TOKYO J. MATH.
VOL. 39, NO. 3, 2017

Fitting Ideals of Iwasawa Modules and of the Dual of Class Groups

Dedicated to Professor Ken-ichi SHINODA

Cornelius GREITHER and Masato KURIHARA

Universität der Bundeswehr München and Keio University

Abstract. In this paper we study some problems related to a refinement of Iwasawa theory, especially questions about the Fitting ideals of several natural Iwasawa modules and of the dual of the class groups, as a sequel to our previous papers [8], [3]. Among other things, we prove that the annihilator of $\mathbf{Z}_p(1)$ times the Stickelberger element is not in the Fitting ideal of the dualized Iwasawa module if the p-component of the bottom Galois group is elementary p-abelian with p-rank ≥ 4. Our results can be applied to the case that the base field is $\mathbf{Q}$.

1. Introduction

1-1. Suppose that k is a totally real number field, and at first suppose that L/k is a finite abelian extension of totally real number fields. We fix an odd prime number p and denote by k_∞/k, L_∞/L the cyclotomic $\mathbf{Z}_p$-extensions. We assume $L \cap k_\infty = k$. Suppose that S is a finite set of primes of k, which contains all ramifying primes in L_∞. Note that S automatically contains S_p, the set of primes of k above p. Let $\mathcal{X}_{L,S}$ be the S-ramified Iwasawa module, namely the Galois group of $\mathcal{L}_{L_\infty,S}/L_\infty$ which is the maximal abelian pro-p extension unramified outside S. Then the main conjecture which was proved by Wiles in [14] Theorem 1.3 can be stated in terms of $\mathcal{X}_{L,S}$. Indeed the main conjecture (roughly) says that for any character χ of $\mathrm{Gal}(L/k)$ the characteristic ideal of the χ-quotient of $\mathcal{X}_{L,S}$ is generated by the χ-component of the S-truncated p-adic L-function $\Theta_{L_\infty/k,S}$ (for the precise statement, see §4). Since the characteristic ideal of a power series ring is closely related to the Fitting ideal, we are naturally led to the question whether (the annihilator of $\mathbf{Z}_p$ times) the S-truncated p-adic L-function $\Theta_{L_\infty/k,S}$ is in the Fitting ideal of the Λ_L-module $\mathcal{X}_{L,S}$ where $\Lambda_L = \mathbf{Z}_p[[\mathrm{Gal}(L_\infty/k)]]$ (concerning general properties of Fitting ideals, see [10]). Using our previous results, we can show that the answer is always No if the p-component of $\mathrm{Gal}(L/k)$ is not cyclic. Actually, we can describe the Fitting ