in a certain case. We will see that these stronger versions hold in a certain case. It is known that the stronger version (SB) does not hold in general. We will prove in this paper that the dual version (DSB) does not hold in general, either.

0. Introduction

0.1. In number theory, it is very important to know the Galois action on the ideal class group of a number field. Concerning the Galois action, an interesting phenomenon is the annihilation of the class group by some analytic element whose origin is the zeta functions in some Galois group ring. Let k be a totally real number field, and L be a CM-field such that L/k is finite and abelian. We fix an odd prime number p and consider the p-component A_L of the ideal class group Cl_L of L. Put $R_L = \mathbf{Z}_p[\mathrm{Gal}(L/k)]$, and regard A_L as an R_L-module.

Let $\mu_{p^\infty}(L)$ be the group of roots of unity with order a power of p in L, and $I_L = \mathrm{Ann}_{R_L}(\mu_{p^\infty}(L))$ the annihilator ideal of $\mu_{p^\infty}(L)$ in R_L. We denote by $\theta_{L/k} \in \mathbf{Q}[\mathrm{Gal}(L/k)]$ the Stickelberger element, which is defined by the values of partial zeta functions (see §2.1). Then by Deligne and Ribet [3] we know $I_L\theta_{L/k} \subset R_L$. Brumer's conjecture claims that $I_L\theta_{L/k} \subset \mathrm{Ann}_{R_L}(A_L)$. We consider the following property (SB) which is stronger than this;

$$\text{(SB)} \qquad I_L\theta_{L/k} \subset \mathrm{Fitt}_{R_L}(A_L)$$

where $\mathrm{Fitt}_{R_L}(A_L)$ is the Fitting ideal of A_L (see §2.2). Since $\mathrm{Fitt}_{R_L}(A_L) \subset \mathrm{Ann}_{R_L}(A_L)$, (SB) is certainly stronger than Brumer's conjecture. The main result in the paper [12] by Miura and the author implies that (SB) holds if $k = \mathbf{Q}$. In the paper [7] by Greither and the author, we showed that (SB) does not hold in general, and the dual version is more natural and likely to hold. Let $(A_L)^\vee$ be the Pontryagin dual of A_L with cogredient Galois action, namely $(\sigma f)(x) = f(\sigma x)$ for $\sigma \in \mathrm{Gal}(L/k)$, $f \in (A_L)^\vee$ and $x \in A_L$. Then the dual version means

$$\text{(DSB)} \qquad I_L\theta_{L/k} \subset \mathrm{Fitt}_{R_L}((A_L)^\vee)\,.$$

Received April 30, 2010

Our explicit example in [7] §3.2 does not satisfy (SB), but satisfies (DSB). In [6], Greither proved a beautiful theorem that the equivariant Tamagawa number conjecture implies (DSB) if $\mu_{p^\infty}(L)$ is cohomologically trivial. Concerning the exposition of Brumer's conjecture and the Fitting ideals, see Greither [4].

In this paper, we prove the existence of number fields for which neither (DSB) nor (SB) holds (see Corollary 0.5). (Under the assumptions of Corollary 0.5, $\mu_{p^\infty}(L)$ is not cohomologically trivial.)

We study the Iwasawa theoretic version of (DSB). Let L be as above and L_∞/L be the cyclotomic $\mathbf{Z}_p$-extension. We define

$$A_{L_\infty} = \varinjlim A_{L_n}$$

where L_n is the intermediate field such that $[L_n : L] = p^n$ for $n > 0$. Put $\Lambda_{L_\infty} = \mathbf{Z}_p[[\mathrm{Gal}(L_\infty/k)]]$. We study the Pontryagin dual $(A_{L_\infty})^\vee$ which is a finitely generated torsion Λ_{L_∞}-module. We define $I_{L_\infty} = \mathrm{Ann}_{\Lambda_{L_\infty}}(\mu_{p^\infty}(L_\infty)) \subset \Lambda_{L_\infty}$. By Deligne and Ribet [3], there is a unique element $\theta_{L_\infty/k}$ in the total quotient ring of Λ_{L_∞}, which is the "projective limit" of $\theta_{L_n/k}$ (more precisely, see §2.1).

We study the Iwasawa theoretic version

$$\text{(IDSB)} \qquad I_{L_\infty}\theta_{L_\infty/k} \subset \mathrm{Fitt}_{\Lambda_{L_\infty}}((A_{L_\infty})^\vee)$$

of (DSB). Theorem A.5 in [11] implies that (IDSB) holds outside the Teichmüller character component if we assume the Leopoldt conjecture and the vanishing of the Iwasawa μ-invariant of L. In particular, if $\mu_p \not\subset L$ where μ_p is the group of p-th roots of unity, (IDSB) is true under the above assumptions. In this paper, we mainly study the case $\mu_p \subset L$.

We assume that $L \cap k_\infty = k$ where k_∞ is the cyclotomic $\mathbf{Z}_p$-extension of k. We denote by $\Gamma(L/k)$ the p-component of $\mathrm{Gal}(L/k)$, so $\mathrm{Gal}(L/k) = \Gamma(L/k) \times \Delta$ for some abelian group Δ with $p \nmid \#\Delta$.

Suppose at first that $\Gamma(L/k) \simeq \mathbf{Z}/p\mathbf{Z}$. If $\Gamma(L/k)$ is cyclic, by Theorem 3, Proposition 4 in Greither [5] and Corollary A. 13 in [7], we know that (IDSB) holds, assuming the vanishing of the μ-invariant. Moreover, $\mathrm{Fitt}_{\Lambda_{L_\infty}}((A_{L_\infty})^\vee)$ is determined outside the component of the Teichmüller character by Theorem 3 in Greither [5] and Corollary A. 13 in [7]. In this paper, we determine the Teichmüller character component of the Fitting ideal in the case that $\Gamma(L/k) \simeq \mathbf{Z}/p\mathbf{Z}$.

Suppose that $\mu_p \subset L$. We denote by K the subfield of L such that $\Gamma(L/k) = \mathrm{Gal}(L/K)$, so $[K : k]$ is prime to p. Let ω be the Teichmüller character giving the action of $\mathrm{Gal}(K/k)$ on μ_p. Since $[K : k]$ is prime to p, A_{L_∞} is decomposed into $A_{L_\infty} = \bigoplus_\chi A_{L_\infty}^\chi$ where χ runs over all equivalence classes of $\overline{\mathbf{Q}}_p^\times$-valued characters of $\mathrm{Gal}(K/k)$ (see §1.2). In particular, we know that determining $\mathrm{Fitt}_{\Lambda_{L_\infty}}((A_{L_\infty})^\vee)$ is equivalent to determining $\mathrm{Fitt}_{\Lambda_{L_\infty}^\chi}((A_{L_\infty}^\chi)^\vee)$ for all characters χ of $\mathrm{Gal}(K/k)$ (for the definition of the χ-components $A_{L_\infty}^\chi$, $\Lambda_{L_\infty}^\chi$, see §1.2). For any odd character χ such that $\chi \neq \omega$, we know $\mathrm{Fitt}_{\Lambda_{L_\infty}^\chi}((A_{L_\infty}^\chi)^\vee)$ is determined (see (2.3.2)). We study the ω-component. To do this, we may assume $K = k(\mu_p)$ (see §2.2).

We take a generator γ of $\mathrm{Gal}(L_\infty/L) = \mathrm{Gal}(K_\infty/K)$. We denote the cyclotomic character by $\kappa : \mathrm{Gal}(L_\infty/k) \longrightarrow \mathbf{Z}_p^\times$. The cyclotomic character of $\mathrm{Gal}(K_\infty/k)$ is also denoted by κ. Suppose that $\mathrm{Gal}(L_\infty/K_\infty)$ is generated by σ. Then I_{L_∞} is generated by $\gamma - \kappa(\gamma)$ and $\sigma - 1$. In the following, we suppose that L_0/k is a finite abelian p-extension (so L_0 is also totally real) and $L = L_0(\mu_p)$. We will state our theorems without explaining all notations.

THEOREM 0.1. *Suppose that L_0/k is a cyclic extension of degree p with $L_0 \cap k_\infty = k$. We put $L = L_0(\mu_p)$, and assume that the Iwasawa μ-invariant of L_∞/L vanishes, namely $\mu((A_{L_\infty})^\vee) = 0$. We denote by S the set of primes of k which are prime to p and which are ramified in L.*

(1) *Suppose at first that S is not empty. Then we have*

$$\begin{aligned}&\mathrm{Fitt}_{\Lambda^\omega_{L_\infty}}((A^\omega_{L_\infty})^\vee)\\ &\quad = \left(\sum_{\mathfrak{l}\in S}\left(\prod_{\substack{\mathfrak{l}'\neq\mathfrak{l}\\ \mathfrak{l}'\in S}}\left(1, \nu\left(\frac{1}{1-\kappa(\varphi_{\mathfrak{l}'})\varphi_{\mathfrak{l}'}^{-1}}\right)\right)\right)\left(1, \nu\left(\frac{\gamma-\kappa(\gamma)}{1-\kappa(\varphi_{\mathfrak{l}})\varphi_{\mathfrak{l}}^{-1}}\right)\right)\vartheta_{L_\infty/k}\right)^\omega .\end{aligned}$$

Here, the right hand side is defined in (2.3.8); *ν is the map defined in* §2.1, *$\varphi_{\mathfrak{l}}$ is the Frobenius of $\mathfrak{l}$ in* $\mathrm{Gal}(K_\infty/k)$, *and $\vartheta_{L_\infty/k}$ is a modified Stickelberger element of Greither, which is defined in* (2.3.4), *and which is described by using $\theta_{L_\infty/k}$ and $\theta_{K_\infty/k}$ (see* (2.3.7)). *In this case, we have*

$$I_{L_\infty}\theta_{L_\infty/k} \subsetneq \mathrm{Fitt}_{\Lambda_{L_\infty}}((A_{L_\infty})^\vee) .$$

(2) *Suppose that $S = \phi$, namely L/k is unramified outside p. Then we have*

$$\mathrm{Fitt}_{\Lambda^\omega_{L_\infty}}((A^\omega_{L_\infty})^\vee) = (I_{L_\infty}\theta_{L_\infty/k})^\omega .$$

We define the standard Iwasawa module X_{L_∞} by

$$X_{L_\infty} = \varprojlim A_{L_n}$$

where the limit is taken with respect to the norm maps. We consider the following property

$$\text{(ISB)} \qquad I_{L_\infty}\theta_{L_\infty/k} \subset \mathrm{Fitt}_{\Lambda_{L_\infty}}(X_{L_\infty}) .$$

In general, (ISB) does not hold (see [7] Theorem 1.1 and also §3.3). Suppose that L/k is as in Theorem 0.1. Then we encounter a phenomenon that (IDSB) holds, but (ISB) does not. We will explain in §3.3 that X_{L_∞} is not isomorphic to $(A_{L_\infty})^\vee$ as a $\mathbf{Z}_p[\Gamma(L/k)]$-module, in general (see (3.3.1) and (3.3.2)).

0.2. We summarize here some *affirmative results* for (SB) and (DSB). As we mentioned above, if we assume the μ-invariant of L_∞/L vanishes and $\Gamma(L/k)$ is cyclic, (IDSB) holds by Theorem 3, Proposition 4 in Greither [5] and Corollary A. 13 in [7].

By the standard descent technique, we obtain the following results.

COROLLARY 0.2. *Suppose that L/k is a finite abelian extension such that $\Gamma(L/k)$ is cyclic and $L \cap K_\infty = K$. We assume that the Iwasawa μ-invariant of L_∞/L is zero.*

(1) *Suppose that n is sufficiently large such that all the primes above p of k are ramified in the n-th layer L_n of the cyclotomic $\mathbf{Z}_p$-extension L_∞/L. Then* (DSB) *holds for L_n/k.*

(2) *For any prime $\mathfrak{p}$ of k above p, we assume at least one of the following*;

(i) *no prime above $\mathfrak{p}$ splits in L/L^+, or*

(ii) *$\mathfrak{p}$ is ramified in L.*

Then both (DB) *and* (DSB) *hold for L/k.*

This corollary will be proved in §3.4.

0.3. Next, we consider the case that $\Gamma(L/k)$ is *not cyclic*, and will obtain *negative results* for (IDSB) and (DSB). As in Theorem 0.1, we study the ω-component.

THEOREM 0.3. *Suppose that L_0/k is a finite abelian p-extension such that $L_0 \cap k_\infty = k$ and* $\mathrm{Gal}(L_0/k)$ *is not cyclic. We put $L = L_0(\mu_p)$, and assume that L/k is unramified outside p. Then we have*

$$(\gamma - \kappa(\gamma))\theta_{L_\infty/k} \notin \mathrm{Fitt}_{\Lambda_{L_\infty}}((A_{L_\infty})^\vee)\,.$$

In particular, (IDSB) *does not hold, namely*

$$I_{L_\infty}\theta_{L_\infty/k} \not\subset \mathrm{Fitt}_{\Lambda_{L_\infty}}((A_{L_\infty})^\vee)\,.$$

REMARK 0.4. (1) There are many examples of (k, L) satisfying the conditions of Theorem 0.3. For example, if $\dim_{\mathbf{F}_p} A_k/pA_k \geq 2$, there is an unramified extension L_0/k with non-cyclic Galois group of order a power of p, so $L = L_0(\mu_p)$ satisfies the condition. (We give an explicit example in Example 0.6 such that L_0/k is ramified.)

(2) In the setting of Theorems 0.1 and 0.3, $\mu_{p^\infty}(L)$ is not cohomologically trivial because $\Gamma(L/k) = \mathrm{Gal}(L_0/k)$ acts on $\mu_{p^\infty}(L)$ trivially, which implies $\hat{H}^0(\Gamma(L/k), \mu_{p^\infty}(L)) \neq 0$.

(3) If $k = \mathbf{Q}$, there is no L_0 as in Theorem 0.1 (2) or Theorem 0.3. In fact, if $L_0 \cap \mathbf{Q}_\infty = \mathbf{Q}$ and $L_0/\mathbf{Q}$ is a finite abelian p-extension which is unramified outside p, we have $L_0 = \mathbf{Q}$.

COROLLARY 0.5. (1) *Let L_0/k be a finite abelian p-extension which is unramified outside p such that $L_0 \cap k_\infty = k$ and* $\mathrm{Gal}(L_0/k)$ *is not cyclic. Then, for sufficiently large n,* (DSB) *does not hold for $L_0(\mu_{p^n})/k$.*

(2) *Suppose that L_0 is as above. We denote by P_{p,k_∞} the set of primes of k_∞ above p, and assume that*

$$\#\{\mathfrak{P} \in P_{p,k_\infty} \mid \mathfrak{P} \text{ splits completely in } k(\mu_{p^\infty}) \text{ and ramified in } L_0(\mu_{p^\infty})\} \geq 2\,.$$

Then, for sufficiently large n, neither (SB) *nor* (DSB) *holds for $L_0(\mu_{p^n})/k$.*

We will prove Theorems 0.1, 0.3 and Corollary 0.5 in §3.

EXAMPLE 0.6. Let F_1 be the minimal splitting field of $x^3 - 39x - 16 = 0$. We know $\sqrt{79} \in F_1$ and $F_1/\mathbf{Q}(\sqrt{79})$ is unramified everywhere. Let F_2 be the minimal splitting field of $x^3 - 6x - 3 = 0$. We know $\sqrt{69} \in F_2$ and $F_2/\mathbf{Q}(\sqrt{69})$ is unramified outside 3 and ramified at the prime above 3. Let $F_{2,\infty}/F_2$ be the cyclotomic $\mathbf{Z}_3$-extension. Since the class number of $\mathbf{Q}(\sqrt{69})$ is 1, the prime above 3 is totally ramified in $F_{2,\infty}/\mathbf{Q}(\sqrt{69})$. We put $k = \mathbf{Q}(\sqrt{69}, \sqrt{79})$ and take $p = 3$. There are two primes $\mathfrak{p}_1$, $\mathfrak{p}_2$ of k above 3, and both of them are totally ramified in k_∞. We denote by $\mathfrak{P}_1$ (resp. $\mathfrak{P}_2$) the prime of k_∞ above $\mathfrak{p}_1$ (resp. $\mathfrak{p}_2$). Since $\mathfrak{p}_1$ and $\mathfrak{p}_2$ split in $k(\mu_3) = k(\sqrt{-3}) = k(\sqrt{-23})$, $\mathfrak{P}_1$ and $\mathfrak{P}_2$ split in $k_\infty(\mu_3)$. Put $L_0 = F_1F_2$. So $\mathrm{Gal}(L_0/k) \simeq \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$. Since $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are totally ramified in $F_{2,\infty}k/k$, $\mathfrak{P}_1$ and $\mathfrak{P}_2$ are totally ramified in $F_{2,\infty}k/k_\infty$. Thus, L_0/k satisfies all the conditions of Corollary 0.5. Therefore, neither (SB) nor (DSB) holds for $L = L_0(\mu_{p^n})$ with $n \gg 0$. We can construct many examples in this way.

The author would like to thank heartily C. Greither for the discussion on the subjects in this paper, and for his useful comments by which the author could improve Theorem 0.3. (In the first draft, only the case $\Gamma(L/k) = \mathbf{Z}/p\mathbf{Z} \oplus \mathbf{Z}/p\mathbf{Z}$ was studied in Theorem 0.3.)

NOTATION. Throughout this paper, we fix an odd prime number p. For any number field F, we denote by A_F the p-component of the ideal class group of F. The cyclotomic $\mathbf{Z}_p$-extension of F is denoted by F_∞, and we define $A_{F_\infty} = \varinjlim A_{F_n}$ where F_n is the n-th layer of F_∞/F for $n > 0$. We denote by P_F the set of all finite primes of F, and by $P_{p,F}$ the subset of P_F consisting of primes above p. We define $P'_F = P_F \setminus P_{p,F}$. For a group G and a G-module M, we denote by M^G the G-invariant part of M (the maximal subgroup of M on which G acts trivially), and by M_G the G-coinvariant of M (the maximal quotient of M on which G acts trivially).

1. Computation of some Tate cohomology groups

1.1. In this section we suppose that k is a totally real base field, and K and L are CM-fields such that $k \subset K \subset L$ and that L/k is a finite abelian extension. We assume that L/K is a p-extension.

Put $G = \mathrm{Gal}(L/K)$. In this section we study the p-component A_L of the ideal class group of L, especially the minus part A_L^- on which the complex conjugation acts as -1. Throughout this paper, for any module M on which the complex conjugation ρ acts, we define the minus part M^- by $M^- = \{x \in M \mid \rho(x) = -x\}$. We compute the Tate cohomology groups $\hat{H}^q(G, A_{L_\infty}^-) = \hat{H}^q(G, A_{L_\infty})^-$ (cf. Serre [15] Chap. 8).

By Lemma 5.1 (2) in [10], we have an exact sequence

$$\hat{H}^0(G, E_L)^- \longrightarrow \hat{H}^0\Big(G, \prod_{w \in P_L} E_{L_w}\Big)^- \longrightarrow \hat{H}^{-1}(G, A_L)^-$$

$$\longrightarrow H^1(G, E_L)^- \longrightarrow H^1\Big(G, \prod_{w\in P_L} E_{L_w}\Big)^- \longrightarrow \hat{H}^0(G, A_L)^-$$
$$\longrightarrow H^2(G, E_L)^- \longrightarrow H^2\Big(G, \prod_{w\in P_L} E_{L_w}\Big)^-$$

where E_L (resp. E_{L_w}) is the unit group of L (resp. of the local field L_w), and P_L is the set of all finite primes of L as in Notation. For each prime $v \in P_K$, we denote by G_v the decomposition subgroup of G at v. We know $\hat{H}^q(G, \prod_{w\in P_L} E_{L_w}) = \bigoplus_{v\in P_K} \hat{H}^q(G_v, E_{L_w})$ where in the right hand side we fix a prime w of L above v for $v \in P_K$ (note that $\hat{H}^q(G_v, E_{L_w}) = 0$ if v is unramified in L). More concretely, we have $\hat{H}^0(G_v, E_{L_w}) = I_v$ by local class field theory where I_v is the inertia subgroup of G at v. Since $H^1(G_v, L_w^\times) = 0$, from the exact sequence $0 \longrightarrow E_{L_w} \longrightarrow L_w^\times \longrightarrow \mathbf{Z} \longrightarrow 0$ we have $H^1(G_v, E_{L_w}) = \mathbf{Z}/e_v\mathbf{Z}$ where e_v is the ramification index of v in L/K, and $H^2(G_v, E_{L_w}) \subset \mathrm{Br}(K_v)[p^\infty]$ where $\mathrm{Br}(K_v)[p^\infty]$ is the subgroup of the Brauer group of K_v consisting of elements with order a power of p.

Consider the cyclotomic $\mathbf{Z}_p$-extensions K_∞/K, L_∞/L, and the n-th layers K_n, L_n. We assume that $L \cap K_\infty = K$. By the above descriptions, we have

$$\varinjlim \bigoplus_{v\in P_{K_n}} \hat{H}^0(G_v, E_{L_{n,w}}) = \varinjlim \bigoplus_{v\in P_{K_n}} H^2(G_v, E_{L_{n,w}}) = 0\,.$$

Suppose that w_{n+1} is a prime of L_{n+1} and w_n, v_{n+1}, v_n are the primes of L_n, K_{n+1}, K_n below w_{n+1}, respectively. Then the natural map $H^1(G_{v_n}, E_{L_{w_n}}) = \mathbf{Z}/e_{v_n}\mathbf{Z} \longrightarrow H^1(G_{v_{n+1}}, E_{L_{w_{n+1}}}) = \mathbf{Z}/e_{v_{n+1}}\mathbf{Z}$ is the multiplication by $e_{w_{n+1,n}}$ which is the ramification index of w_n in L_{n+1}/L_n. Each prime above p is totally ramified in L_∞/L_n for sufficiently large n, and a prime v which is not above p is unramified in L_∞/L. It follows that

$$\varinjlim \bigoplus_{v\in P_{K_n}} H^1(G_v, E_{L_{n,w}}) = \bigoplus_{v\in P'_{K_\infty}} \mathbf{Z}/e_v\mathbf{Z}$$

where P'_{K_∞} denotes the set of all finite primes of K_∞ which are prime to p (as in Notation), and e_v is the ramification index of v in L_∞/K_∞. We define $A_{L_\infty} = \varinjlim A_{L_n}$ as in Notation, and $E_{L_\infty} = \varinjlim E_{L_n}$. Taking the direct limit of the above exact sequence, we obtain the following lemma.

LEMMA 1.1. *We have an exact sequence*

$$0 \longrightarrow \hat{H}^{-1}(G, A_{L_\infty})^- \longrightarrow H^1(G, E_{L_\infty})^- \longrightarrow \Big(\bigoplus_{v\in P'_{K_\infty}} \mathbf{Z}/e_v\mathbf{Z}\Big)^-$$
$$\longrightarrow \hat{H}^0(G, A_{L_\infty})^- \longrightarrow H^2(G, E_{L_\infty})^- \longrightarrow 0\,.$$

1.2. Now, we assume that $[K : k]$ is prime to p. Hence $\Gamma(L/k) = G$ in the terminology of §0. The group ring $\mathbf{Z}_p[\mathrm{Gal}(K/k)]$ is a product of discrete valuation rings. More explicitly, it is described as follows. For two $\overline{\mathbf{Q}}_p^\times$-valued characters χ_1 and χ_2 of $\mathrm{Gal}(K/k)$, we say χ_1 and χ_2 are $\mathbf{Q}_p$-conjugate if $\sigma\chi_1 = \chi_2$ for some $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$. For a $\overline{\mathbf{Q}}_p^\times$-valued character χ of $\mathrm{Gal}(K/k)$, we put $O_\chi = \mathbf{Z}_p[\mathrm{Image}\,\chi]$. We regard O_χ as a $\mathbf{Z}_p[\mathrm{Gal}(K/k)]$ module by $\sigma \cdot x = \chi(\sigma)x$ for any $\sigma \in \mathrm{Gal}(K/k)$. We have

$$\mathbf{Z}_p[\mathrm{Gal}(K/k)] = \bigoplus_\chi O_\chi \tag{1.2.1}$$

where the sum is taken over the equivalence classes of $\overline{\mathbf{Q}}_p^\times$-valued characters of $\mathrm{Gal}(K/k)$ (we choose a character χ from each equivalence class).

For any $\mathbf{Z}_p[\mathrm{Gal}(K/k)]$-module M, we define $M^\chi = M \otimes_{\mathbf{Z}_p[\mathrm{Gal}(K/k)]} O_\chi$. Note that M^χ is a direct summand of M because (1.2.1) implies $M = \bigoplus_\chi M^\chi$. We put $\Lambda_{K_\infty} = \mathbf{Z}_p[[\mathrm{Gal}(K_\infty/k)]]$ and $\Lambda_{L_\infty} = \mathbf{Z}_p[[\mathrm{Gal}(L_\infty/k)]]$. Since $\mathrm{Gal}(K/k)$ is a direct summand of $\mathrm{Gal}(L_\infty/k)$, any Λ_{L_∞}-module M is naturally a $\mathbf{Z}_p[\mathrm{Gal}(K/k)]$-module and M^χ is defined. For such M, M^χ can be written as $M^\chi = M \otimes_{\mathbf{Z}_p[\mathrm{Gal}(K/k)]} O_\chi = M \otimes_{\Lambda_{L_\infty}} O_\chi[[\mathrm{Gal}(L_\infty/K)]]$. In the same way, for a Λ_{K_∞}-module M, $M^\chi = M \otimes_{\mathbf{Z}_p[\mathrm{Gal}(K/k)]} O_\chi = M \otimes_{\Lambda_{K_\infty}} O_\chi[[\mathrm{Gal}(K_\infty/K)]]$.

When K contains a primitive p-th root of unity, we denote by ω the Teichmüller character which gives the action on μ_p.

PROPOSITION 1.2. (1) *Suppose that χ is an odd character such that $\chi \neq \omega$. Then we have*

$$\hat{H}^{-1}(G, A_{L_\infty}^\chi) = 0 \quad \text{and} \quad \hat{H}^0(G, A_{L_\infty}^\chi) = \Big(\bigoplus_{v \in P'_{K_\infty}} \mathbf{Z}/e_v\mathbf{Z}\Big)^\chi .$$

(2) *Suppose that $K = k(\mu_p)$ and $[L : K] = p$. Let P'_k be the set of all finite primes of k which are prime to p as in Notation, and put*

$$S = \{\mathfrak{l} \in P'_k \mid \mathfrak{l} \text{ is ramified in } L/k\}.$$

If S is not empty, we have

$$\hat{H}^{-1}(G, A_{L_\infty}^\omega) = 0 \quad \text{and} \quad \hat{H}^0(G, A_{L_\infty}^\omega) = \mathrm{Coker}\Big(\mu_p \longrightarrow \bigoplus_{\mathfrak{L} \in S_{k_\infty}} \mu_p\Big)$$

where μ_p is the group of p-th roots of unity, the map is the diagonal map, and S_{k_∞} is the set of primes of k_∞ which are above S.

(3) *Next, we assume $K = k(\mu_p)$ and L/K is a (general abelian) p-extension which is*

unramified outside p (*namely*, *the set* S *defined above is empty*). *Then we have*

$$\hat{H}^{-1}(G, A^{\omega}_{L_\infty}) \simeq G^{\vee}(1) \quad \textit{and} \quad \hat{H}^{0}(G, A^{\omega}_{L_\infty}) \simeq \left(\bigwedge^{2} G\right)^{\vee}(1)$$

where $G^{\vee}$, $(\bigwedge^2 G)^{\vee}$ *are the Pontryagin duals of* G, $\bigwedge^2 G$ (*the second exterior power of* G), *and* (1) *is the Tate twist. In particular*, $\hat{H}^0(G, A^{\omega}_{L_\infty}) = 0$ *if and only if* G *is cyclic.*

PROOF. First of all, since $\mathrm{Gal}(K/k)$ acts on G trivially, we have $\hat{H}^q(G, M)^{\chi} = \hat{H}^q(G, M^{\chi})$ for any χ and any Λ_{L_∞}-module M.

(1) Since $\chi \neq \omega$, we know $(E_{L_\infty})^{\chi} = 0$. This implies that $H^q(G, E_{L_\infty})^{\chi} = H^q(G, (E_{L_\infty})^{\chi}) = 0$. Therefore, Lemma 1.1 implies the conclusion of (1).

(2) Since $\mu_p \subset K$, we know $(E_{L_\infty})^{\omega} = \mu_{p^\infty} = \mathbf{Q}_p/\mathbf{Z}_p(1)$. Therefore, using $G = \mathbf{Z}/p\mathbf{Z}$, we have $H^1(G, E_{L_\infty})^{\omega} = H^1(G, \mathbf{Q}_p/\mathbf{Z}_p(1)) = \mu_p$ and

$$H^2(G, E_{L_\infty})^{\omega} = H^2(G, \mathbf{Q}_p/\mathbf{Z}_p)(1) = \hat{H}^0(G, \mathbf{Q}_p/\mathbf{Z}_p)(1) = 0\,.$$

Suppose that $\mathfrak{l}$ is in S. Since $\mathfrak{l}$ is unramified in $K = k(\mu_p)$, $\mathfrak{l} \in S$ implies that the inertia group of $\mathfrak{l}$ in $\mathrm{Gal}(L/k)$ is of order divisible by p. Hence $N(\mathfrak{l}) \equiv 1 \pmod{p}$ where $N(\mathfrak{l})$ is the norm of $\mathfrak{l}$. This implies that $\mathfrak{l}$ splits completely in $K = k(\mu_p)$. Let $\mathfrak{L}$ be a prime of k_∞ above $\mathfrak{l}$, and let v be a prime of K_∞ above $\mathfrak{L}$. Then v is ramified in L_∞ and $[L_\infty : K_\infty] = p$, so v is totally ramified in L_∞. Hence $G = G_v$ (where G_v is the decomposition group of G at v). Since $\mathfrak{l}$ splits completely in K, $\mathfrak{L}$ splits completely in K_∞ and we have

$$\left(\bigoplus_{v|\mathfrak{L}} H^1(G_v, \mathbf{Q}_p/\mathbf{Z}_p(1))\right)^{\omega} = \left(\bigoplus_{v|\mathfrak{L}} \mu_p\right)^{\omega} = \mu_p\,.$$

It follows that $(\bigoplus_{v \in P'_{K_\infty}} H^1(G_v, E_{L_{\infty,w}}))^{\omega} = \bigoplus_{\mathfrak{L} \in S_{k_\infty}} \mu_p$.

Therefore, the natural map $H^1(G, E_{L_\infty})^{\omega} \longrightarrow (\bigoplus_{v \in P'_{K_\infty}} H^1(G_v, E_{L_{\infty,w}}))^{\omega}$ is the diagonal map $\mu_p \longrightarrow \bigoplus_{\mathfrak{L} \in S_{k_\infty}} \mu_p$. In particular, it is injective because $S \neq \phi$. Thus, by Lemma 1.1 we obtain $\hat{H}^{-1}(G, A^{\omega}_{L_\infty}) = 0$, and $\hat{H}^0(G, A^{\omega}_{L_\infty}) = \mathrm{Coker}(\mu_p \longrightarrow \bigoplus_{\mathfrak{L} \in S_{k_\infty}} \mu_p)$.

(3) In this case, since $\bigoplus_{v \in P'_{K_\infty}} \mathbf{Z}/e_v\mathbf{Z} = 0$, using Lemma 1.1, we have

$$\hat{H}^{-1}(G, A^{\omega}_{L_\infty}) = H^1(G, E_{L_\infty})^{\omega} = H^1(G, \mathbf{Q}_p/\mathbf{Z}_p(1)) = G^{\vee}(1)$$

and

$$\hat{H}^0(G, A^{\omega}_{L_\infty}) = H^2(G, E_{L_\infty})^{\omega} = H^2(G, \mathbf{Q}_p/\mathbf{Z}_p)(1)\,.$$

Therefore, the next lemma implies the conclusion. This completes the proof of Proposition 1.2.

LEMMA 1.3. *Suppose that G is an abelian p-group. Then $H^2(G, \mathbf{Q}_p/\mathbf{Z}_p)$ is isomorphic to* $\mathrm{Hom}(\bigwedge^2 G, \mathbf{Q}_p/\mathbf{Z}_p)$. *In particular, if G is not cyclic, we have $H^2(G, \mathbf{Q}_p/\mathbf{Z}_p) \neq 0$.*

PROOF. In fact, by the duality Proposition 7.1 in Chap. VI in [1] (or the universal coefficient sequence (cf. page 60 in Chap. III in [1])), we have

$$H^2(G, \mathbf{Q}_p/\mathbf{Z}_p) \simeq \mathrm{Hom}(H_2(G, \mathbf{Z}), \mathbf{Q}_p/\mathbf{Z}_p)\,.$$

Since G is abelian, we know $H_2(G, \mathbf{Z}) = \bigwedge^2 G$ (Theorem 6.4 (iii) in Chap. V in [1]). This completes the proof of Lemma 1.3.

2. Stickelberger elements and Fitting ideals

2.1. Let k be a totally real number field and L be a CM-field such that L/k is finite and abelian. The Stickelberger element $\theta_{L/k}$ is defined by

$$\theta_{L/k} = \sum_{\sigma \in \mathrm{Gal}(L/k)} \zeta(0, \sigma)\sigma^{-1} \in \mathbf{Q}[\mathrm{Gal}(L/k)]$$

where $\zeta(s, \sigma) = \sum_{(\frac{L/k}{\mathfrak{a}})=\sigma} N(\mathfrak{a})^{-s}$ is the partial zeta function ($\mathfrak{a}$ runs over integral ideals which are prime to the discriminant of L/k).

Let L_∞/L be the cyclotomic $\mathbf{Z}_p$-extension and $\Lambda_{L_\infty} = \mathbf{Z}_p[[\mathrm{Gal}(L_\infty/k)]]$. We denote by $\kappa : \mathrm{Gal}(L_\infty/k) \longrightarrow \mathbf{Z}_p^\times$ the cyclotomic character. By Deligne and Ribet ([3]), we know that there is a unique element $\theta_{L_\infty/k}$ in the total quotient ring of Λ_{L_∞} satisfying the following property. For any $\sigma \in \mathrm{Gal}(L_\infty/k)$, $(\sigma - \kappa(\sigma))\theta_{L_\infty/k}$ is in Λ_{L_∞} and is a projective limit of $(\sigma - \kappa(\sigma))\theta_{L_n/k} \in \mathbf{Z}_p[\mathrm{Gal}(L_n/k)]$ for $n \gg 0$. We denote by

$$\tilde{\kappa} : \Lambda_{L_\infty} \longrightarrow \Lambda_{L_\infty} \tag{2.1.1}$$

the ring homomorphism induced by $\tilde{\kappa}(\sigma) = \kappa(\sigma)\sigma$ for all $\sigma \in \mathrm{Gal}(L_\infty/k)$. Clearly, $\tilde{\kappa}$ is bijective. We extend $\tilde{\kappa}$ to the total quotient ring of Λ_{L_∞}. Then $\tilde{\kappa}(\theta_{L_\infty/k})$ is a pseudo-measure in the sense of Serre ([16]), and is the p-adic L-function of Deligne and Ribet.

Suppose that K is the intermediate field of L/k such that L/K is a p-extension and $[K : k]$ is prime to p. Put $\Lambda_{K_\infty} = \mathbf{Z}_p[[\mathrm{Gal}(K_\infty/k)]]$ and $G = \mathrm{Gal}(L/K)$. We assume that $L \cap k_\infty = k$. Then we have $\Lambda_{L_\infty} = \Lambda_{K_\infty}[G]$. We regard Λ_{L_∞} as a Λ_{K_∞}-module by this identification. We will use two maps c and ν. The ring homomorphism

$$c : \Lambda_{L_\infty} \longrightarrow \Lambda_{K_\infty}$$

is defined by the restriction $\sigma \mapsto \sigma_{|K_\infty}$ for $\sigma \in \mathrm{Gal}(L_\infty/k)$. The Λ_{K_∞}-homomorphism

$$\nu : \Lambda_{K_\infty} \longrightarrow \Lambda_{L_\infty}$$

is defined by $\sigma \mapsto \Sigma\tau$, where for $\sigma \in \mathrm{Gal}(K_\infty/k)$, τ runs over all elements in $\mathrm{Gal}(L_\infty/k)$ such that $c(\tau) = \sigma$. We have

$$\nu(x)y = \nu(xc(y)) \quad \text{for all } x \in \Lambda_{K_\infty} \text{ and } y \in \Lambda_{L_\infty}\,. \tag{2.1.2}$$

This implies

(2.1.3) $\nu(x)\nu(y) = \nu(xc(\nu(y))) = [L : K]\nu(xy)$ for all $x, y \in \Lambda_{K_\infty}$.

Let $Q(\Lambda_{L_\infty})$ (resp. $Q(\Lambda_{K_\infty})$) be the total quotient ring of Λ_{L_∞} (resp. Λ_{K_∞}). We naturally extend c to the ring homomorphism $c : Q(\Lambda_{L_\infty}) \longrightarrow Q(\Lambda_{K_\infty})$. We can extend ν to the Λ_{K_∞}-homomorphism $\nu : Q(\Lambda_{K_\infty}) \longrightarrow Q(\Lambda_{L_\infty})$ such that $\nu(c(x)) = \Sigma_{\sigma\in G}\sigma x$ for $x \in Q(\Lambda_{L_\infty})$.

We set

$$S = \{\mathfrak{l} \in P'_k \mid \mathfrak{l} \text{ is unramified in } K, \text{ and } \mathfrak{l} \text{ is ramified in } L\}.$$

We have

$$c(\theta_{L_\infty/k}) = \left(\prod_{\mathfrak{l}\in S}(1 - \varphi_{\mathfrak{l}}^{-1})\right)\theta_{K_\infty/k} \tag{2.1.4}$$

where $\varphi_{\mathfrak{l}} = (\frac{\mathfrak{l}}{K_\infty/k})$ is the Frobenius of $\mathfrak{l}$ in $\mathrm{Gal}(K_\infty/k)$ (Lemma 2.1 in [10]).

2.2. For a commutative ring R and a finitely presented R-module M such that $R^m \xrightarrow{f} R^n \longrightarrow M \longrightarrow 0$ is exact, the Fitting ideal of M is defined to be the ideal of R generated by all $n \times n$ minors of the matrix A_f which corresponds to f. This ideal does not depend on the choice of the exact sequence. We denote it by $\mathrm{Fitt}_R(M)$. We obtain $\mathrm{Fitt}_R(M) \subset \mathrm{Ann}_R(M)$ from the definition.

We consider $\mathcal{X}_{L_\infty} = (A_{L_\infty})^\vee$ and the minus part $\mathcal{X}_{L_\infty}^-$. As we mentioned in §1.2, we have decomposition $\mathcal{X}_{L_\infty} = \bigoplus_\chi \mathcal{X}_{L_\infty}^\chi$ where χ runs over the equivalence classes of $\overline{\mathbf{Q}}_p^\times$-valued characters of $\mathrm{Gal}(K/k)$. From $\mathcal{X}_{L_\infty}^- = \bigoplus_{\chi:\mathrm{odd}} \mathcal{X}_{L_\infty}^\chi$, knowing $\mathrm{Fitt}_{\Lambda_{L_\infty}}(\mathcal{X}_{L_\infty}^-)$ is equivalent to knowing $\mathrm{Fitt}_{\Lambda_{L_\infty}^\chi}(\mathcal{X}_{L_\infty}^\chi)$ for all odd characters χ. We regard $\mathrm{Ker}\,\chi \subset \mathrm{Gal}(K/k)$ as a subgroup of $\mathrm{Gal}(L/k)$ and denote by L_χ (resp. K_χ) the subfield of L (resp. K) such that $\mathrm{Gal}(L/L_\chi) = \mathrm{Ker}\,\chi$ (resp. $\mathrm{Gal}(K/K_\chi) = \mathrm{Ker}\,\chi$). Since $[L_\infty : L_{\chi,\infty}]$ is prime to p, $A_{L_{\chi,\infty}} \xrightarrow{\simeq} A_{L_\infty}^{\mathrm{Gal}(L_\infty/L_{\chi,\infty})}$ is an isomorphism. Therefore, $\mathcal{X}_{L_\infty}^\chi \xrightarrow{\simeq} \mathcal{X}_{L_{\chi,\infty}}^\chi$ is bijective. Since we clearly have $\Lambda_{L_\infty}^\chi = \Lambda_{L_{\chi,\infty}}^\chi$, we obtain

$$\mathrm{Fitt}_{\Lambda_{L_\infty}^\chi}(\mathcal{X}_{L_\infty}^\chi) = \mathrm{Fitt}_{\Lambda_{L_{\chi,\infty}}^\chi}(\mathcal{X}_{L_{\chi,\infty}}^\chi).$$

So we may assume $K = K_\chi$ when we study the χ-component. In particular, we may assume that the conductor of K/k is the same as that of χ for the computation of the Fitting ideal of $\mathcal{X}_{L_\infty}^\chi$.

2.3. In this subsection, we further assume that $[L : K] = p$. We fix an odd character χ of $\mathrm{Gal}(K/k)$, and assume that the conductor of χ is equal to the conductor of K/k.

1) Suppose that $\chi \neq \omega$. We extend χ to the ring homomorphism $Q(\Lambda_{L_\infty}) \longrightarrow Q(\Lambda_{L_\infty}^\chi)$ and the image of $x \in Q(\Lambda_{L_\infty})$ is denoted by $x^\chi \in Q(\Lambda_{L_\infty}^\chi)$. We know

$\theta^{\chi}_{K_\infty/k} \in \Lambda^{\chi}_{K_\infty}$ and $\theta^{\chi}_{L_\infty/k} \in \Lambda^{\chi}_{L_\infty}$ by Deligne and Ribet. Let S be as in §2.1. Following the idea of Greither [5] (cf. Theorem 7 in [5]), we consider a fractional ideal $(1, \nu(\frac{1}{1-\varphi_{\mathfrak{l}}^{-1}}))$ of Λ_{L_∞} for $\mathfrak{l} \in S$, and define

$$\Theta = \left(\prod_{\mathfrak{l}\in S}\left(1, \nu\left(\frac{1}{1-\varphi_{\mathfrak{l}}^{-1}}\right)\right)\right)\theta_{L_\infty/k} \tag{2.3.1}$$

which is a fractional ideal of Λ_{L_∞}. Consider the χ-component Θ^{χ}. By (2.1.2), (2.1.3), and (2.1.4), we obtain $\Theta^{\chi} \subset \Lambda^{\chi}_{L_\infty}$, so Θ^{χ} is an ideal of $\Lambda^{\chi}_{L_\infty}$. By Theorem 3 in Greither [5] and Corollary A. 13 in [7], we have

$$\mathrm{Fitt}_{\Lambda^{\chi}_{L_\infty}}(\mathcal{X}^{\chi}_{L_\infty}) = \mathrm{Fitt}_{\Lambda^{\chi}_{L_\infty}}((A^{\chi}_{L_\infty})^{\vee}) = \Theta^{\chi}\,. \tag{2.3.2}$$

We will give another proof of (2.3.2) by the same method as the proof of Theorem 0.1 in Remark 3.5.

2) Next, we suppose that $\chi = \omega$ and there is a prime $\mathfrak{l} \in P'_k$ which is ramified in L/K. We assume $K = k(\mu_p)$ (we may assume this as we explained in §2.2). Let S be as in §2.1. Note that S is not empty by our assumption. Following Greither [5] (cf. page 753 in [5]), we introduce a modified Stickelberger element $\vartheta_{L_\infty/k}$ (which corresponds to Ψ_S in [5] though our element is slightly modified).

We put

$$\xi = \nu\left(\frac{1}{p}\prod_{\mathfrak{l}\in S}\frac{1-\kappa(\varphi_{\mathfrak{l}})\varphi_{\mathfrak{l}}^{-1}}{1-\varphi_{\mathfrak{l}}^{-1}}\right) + \left(1-\nu\left(\frac{1}{p}\right)\right), \tag{2.3.3}$$

which is an element of the total quotient ring of Λ_{L_∞} where $\varphi_{\mathfrak{l}}$ is the Frobenius of $\mathfrak{l}$ in $\mathrm{Gal}(K_\infty/k)$. We define

$$\vartheta_{L_\infty/k} = \xi\theta_{L_\infty/k}\,. \tag{2.3.4}$$

Using the definition of $\vartheta_{L_\infty/k}$ and (2.1.4), we have

$$c(\vartheta_{L_\infty/k}) = \left(\prod_{\mathfrak{l}\in S}(1-\kappa(\varphi_{\mathfrak{l}})\varphi_{\mathfrak{l}}^{-1})\right)\theta_{K_\infty/k}\,. \tag{2.3.5}$$

LEMMA 2.1 (C. Greither). *If S is not empty, we have*

$$\vartheta_{L_\infty/k} \in \Lambda_{L_\infty}\,. \tag{2.3.6}$$

PROOF. This corresponds to Proposition 9 in Greither [5]. We give here a proof by computing $\vartheta_{L_\infty/k}$ directly. Using (2.1.2) and (2.1.4), we compute

$$\vartheta_{L_\infty/k} = \nu\left(\frac{\prod_{\mathfrak{l}\in S}(1-\kappa(\varphi_{\mathfrak{l}})\varphi_{\mathfrak{l}}^{-1}) - \prod_{\mathfrak{l}\in S}(1-\varphi_{\mathfrak{l}}^{-1})}{p}\theta_{K_\infty/k}\right) + \theta_{L_\infty/k}\,. \tag{2.3.7}$$

As we explained in the proof of Proposition 1.2 (2), $\mathfrak{l} \in S$ satisfies $N(\varphi_{\mathfrak{l}}) \equiv 1 \pmod{p}$, so $\kappa(\varphi_{\mathfrak{l}}) \equiv 1 \pmod{p}$. Therefore,

$$\frac{\prod_{\mathfrak{l}\in S}(1-\kappa(\varphi_{\mathfrak{l}})\varphi_{\mathfrak{l}}^{-1}) - \prod_{\mathfrak{l}\in S}(1-\varphi_{\mathfrak{l}}^{-1})}{p} \in \Lambda_{K_\infty}\,.$$

Let γ be a generator of $\mathrm{Gal}(L_\infty/L)$. Since $(\gamma-\kappa(\gamma))\theta_{K_\infty/k} \in \Lambda_{K_\infty}$ and $(\gamma-\kappa(\gamma))\theta_{L_\infty/k} \in \Lambda_{L_\infty}$, we obtain $(\gamma-\kappa(\gamma))\vartheta_{L_\infty/k} \in \Lambda_{L_\infty}$. We have to show $(\gamma-\kappa(\gamma))\vartheta_{L_\infty/k} \in (\gamma-\kappa(\gamma))\Lambda_{L_\infty}$.

Let $\tilde{\kappa}$ be the automorphism of $Q(\Lambda_{L_\infty})$ defined in (2.1.1), and $\pi_{L_\infty} : \Lambda_{L_\infty} \longrightarrow \mathbf{Z}_p$ (resp. $\pi_{K_\infty} : \Lambda_{K_\infty} \longrightarrow \mathbf{Z}_p$) be the augmentation map. Since $\tilde{\kappa}(\vartheta_{L_\infty/k})$ is a pseudo-measure in the sense of Serre [16], it suffices to prove $\pi_{L_\infty}((\gamma-1)\tilde{\kappa}(\vartheta_{L_\infty/k})) = 0$ (see [16] 1.14). Using (2.3.5), we compute

$$\begin{aligned}\pi_{L_\infty}((\gamma-1)\tilde{\kappa}(\vartheta_{L_\infty/k})) &= \pi_{K_\infty}\left((\gamma-1)\tilde{\kappa}\left(\left(\prod_{\mathfrak{l}\in S}(1-\kappa(\varphi_{\mathfrak{l}})\varphi_{\mathfrak{l}}^{-1})\right)\theta_{K_\infty/k}\right)\right)\\ &= \pi_{K_\infty}\left(\left(\prod_{\mathfrak{l}\in S}(1-\varphi_{\mathfrak{l}}^{-1})\right)(\gamma-1)\tilde{\kappa}(\theta_{K_\infty/k})\right)\\ &= 0\,.\end{aligned}$$

Note that we used $S \neq \phi$ to obtain the final equation. This completes the proof of Lemma 2.1.

Note that $1-\kappa(\varphi_{\mathfrak{l}})\varphi_{\mathfrak{l}}^{-1}$ is divisible by $\gamma-\kappa(\gamma)$ in Λ_{K_∞}. We consider a fractional ideal $(1, \nu((\gamma-\kappa(\gamma))/(1-\kappa(\varphi_{\mathfrak{l}})\varphi_{\mathfrak{l}}^{-1})))$. We define

$$\mathcal{S} = \sum_{\mathfrak{l}\in S}\left(\prod_{\substack{\mathfrak{l}'\neq\mathfrak{l}\\ \mathfrak{l}'\in S}}\left(1, \nu\left(\frac{1}{1-\kappa(\varphi_{\mathfrak{l}'})\varphi_{\mathfrak{l}'}^{-1}}\right)\right)\right)\left(1, \nu\left(\frac{\gamma-\kappa(\gamma)}{1-\kappa(\varphi_{\mathfrak{l}})\varphi_{\mathfrak{l}}^{-1}}\right)\right)\vartheta_{L_\infty/k}\,. \tag{2.3.8}$$

By (2.1.2), (2.1.3), (2.3.5) and (2.3.6), we obtain that

$$\mathcal{S} \subset \Lambda_{L_\infty}\,, \tag{2.3.9}$$

namely, $\mathcal{S}$ is an ideal of Λ_{L_∞}. We study the ω-component $\mathcal{S}^\omega \subset \Lambda_{L_\infty}^\omega$. Our $\mathcal{S}^\omega$ coincides with the ideal in Greither [5] Proposition 10.

LEMMA 2.2. *Suppose that I_{L_∞} is the ideal of Λ_{L_∞} defined in §0. We have $(I_{L_\infty}\theta_{L_\infty/k})^\omega \neq \mathcal{S}^\omega$.*

PROOF. We put $\Lambda = \mathbf{Z}_p[[\mathrm{Gal}(k_\infty/k)]]$. Then $\Lambda_{L_\infty} = \Lambda[\mathrm{Gal}(L/k)]$ and $\Lambda_{L_\infty}^\omega \simeq \Lambda[\mathrm{Gal}(L/K)]$. Let $\psi : \mathrm{Gal}(L/K) \longrightarrow \mu_p$ be a faithful character (namely, a bijective homomorphism). This ψ induces a ring homomorphism $\Lambda_{L_\infty}^\omega = \Lambda[\mathrm{Gal}(L/K)] \longrightarrow \Lambda[\mu_p]$, which we also denote by ψ. By (2.3.7) and (2.3.8), we obtain

$$\psi(\theta_{L_\infty/k}^\omega) = \psi(\vartheta_{L_\infty/k}^\omega) \in \psi(\mathcal{S}^\omega)\,.$$

On the other hand, concerning $(I_{L_\infty}\theta_{L_\infty/k})^\omega$, if σ is a generator of $\mathrm{Gal}(L/K)$, we have

$$\psi((I_{L_\infty}\theta_{L_\infty/k})^\omega) = (\psi(\sigma)-1, \gamma-\kappa(\gamma))\psi(\theta^\omega_{L_\infty/k}) .$$

Since $(\psi(\sigma)-1, \gamma-\kappa(\gamma)) \neq \Lambda[\mu_p]$, we have $\psi(\theta^\omega_{L_\infty/k}) \notin \psi((I_{L_\infty}\theta_{L_\infty/k})^\omega)$. Therefore, $\psi((I_{L_\infty}\theta_{L_\infty/k})^\omega) \neq \psi(\mathcal{S}^\omega)$, and we obtain the conclusion.

We will prove $\mathrm{Fitt}_{\Lambda^\omega_{L_\infty}}(\mathcal{X}^\omega_{L_\infty}) = \mathrm{Fitt}_{\Lambda^\omega_{L_\infty}}((A^\omega_{L_\infty})^\vee) = \mathcal{S}^\omega$ (Theorem 0.1 (1)) in the next section.

3) Finally, we suppose that $\chi = \omega$ and L/K is unramified outside p. In other words, we suppose $S = \phi$. We cannot define a good element $\vartheta_{L_\infty/k}$ in Λ_{L_∞} in this case. We will use $\theta_{L_\infty/k}$. Let I_{L_∞} be the ideal of Λ_{L_∞} defined in §0. By Deligne and Ribet, we know $I_{L_\infty}\theta_{L_\infty/k} \subset \Lambda_{L_\infty}$. We consider $(I_{L_\infty}\theta_{L_\infty/k})^\omega$ which is an ideal of $\Lambda^\omega_{L_\infty}$. What we will prove in the next section is

$$\mathrm{Fitt}_{\Lambda^\omega_{L_\infty}}(\mathcal{X}^\omega_{L_\infty}) = \mathrm{Fitt}_{\Lambda^\omega_{L_\infty}}((A^\omega_{L_\infty})^\vee) = (I_{L_\infty}\theta_{L_\infty/k})^\omega .$$

3. Proof of Theorems

3.1. We go back to the general situation, and suppose that L_0/k is a finite abelian p-extension such that $L_0 \cap k_\infty = k$. We put $K = k(\mu_p)$ and $L = L_0(\mu_p)$ (we do not assume $[L:K] = p$). We study $\mathcal{X}^\omega_{L_\infty} = (A^\omega_{L_\infty})^\vee$. Let $L_{0,\infty}$ be the cyclotomic $\mathbf{Z}_p$-extension of L_0, and let $M_{L_{0,\infty}}/L_{0,\infty}$ (resp. M_{k_∞}/k_∞) be the maximal abelian pro-p extension of $L_{0,\infty}$ (resp. k_∞) which is unramified outside p. By Washington [17] Proposition 13.32, we have canonical isomorphisms $\mathcal{X}^\omega_{L_\infty} = (A^\omega_{L_\infty})^\vee \simeq \mathrm{Gal}(M_{L_{0,\infty}}/L_{0,\infty})(1)$ and $\mathcal{X}^\omega_{K_\infty} = (A^\omega_{K_\infty})^\vee \simeq \mathrm{Gal}(M_{k_\infty}/k_\infty)(1)$ (note that our action is cogredient).

Using these isomorphisms, we obtain

LEMMA 3.1. *Let L'_0/k be the maximal subextension of L_0/k which is unramified outside p. Put $G = \mathrm{Gal}(L/K) = \mathrm{Gal}(L_0/k)$. Then we have an exact sequence*

$$0 \longrightarrow \hat{H}^0(G, A^\omega_{L_\infty})^\vee \longrightarrow (\mathcal{X}^\omega_{L_\infty})_G \xrightarrow{f} \mathcal{X}^\omega_{K_\infty} \longrightarrow \mathrm{Gal}(L'_0/k)(1) \longrightarrow 0 .$$

PROOF. The cokernel of the natural map $\mathrm{Gal}(M_{L_{0,\infty}}/L_{0,\infty}) \longrightarrow \mathrm{Gal}(M_{k_\infty}/k_\infty)$ is $\mathrm{Gal}((L'_0)_\infty/k_\infty) = \mathrm{Gal}(L'_0/k)$. Therefore, the cokernel of f is $\mathrm{Gal}(L'_0/k)(1)$.

For $n > 0$, we regard A_{L_n} as the Galois group of the maximal unramified abelian p-extension of L_n, and A_{K_n} similarly. Then the norm map is the restriction map, so $A^\omega_{L_n} \longrightarrow A^\omega_{K_n}$ is surjective because $\mathrm{Gal}(K/k)$ acts on $A^\omega_{L_n}$ via ω and acts on $\mathrm{Gal}(L_n/K_n)$ trivially. This implies that the norm map $A^\omega_{L_\infty} \longrightarrow A^\omega_{K_\infty}$ is surjective. Therefore, $N_G A^\omega_{L_\infty}$ coincides with the image of the natural map $A^\omega_{K_\infty} \longrightarrow A^\omega_{L_\infty}$ where $N_G = \Sigma_{\sigma\in G}\sigma$. This implies that

$$A^\omega_{K_\infty} \longrightarrow (A^\omega_{L_\infty})^G \longrightarrow \hat{H}^0(G, A^\omega_{L_\infty}) \longrightarrow 0$$

is exact. Taking the dual, we obtain the kernel of f.

3.2. We first prove Theorem 0.1. Suppose that $[L : K] = [L_0 : k] = p$, so $G = \mathrm{Gal}(L/K)$ is of order p. Put $\Lambda = \mathbf{Z}_p[[\mathrm{Gal}(k_\infty/k)]]$. Then $\mathcal{X}^\omega_{L_\infty}$ is a $\Lambda^\omega_{L_\infty} = \Lambda[G]$-module. Let $\psi : G \longrightarrow \overline{\mathbf{Q}}_p^\times$ be a faithful character. We extend ψ to the ring homomorphism

$$\psi : \Lambda^\omega_{L_\infty} = \Lambda[G] \longrightarrow \Lambda[\mu_p]$$

as in the proof of Lemma 2.2. For any $\Lambda^\omega_{L_\infty}$-module M, we define M_ψ to be $M \otimes_{\Lambda^\omega_{L_\infty}} \Lambda[\mu_p]$ where $\Lambda[\mu_p]$ is regarded as a $\Lambda^\omega_{L_\infty}$-module via ψ.

We have to prepare three more lemmas.

LEMMA 3.2. *Let M be a $\Lambda[G]$-module such that M is a free $\mathbf{Z}_p$-module of finite rank. We regard M_ψ as a $\mathbf{Z}_p[\mu_p]$-module. If $\hat{H}^0(G, M) = (\mathbf{Z}/p\mathbf{Z})^{\oplus r}$, the maximal $\mathbf{Z}_p[\mu_p]$-torsion submodule of M_ψ is isomorphic to $(\mathbf{Z}/p\mathbf{Z})^{\oplus r}$.*

PROOF. This is well-known. We know M is isomorphic to $\mathbf{Z}_p[G]^{\oplus a} \oplus \mathbf{Z}_p[\mu_p]^{\oplus b} \oplus \mathbf{Z}_p^{\oplus c}$ as a $\mathbf{Z}_p[G]$-module. Then $\hat{H}^0(G, M) = (\mathbf{Z}/p\mathbf{Z})^{\oplus r}$ implies $c = r$. We know $M_\psi = M \otimes_{\Lambda[G]} \Lambda[\mu_p] = M \otimes_{\mathbf{Z}_p[G]} \mathbf{Z}_p[\mu_p] \simeq \mathbf{Z}_p[\mu_p]^{\oplus(a+b)} \oplus (\mathbf{Z}/p\mathbf{Z})^{\oplus c}$. Therefore, the $\mathbf{Z}_p[\mu_p]$-torsion submodule is $(\mathbf{Z}/p\mathbf{Z})^{\oplus c}$.

Suppose that G is generated by σ, and consider two homomorphisms $c : \Lambda[G] \longrightarrow \Lambda$ which is induced by $\sigma \mapsto 1$, and $\psi : \Lambda[G] \longrightarrow \Lambda[\mu_p]$ which is as above.

LEMMA 3.3. *Let I and J be two ideals of $\Lambda[G]$. We assume that $c(I) = c(J)$ and $\psi(I) = \psi(J)$. Furthermore, we assume one of the following.*

i) *$c(I)$ is a principal ideal generated by a non-zero element $g \in \Lambda$, whose μ invariant is zero.*

ii) *$\psi(I)$ is a principal ideal generated by a non-zero element $h \in \Lambda[\mu_p]$, whose μ invariant is zero.*

Then we have $I = J$.

PROOF. We first assume i). Let x be an element of I. We will show $x \in J$. Put $\Phi = \sum_{i=0}^{p-1} \sigma^i$. The kernel of $\psi : \Lambda[G] \longrightarrow \Lambda[\mu_p]$ is generated by Φ. Since $\psi(I) = \psi(J)$, we can write $x = y + \Phi z$ for some $y \in J$ and $z \in \Lambda[G]$. We have $c(x) = c(y) + pc(z)$. Therefore, $c(I) = c(J) = (g)$ implies that g divides $pc(z)$. This shows that g divides $c(z)$ because we assumed the μ-invariant of g is zero. Therefore, using $c(I) = c(J)$, we can write $z = u + (\sigma - 1)v$ for some $u \in J$ and $v \in \Lambda[G]$. We have $x = y + \Phi u$ because $\Phi(\sigma - 1) = 0$. This shows that $x \in J$. Hence $I \subset J$. The other inclusion $J \subset I$ is obtained by the same method, so we have $I = J$.

Suppose ii) is satisfied, and $x \in I$. Using $c(I) = c(J)$, we can write $x = y + (\sigma - 1)z$ for some $y \in J$ and $z \in \Lambda[G]$. Now, $\psi(x) = \psi(y) + (\zeta_p - 1)\psi(z)$ where $\zeta_p = \psi(\sigma)$ is a primitive p-th root of unity. Therefore, h divides $\psi(z)$. So we can write $z = u + \Phi v$ for some $u \in J$ and $v \in \Lambda[G]$. This implies that $x = y + (\sigma - 1)u \in J$. Thus, $I \subset J$. The other inclusion is proved in the same way, and we have $I = J$.

LEMMA 3.4. *Let R be the ring of integers of a finite extension of* $\mathbf{Q}_p$, *and* $A = R[[T]]$. *Suppose that*

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

is an exact sequence of finitely generated torsion A-modules, and that M_3 contains no nontrivial finite submodule. Then we have

$$\mathrm{Fitt}_A(M_2) = \mathrm{Fitt}_A(M_1)\,\mathrm{char}_A(M_3)$$

where $\mathrm{char}_A(M_3)$ *is the characteristic ideal of* M_3.

PROOF. (cf. also [2] Lemma 3.) By [19] Proposition 2.1, M_3 has a free resolution of the form $0 \longrightarrow A^m \longrightarrow A^m \longrightarrow M_3 \longrightarrow 0$. Therefore, we have $\mathrm{Fitt}_A(M_3) = \mathrm{char}_A(M_3)$, and we can apply Theorem 22 in Chapter 3 of Northcott [14] to obtain

$$\begin{aligned}\mathrm{Fitt}_A(M_2) &= \mathrm{Fitt}_A(M_1)\,\mathrm{Fitt}_A(M_3)\\ &= \mathrm{Fitt}_A(M_1)\,\mathrm{char}_A(M_3)\,.\end{aligned}$$

PROOF OF THEOREM 0.1 (1). Suppose that $S \neq \phi$. By Lemma 3.1, we have an exact sequence

$$0 \longrightarrow \hat{H}^0(G, A^{\omega}_{L_\infty})^{\vee} \longrightarrow (\mathcal{X}^{\omega}_{L_\infty})_G \longrightarrow \mathcal{X}^{\omega}_{K_\infty} \longrightarrow 0$$

of Λ-modules because $L'_0 = k$ in this case. By Iwasawa [8] Theorem 18, $\mathcal{X}^{\omega}_{K_\infty}$ contains no nontrivial finite submodule. Therefore, using Lemma 3.4 and the Iwasawa main conjecture proved by Wiles [18], we have

$$\begin{aligned}\mathrm{Fitt}_\Lambda((\mathcal{X}^{\omega}_{L_\infty})_G) &= \mathrm{Fitt}_\Lambda(\hat{H}^0(G, A^{\omega}_{L_\infty})^{\vee})\,\mathrm{char}_\Lambda(\mathcal{X}^{\omega}_{K_\infty})\\ &= \mathrm{Fitt}_\Lambda(\hat{H}^0(G, A^{\omega}_{L_\infty})^{\vee})((\gamma - \kappa(\gamma))\theta^{\omega}_{K_\infty/k})\,.\end{aligned} \tag{3.2.1}$$

We will compute $\mathrm{Fitt}_\Lambda(\hat{H}^0(G, A^{\omega}_{L_\infty})^{\vee})$. Since $\hat{H}^0(G, A^{\omega}_{L_\infty})$ is finite, we know $\mathrm{Fitt}_\Lambda(\hat{H}^0(G, A^{\omega}_{L_\infty})^{\vee}) = \mathrm{Fitt}_\Lambda(\hat{H}^0(G, A^{\omega}_{L_\infty}))$ by [13] Appendix Proposition 3. Suppose that $S = \{\mathfrak{l}_1, \dots, \mathfrak{l}_r\}$. For $\mathfrak{l} \in S$, we put $\alpha_{\mathfrak{l}} = (1 - \kappa(\varphi_{\mathfrak{l}})\varphi_{\mathfrak{l}}^{-1})^{\omega}$, $\beta_{\mathfrak{l}} = \alpha_{\mathfrak{l}}/(\gamma - \kappa(\gamma)) \in \Lambda^{\omega}_{K_\infty} = \Lambda$. By Proposition 1.2 (2), $\hat{H}^0(G, A^{\omega}_{L_\infty})$ is isomorphic to $\mathrm{Coker}(\mathbf{Z}/p\mathbf{Z} \xrightarrow{j} \bigoplus_{i=1}^{r} \Lambda^{\omega}_{K_\infty}/(p, \alpha_{\mathfrak{l}_i}))$ where the map j is defined by $j(1) = (\beta_{\mathfrak{l}_1}, \dots, \beta_{\mathfrak{l}_r})$. Therefore, a relation matrix of $\hat{H}^0(G, A^{\omega}_{L_\infty})$ is

$$\begin{pmatrix} p & 0 & \dots & 0 \\ \alpha_{\mathfrak{l}_1} & 0 & \dots & 0 \\ 0 & p & \dots & 0 \\ 0 & \alpha_{\mathfrak{l}_2} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & p \\ 0 & 0 & \dots & \alpha_{\mathfrak{l}_r} \\ \beta_{\mathfrak{l}_1} & \beta_{\mathfrak{l}_2} & \dots & \beta_{\mathfrak{l}_r} \end{pmatrix}.$$

This shows that $\mathrm{Fitt}_\Lambda(\hat{H}^0(G, A^\omega_{L_\infty}))$ is generated by the elements of the form

i) $p^{r-\#T}\prod_{\mathfrak{l}\in T}\alpha_\mathfrak{l}$ (where $T \subset S$ and $T \neq \phi$),

ii) $p^{r-1-\#T}\beta_\mathfrak{l}\prod_{\mathfrak{l}'\in T}\alpha_{\mathfrak{l}'}$ (where $\mathfrak{l} \in S$ and $T \subset S \setminus \{\mathfrak{l}\}$), and

iii) p^r.

Since an element of the form i) is a multiple of some element of the form ii), we only need ii) and iii). We have

$$\mathrm{Fitt}_\Lambda(\hat{H}^0(G, A^\omega_{L_\infty})) = \sum_{\mathfrak{l}\in S}\Bigg(\prod_{\substack{\mathfrak{l}'\neq\mathfrak{l}\\ \mathfrak{l}'\in S}}(\alpha_{\mathfrak{l}'}, p)\Bigg)(\beta_\mathfrak{l}, p).$$

Thus, it follows from (3.2.1) that

$$c(\mathrm{Fitt}_{\Lambda[G]}(\mathcal{X}^\omega_{L_\infty})) = \mathrm{Fitt}_\Lambda((\mathcal{X}^\omega_{L_\infty})_G) = \sum_{\mathfrak{l}\in S}\Bigg(\prod_{\substack{\mathfrak{l}'\neq\mathfrak{l}\\ \mathfrak{l}'\in S}}(\alpha_{\mathfrak{l}'}, p)\Bigg)(\beta_\mathfrak{l}, p)(\gamma-\kappa(\gamma))\theta^\omega_{K_\infty/k}.$$

On the other hand, using the definition of $\mathcal{S}$ (see (2.3.8)), we have

$$\begin{aligned} c(\mathcal{S}^\omega) &= \sum_{\mathfrak{l}\in S}\Bigg(\prod_{\substack{\mathfrak{l}'\neq\mathfrak{l}\\ \mathfrak{l}'\in S}}\Big(1, \frac{p}{\alpha_{\mathfrak{l}'}}\Big)\Bigg)\Big(1, \frac{p}{\beta_\mathfrak{l}}\Big)\Big(\prod_{\mathfrak{l}\in S}\alpha_\mathfrak{l}\Big)\theta^\omega_{K_\infty/k} \\ &= \sum_{\mathfrak{l}\in S}\Bigg(\prod_{\substack{\mathfrak{l}'\neq\mathfrak{l}\\ \mathfrak{l}'\in S}}(\alpha_{\mathfrak{l}'}, p)\Bigg)(\beta_\mathfrak{l}, p)(\gamma-\kappa(\gamma))\theta^\omega_{K_\infty/k}. \end{aligned}$$

Therefore, we obtain $c(\mathrm{Fitt}_{\Lambda[G]}(\mathcal{X}^\omega_{L_\infty})) = c(\mathcal{S}^\omega)$.

By Proposition 1.2 (2), we have $\hat{H}^0(G, \mathcal{X}^\omega_{L_\infty}) = \hat{H}^{-1}(G, A^\omega_{L_\infty}))^\vee = 0$. Therefore, by Lemma 3.2, $(\mathcal{X}^\omega_{L_\infty})_\psi$ contains no nontrivial finite submodule. Hence we have

$$\mathrm{Fitt}_{\Lambda[\mu_p]}((\mathcal{X}^\omega_{L_\infty})_\psi) = \mathrm{char}_{\Lambda[\mu_p]}((\mathcal{X}^\omega_{L_\infty})_\psi) = (\psi(\theta^\omega_{L_\infty/k}))$$

by the main conjecture proved by Wiles [18]. Since it is easy to see $\psi(\mathcal{S}^\omega) = (\psi(\theta^\omega_{L_\infty/k}))$, we obtain $\psi(\mathrm{Fitt}_{\Lambda[G]}(\mathcal{X}^\omega_{L_\infty})) = \psi(\mathcal{S}^\omega)$. Therefore, the conditions of Lemma 3.3 are satisfied (the condition ii) is satisfied), and we obtain

$$\mathrm{Fitt}_{\Lambda[G]}(\mathcal{X}_{L_\infty}^{\omega}) = \mathcal{S}^{\omega}\,.$$

Next, we will prove $I_{L_\infty}\theta_{L_\infty/k} \subsetneq \mathrm{Fitt}_{\Lambda_{L_\infty}}(\mathcal{X}_{L_\infty})$. We take $a \in I_{L_\infty}$. It is easy to see $\psi(a\theta_{L_\infty/k}^{\omega}) \in \psi(\mathcal{S}^{\omega})$ and $c(a\theta_{L_\infty/k}^{\omega}) \in c(\mathcal{S}^{\omega})$ from the above descriptions of $\psi(\mathcal{S}^{\omega})$ and $c(\mathcal{S}^{\omega})$ (cf. also (2.1.4)). By the same argument as the proof of Lemma 3.3, we have $a\theta_{L_\infty/k}^{\omega} \in \mathcal{S}^{\omega}$. We saw in Lemma 2.2 that $(I_{L_\infty}\theta_{L_\infty/k})^{\omega} \neq \mathcal{S}^{\omega}$, so we obtain $(I_{L_\infty}\theta_{L_\infty/k})^{\omega} \subsetneq \mathrm{Fitt}_{\Lambda_{L_\infty}}(\mathcal{X}_{L_\infty}^{\omega})$. If χ is odd and $\chi \neq \omega$, we have $\theta_{L_\infty/k}^{\chi} \in \mathrm{Fitt}_{\Lambda_{L_\infty}}(\mathcal{X}_{L_\infty}^{\chi})$ by (2.3.2). If χ is even, $\theta_{L_\infty/k}^{\chi} = 0$. Therefore, we obtain $I_{L_\infty}\theta_{L_\infty/k} \subsetneq \mathrm{Fitt}_{\Lambda_{L_\infty}}(\mathcal{X}_{L_\infty})$. This completes the proof of Theorem 0.1 (1). □

PROOF OF THEOREM 0.1 (2). We prove this statement by the same strategy as the proof of Theorem 0.1 (1). By Proposition 1.2 (3) and Lemma 3.1, we have an exact sequence

$$0 \longrightarrow (\mathcal{X}_{L_\infty}^{\omega})_G \longrightarrow \mathcal{X}_{K_\infty}^{\omega} \longrightarrow \mathbf{Z}/p\mathbf{Z} \longrightarrow 0\,.$$

Since $\mathcal{X}_{K_\infty}^{\omega}$ contains no nontrivial finite submodule ([8] Theorem 18), $(\mathcal{X}_{L_\infty}^{\omega})_G$ also has this property. Therefore, $\mathrm{Fitt}_{\Lambda}((\mathcal{X}_{L_\infty}^{\omega})_G) = \mathrm{char}_{\Lambda}((\mathcal{X}_{L_\infty}^{\omega})_G)$ ([19] Proposition 2.1), and

$$\mathrm{Fitt}_{\Lambda}((\mathcal{X}_{L_\infty}^{\omega})_G) = \mathrm{char}_{\Lambda}((\mathcal{X}_{L_\infty}^{\omega})_G) = \mathrm{char}_{\Lambda}(\mathcal{X}_{K_\infty}^{\omega}) = ((\gamma-\kappa(\gamma))\theta_{K_\infty/k}^{\omega})$$

by the Iwasawa main conjecture [18]. Since $c((I_{L_\infty}\theta_{L_\infty/k})^{\omega}) = ((\gamma-\kappa(\gamma))\theta_{K_\infty/k}^{\omega})$, we obtain

$$c(\mathrm{Fitt}_{\Lambda[G]}(\mathcal{X}_{L_\infty}^{\omega})) = \mathrm{Fitt}_{\Lambda}((\mathcal{X}_{L_\infty}^{\omega})_G) = c((I_{L_\infty}\theta_{L_\infty/k})^{\omega})\,.$$

Next, we consider $(\mathcal{X}_{L_\infty}^{\omega})_{\psi}$. It follows from Proposition 1.2 (3) that

$$\hat{H}^0(G, \mathcal{X}_{L_\infty}^{\omega}) = \hat{H}^{-1}(G, A_{L_\infty}^{\omega})^{\vee} \simeq \mathbf{Z}/p\mathbf{Z}\,.$$

Therefore, Lemma 3.2 implies that the maximal finite torsion submodule of $(\mathcal{X}_{L_\infty}^{\omega})_{\psi}$ is of order p. Thus, we have an exact sequence

$$0 \longrightarrow \mathbf{Z}/p\mathbf{Z} \longrightarrow (\mathcal{X}_{L_\infty}^{\omega})_{\psi} \longrightarrow M \longrightarrow 0$$

of $\Lambda[\mu_p]$-modules where $M = (\mathcal{X}_{L_\infty}^{\omega})_{\psi}/((\mathcal{X}_{L_\infty}^{\omega})_{\psi})_{tors}$ contains no nontrivial finite submodule. Using Lemma 3.4 and the main conjecture [18], we compute

$$\begin{aligned}\mathrm{Fitt}_{\Lambda[\mu_p]}((\mathcal{X}_{L_\infty}^{\omega})_{\psi}) &= \mathrm{Fitt}_{\Lambda[\mu_p]}(\mathbf{Z}/p\mathbf{Z})\,\mathrm{char}_{\Lambda[\mu_p]}(M)\\ &= \mathrm{Fitt}_{\Lambda[\mu_p]}(\mathbf{Z}/p\mathbf{Z})\,\mathrm{char}_{\Lambda[\mu_p]}((\mathcal{X}_{L_\infty}^{\omega})_{\psi})\\ &= (\zeta_p-1, \gamma-\kappa(\gamma))\psi(\theta_{L_\infty/k}^{\omega})\end{aligned}$$

where $\zeta_p = \psi(\sigma)$ which is a primitive p-th root of unity. On the other hand, it is clear that $\psi((I_{L_\infty}\theta_{L_\infty/k})^{\omega}) = (\zeta_p-1, \gamma-\kappa(\gamma))\psi(\theta_{L_\infty/k}^{\omega})$. This shows that

$$\psi(\mathrm{Fitt}_{\Lambda[G]}(\mathcal{X}_{L_\infty}^{\omega})) = \mathrm{Fitt}_{\Lambda[\mu_p]}((\mathcal{X}_{L_\infty}^{\omega})_{\psi}) = \psi((I_{L_\infty}\theta_{L_\infty/k})^{\omega})\,.$$

Therefore, $\mathrm{Fitt}_{\Lambda[G]}(\mathcal{X}_{L_\infty}^{\omega})) = (I_{L_\infty}\theta_{L_\infty/k})^{\omega}$ by Lemma 3.3 (now the condition i) is satisfied). This completes the proof of Theorem 0.1. □

REMARK 3.5. We can prove (2.3.2) directly by the same method as above. In this Remark 3.5 we put $\Lambda = \Lambda_{K_\infty}^{\chi}$ and $G = \mathrm{Gal}(L/K)$. Then $\Lambda_{L_\infty}^{\chi} = \Lambda[G]$. We use two maps c, ν as in §2.1. For $\chi \neq \omega$, we use an exact sequence

$$0 \longrightarrow \left(\bigoplus_{v \in P'_{K_\infty}} \mathbf{Z}/e_v\mathbf{Z}\right)^{\chi} \longrightarrow (\mathcal{X}_{L_\infty}^{\chi})_G \longrightarrow \mathcal{X}_{K_\infty}^{\chi} \longrightarrow 0\,,$$

which is obtained from Proposition 1.2 (1). Recall that $S = \{\mathfrak{l} \in P'_k \mid \mathfrak{l}$ is unramified in K, and $\mathfrak{l}$ is ramified in $L\}$. We put

$$S_\chi = \left\{\mathfrak{l} \in S \mid \chi\left(\left(\frac{\mathfrak{l}}{K/k}\right)\right) = 1\right\}$$

where $(\frac{\mathfrak{l}}{K/k})$ is the Frobenius of $\mathfrak{l}$ in $\mathrm{Gal}(K/k)$. We can compute

$$\mathrm{Fitt}_\Lambda\left(\left(\bigoplus_{v \in P'_{K_\infty}} \mathbf{Z}/e_v\mathbf{Z}\right)^{\chi}\right) = \prod_{\mathfrak{l} \in S_\chi}(p, \alpha'_{\mathfrak{l}})$$

where $\alpha'_{\mathfrak{l}} = (1 - \varphi_{\mathfrak{l}}^{-1})^{\chi}$. If $\mathfrak{l} \in S \setminus S_\chi$, $\alpha'_{\mathfrak{l}}$ is a unit of Λ. So $\prod_{\mathfrak{l} \in S}(p, \alpha'_{\mathfrak{l}}) = \prod_{\mathfrak{l} \in S_\chi}(p, \alpha'_{\mathfrak{l}})$. Therefore, using Lemma 3.4 and the main conjecture [18], we have

$$\mathrm{Fitt}_\Lambda((\mathcal{X}_{L_\infty}^{\omega})_G) = \left(\prod_{\mathfrak{l} \in S}(p, \alpha'_{\mathfrak{l}})\right)\theta_{K_\infty/k}^{\chi}\,.$$

On the other hand, by the definition (2.3.1) of Θ,

$$c(\Theta^{\chi}) = \left(\prod_{\mathfrak{l} \in S}\left(1, \frac{p}{\alpha'_{\mathfrak{l}}}\right)\right)\left(\prod_{\mathfrak{l} \in S}\alpha'_{\mathfrak{l}}\right)\theta_{K_\infty/k}^{\chi} = \left(\prod_{\mathfrak{l} \in S_\chi}(p, \alpha'_{\mathfrak{l}})\right)\theta_{K_\infty/k}^{\chi}\,.$$

Therefore, we have $c(\mathrm{Fitt}_{\Lambda[G]}(\mathcal{X}_{L_\infty}^{\chi})) = c(\Theta^{\chi})$.

Next, $\psi(\mathrm{Fitt}_{\Lambda[G]}(\mathcal{X}_{L_\infty}^{\chi})) = (\psi(\theta_{L_\infty/k}^{\chi})) = \psi(\Theta^{\chi})$ can be easily checked. Therefore, by Lemma 3.3 (the condition ii) is satisfied), we obtain

$$\mathrm{Fitt}_{\Lambda[G]}(\mathcal{X}_{L_\infty}^{\chi}) = \Theta^{\chi}\,.$$

3.3. In this subsection, we compare $\mathcal{X}_{L_\infty}$ with the standard Iwasawa module. For a number field L, the standard Iwasawa module X_{L_∞} is defined by

$$X_{L_\infty} = \varprojlim A_{L_n}\,.$$

In this subsection 3.3, we consider the case $G = \mathrm{Gal}(L/K)$ is cyclic of order p.

For simplicity, we only consider the case that $K = k(\mu_p)$ and L/k is unramified outside p for the ω-component (the general case can be treated by the same method). We assume $\mu(X_{K_\infty}^\omega) = 0$. We use the same notation as §1.1. We put $a = \dim_{\mathbf{F}_p} \mathrm{Coker}(\mu_p \longrightarrow \bigoplus_{v \in P_{K_n}} I_v)^\omega$ where I_v is the inertia group of v in $G = \mathrm{Gal}(L_\infty/K_\infty)$ and the map is induced by the reciprocity map of local class field theory. Using the argument in §1.1, we have

$$\hat{H}^{-1}(G, X_{L_\infty}^\omega) = \mathrm{Coker}\left(\mu_p \longrightarrow \bigoplus_{v \in P_{K_n}} I_v\right)^\omega$$

(cf. also Proposition 5.2 in [10]). Hence $\dim_{\mathbf{F}_p} \hat{H}^{-1}(G, X_{L_\infty}^\omega) = a$. We can also get $\dim_{\mathbf{F}_p} \hat{H}^0(G, X_{L_\infty}^\omega) = a + 1$. This together with Kida's formula implies that

$$X_{L_\infty}^\omega \simeq \mathbf{Z}_p[G]^{\lambda - a - 1} \oplus (\mathbf{Z}_p[G]/N_G)^a \oplus \mathbf{Z}_p^{a+1} \tag{3.3.1}$$

(cf. Iwasawa [9] §9) as $\mathbf{Z}_p[G]$-modules where λ is the λ-invariant of $X_{K_\infty}^\omega$.

On the other hand, by Proposition 1.2 (3) we have

$$\hat{H}^{-1}(G, \mathcal{X}_{L_\infty}^\omega) = 0 \quad \text{and} \quad \hat{H}^0(G, \mathcal{X}_{L_\infty}^\omega) \simeq \mathbf{Z}/p\mathbf{Z}\,.$$

This shows that

$$\mathcal{X}_{L_\infty}^\omega \simeq \mathbf{Z}_p[G]^{\lambda - 1} \oplus \mathbf{Z}_p\,. \tag{3.3.2}$$

Therefore, if $a > 0$, $\mathcal{X}_{L_\infty}^\omega$ is not isomorphic to $X_{L_\infty}^\omega$ as a G-module.

We further remark that (ISB) does not hold if $a > 0$ (note that (IDSB) always holds by Theorem 0.1). This can be proved by the same method as Theorem 1.1 in [7]. Suppose that $a > 0$. Then the natural map $(X_{L_\infty}^\omega)_G \longrightarrow X_{K_\infty}^\omega$ has non-trivial kernel by Proposition 5.2 in [10]. This together with Lemma 3.4 implies that

$$\mathrm{Fitt}_{\Lambda_{K_\infty}^\omega}((X_{L_\infty}^\omega)_G) \subsetneq \mathrm{Fitt}_{\Lambda_{K_\infty}^\omega}(X_{K_\infty}^\omega)\,.$$

Since the main conjecture implies $\mathrm{Fitt}_{\Lambda_{K_\infty}^\omega}(X_{K_\infty}^\omega) = \mathrm{char}_{\Lambda_{K_\infty}^\omega}(X_{K_\infty}^\omega) = ((\gamma - \kappa(\gamma))\theta_{K_\infty/k}^\omega)$, we have

$$(\gamma - \kappa(\gamma))\theta_{K_\infty/k}^\omega \notin \mathrm{Fitt}_{\Lambda_{K_\infty}^\omega}((X_{L_\infty}^\omega)_G) = c(\mathrm{Fitt}_{\Lambda_{L_\infty}^\omega}(X_{L_\infty}^\omega))$$

where $c : \Lambda_{L_\infty}^\omega \longrightarrow \Lambda_{K_\infty}^\omega$ is the natural map. Since L_∞/K_∞ is unramified outside p, we know $c((\gamma - \kappa(\gamma))\theta_{L_\infty/k}^\omega) = (\gamma - \kappa(\gamma))\theta_{K_\infty/k}^\omega$. It follows that $(\gamma - \kappa(\gamma))\theta_{L_\infty/k}^\omega) \notin \mathrm{Fitt}_{\Lambda_{L_\infty}^\omega}(X_{L_\infty}^\omega)$. Namely, (ISB) does not hold.

3.4. In this subsection, we prove Corollary 0.2. We will first prove (1). By [17] Proposition 13.26, $A_{L_n}^- \longrightarrow A_{L_\infty}^-$ is injective. This implies that

$$\mathrm{Fitt}_{R_{L_n}}((\mathcal{X}_{L_\infty}^-)_{\mathrm{Gal}(L_\infty/L_n)}) \subset \mathrm{Fitt}_{R_{L_n}}((A_{L_n}^-)^\vee)\,.$$

Since (IDSB) holds, we have

$$c_{L_\infty/L_n}(I_{L_\infty}\theta_{L_\infty/k})^- \subset \mathrm{Fitt}_{R_{L_n}}((A_{L_n}^-)^\vee)\,.$$

On the other hand, by our assumption that all the primes of k above p are ramified in L_n, we have $c_{L_\infty/L_n}(I_{L_\infty}\theta_{L_\infty/k}) = I_{L_n}\theta_{L_n/k}$ where c_{L_∞/L_n} is the natural restriction map. Since $I_{L_n}\theta_{L_n/k}$ is in the minus part of R_{L_n} (namely, $(I_{L_n}\theta_{L_n/k})^+ = 0$), we get (DSB) for L_n/k.

Next, we will prove (2). As we have seen above,

$$c_{L_\infty/L}(I_{L_\infty}\theta_{L_\infty/k})^- \subset \mathrm{Fitt}_{R_L}((A_L^-)^\vee)$$

holds. We have

$$c_{L_\infty/L}(a\theta_{L_\infty/k}) = \prod_{\mathfrak{p}\in T}(1-\varphi_{\mathfrak{p}}^{-1})c_{L_\infty/L}(a)\theta_{L/k}$$

for $a \in I_{L_\infty}$ where T is the set of primes of k which are ramified in L_∞ and unramified in L. By our assumption (i) and (ii), if $\mathfrak{p}$ is in T, the primes above $\mathfrak{p}$ do not split in L/L^+. Therefore, $(1-\varphi_{\mathfrak{p}}^{-1})^-$ is a unit, and $\prod_{\mathfrak{p}\in T}(1-\varphi_{\mathfrak{p}}^{-1})^-$ is a unit. Since $c_{L_\infty/L}(I_{L_\infty}) = I_L$, we obtain (DSB). On the other hand, since $\Gamma(L/k)$ is cyclic, we know

$$\mathrm{Fitt}_{R_L}(A_L^-) = \mathrm{Fitt}_{R_L}((A_L^-)^\vee)\,.$$

This implies that (SB) is also true.

3.5. In this subsection, we study the case that $\Gamma(L/k)$ is not cyclic, and will prove Theorem 0.3 and Corollary 0.5.

PROOF OF THEOREM 0.3. Put $K = k(\mu_p)$, $G = \mathrm{Gal}(L/K) = \mathrm{Gal}(L_0/k)$, and $\Lambda = \Lambda_{K_\infty}^\omega$. Then $\Lambda_{L_\infty}^\omega = \Lambda[G]$. Let c be the restriction map in §2.1. Proposition 1.2 (3) implies that

$$\hat{H}^0(G, \mathcal{X}_{L_\infty}^\omega) = \hat{H}^{-1}(G, A_{L_\infty}^\omega)^\vee = \Big(\bigwedge^2 G\Big)(1)\,.$$

It follows from Lemma 3.1 that

$$0 \longrightarrow \Big(\bigwedge^2 G\Big)(1) \longrightarrow (\mathcal{X}_{L_\infty}^\omega)_G \xrightarrow{f} \mathcal{X}_{K_\infty}^\omega \longrightarrow G(1) \longrightarrow 0$$

is exact. By our assumption on G, we have $\bigwedge^2 G \neq 0$. Since $\mathcal{X}_{K_\infty}^\omega$ does not contain a nontrivial finite submodule, neither does Image f. Therefore, by Lemma 3.4 and the main conjecture [18], we obtain

$$\begin{aligned}\mathrm{Fitt}_\Lambda((\mathcal{X}_{L_\infty}^\omega)_G) &= \mathrm{Fitt}_\Lambda\Big(\Big(\bigwedge^2 G\Big)(1)\Big)\,\mathrm{char}_\Lambda(\mathrm{Image}\, f)\\ &\subset (p, \gamma-1)\,\mathrm{char}_\Lambda(\mathrm{Image}\, f)\end{aligned}$$

$$\begin{aligned}&= (p, \gamma - 1)\,\mathrm{char}_{\Lambda}(\mathcal{X}^{\omega}_{K_\infty})\\ &= (p, \gamma - 1)(\gamma - \kappa(\gamma))\theta^{\omega}_{K_\infty/k}\,.\end{aligned}$$

If $(\gamma - \kappa(\gamma))\theta^{\omega}_{L_\infty/k}$ was in $\mathrm{Fitt}_{\Lambda_{L_\infty}}(\mathcal{X}^{\omega}_{L_\infty})$, $c((\gamma - \kappa(\gamma))\theta^{\omega}_{L_\infty/k}) = (\gamma - \kappa(\gamma))\theta^{\omega}_{K_\infty/k}$ would be in

$$c(\mathrm{Fitt}_{\Lambda_{L_\infty}}(\mathcal{X}^{\omega}_{L_\infty})) = \mathrm{Fitt}_{\Lambda}((\mathcal{X}^{\omega}_{L_\infty})_G) \subset (p, \gamma - 1)(\gamma - \kappa(\gamma))\theta^{\omega}_{K_\infty/k}\,.$$

But this is impossible. Therefore, $(\gamma - \kappa(\gamma))\theta^{\omega}_{L_\infty/k}$ is not in $\mathrm{Fitt}_{\Lambda_{L_\infty}}(\mathcal{X}^{\omega}_{L_\infty})$. Thus, we have obtained $(\gamma - \kappa(\gamma))\theta_{L_\infty/k} \notin \mathrm{Fitt}_{\Lambda_{L_\infty}}(\mathcal{X}_{L_\infty})$.

PROOF OF COROLLARY 0.5. The statement (1) follows from Theorem 0.3 and Theorem 2.1 in [7].

Next, we will prove (2). We consider $X_{L_\infty} = \varprojlim A_{L_n}$ and $X_{K_\infty} = \varprojlim A_{K_n}$. By Corollary 5.3 in [10], we have an exact sequence

$$\mathbf{Z}_p(1) \longrightarrow \left(\bigoplus_{v|p} I_v(L_\infty/K_\infty)\right)^{\omega} \longrightarrow (X^{\omega}_{L_\infty})_{\mathrm{Gal}(L_\infty/K_\infty)} \longrightarrow X^{\omega}_{K_\infty} \longrightarrow 0$$

where v runs over all primes of K_∞ above p and $I_v(L_\infty/K_\infty)$ is the inertia group of $\mathrm{Gal}(L_\infty/K_\infty)$ at v. Put

$$\mathcal{P} = \{\mathfrak{P} \in P_{p,k_\infty} \mid \mathfrak{P} \text{ splits completely in } k_\infty(\mu_p) \text{ and ramified in } L_0(\mu_{p^\infty})\}\,.$$

We have

$$\left(\bigoplus_{v|p} I_v(L_\infty/K_\infty)\right)^{\omega} \simeq \bigoplus_{\mathfrak{P}\in\mathcal{P}} I_{\mathfrak{P}}(L_{0,\infty}/k_\infty)$$

where $I_{\mathfrak{P}}(L_{0,\infty}/k_\infty)$ is the inertia group of $\mathrm{Gal}(L_{0,\infty}/k_\infty)$ at $\mathfrak{P}$. We put $N = \mathrm{Coker}(\mathbf{Z}_p(1) \longrightarrow \bigoplus_{\mathfrak{P}\in\mathcal{P}} I_{\mathfrak{P}}(L_{0,\infty}/k_\infty))$. By our assumption $\#\mathcal{P} \geq 2$, we have $N \neq 0$.

We apply Lemma 3.4 to the exact sequence

$$0 \longrightarrow N \longrightarrow (X^{\omega}_{L_\infty})_{\mathrm{Gal}(L_\infty/K_\infty)} \longrightarrow X^{\omega}_{K_\infty} \longrightarrow 0$$

to obtain

$$\mathrm{Fitt}_{\Lambda}((X^{\omega}_{L_\infty})_G) = \mathrm{Fitt}_{\Lambda}(N)(\gamma - \kappa(\gamma))\theta^{\omega}_{K_\infty/k}$$

(using the main conjecture). Since $c(\theta_{L_\infty/k}) = \theta_{K_\infty/k}$ and $\mathrm{Fitt}_{\Lambda}(N) \neq \Lambda$, we have

$$(\gamma - \kappa(\gamma))\theta^{\omega}_{L_\infty/k} \notin \mathrm{Fitt}_{\Lambda_{L_\infty}}(X^{\omega}_{L_\infty})$$

by the same argument as the proof of Theorem 0.3. By Theorem 2.1 in [7], for sufficiently large n, we have

$$(\gamma - \kappa(\gamma))\theta_{L_0(\mu_{p^n})/k} \notin \mathrm{Fitt}_{R_{L_0(\mu_{p^n})}}(A_{L_0(\mu_{p^n})})\,.$$

This completes the proof of Corollary 0.5.

References

[1] BROWN, K. S., *Cohomology of groups*, Graduate Texts in Math. **87**, Springer-Verlag, 1982.

[2] CORNACCHIA, P. and GREITHER, C., Fitting ideals of class groups of real fields with prime power conductor, J. Number Theory **73** (1998), 459–471.

[3] DELIGNE, P. and RIBET, K., Values of abelian L-functions at negative integers over totally real fields, Invent. math. **59** (1980), 227–286.

[4] GREITHER, C., Arithmetic annihilators and Stark-type conjectures, *Stark's Conjectures: Recent Work and New Directions*, Contemporary Math. **358** (2004), 55–78.

[5] GREITHER, C., Computing Fitting ideals of Iwasawa modules, Math. Zeitschrift **246** (2004), 733–767.

[6] GREITHER C., Determining Fitting ideals of minus class groups via the equivariant Tamagawa number conjecture, Compositio Math. **143** (2007), 1399–1426.

[7] GREITHER C. and KURIHARA M., Stickelberger elements, Fitting ideals of class groups of CM fields, and dualisation, Math. Zeitschrift **260** (2008), 905–930.

[8] IWASAWA K., On $\mathbf{Z}_\ell$-extensions of algebraic number fields, Ann. of Math. **98** (1973), 246–326.

[9] IWASAWA K., Riemann-Hurwitz formula and p-adic Galois representations for number fields, Tôhoku Math. J. **33** (1981), 263–288.

[10] KURIHARA, M., Iwasawa theory and Fitting ideals, J. reine angew. Math. **561** (2003), 39–86.

[11] KURIHARA, M., On the structure of ideal class groups of CM-fields, Documenta Mathematica, Extra Volume Kato (2003), 539–563.

[12] KURIHARA, M. and MIURA T., Stickelberger ideals and Fitting ideals of class groups for abelian number fields, Math. Annalen **350** (2011), 549–575.

[13] MAZUR, B. and WILES, A., Class fields of abelian extensions of **Q**, Invent. math. **76** (1984), 179–330.

[14] NORTHCOTT, D. G., *Finite free resolutions*, Cambridge Univ. Press, Cambridge New York, 1976.

[15] SERRE, J.-P., *Corps Locaux*, Hermann, Paris, 1968 (troisième édition).

[16] SERRE, J.-P., Sur le résidu de la fonction zêta p-adique, Comptes Rendus Acad. Sc. Paris, **287** (1978), Série A, 183–188.

[17] WASHINGTON, L., *Introduction to cyclotomic fields*, Graduate Texts in Math. **83**, Springer-Verlag, 1982.

[18] WILES, A., The Iwasawa conjecture for totally real fields, Ann. of Math. **131** (1990), 493–540.

[19] WINGBERG, K., Duality theorems for Γ-extensions of algebraic number fields, Compos. Math. **55** (1985), 333–381.

Present Address:
DEPARTMENT OF MATHEMATICS,
KEIO UNIVERSITY,
3–14–1 HIYOSHI, KOHOKU-KU, YOKOHAMA, 223–8522 JAPAN.
e-mail: kurihara@math.keio.ac.jp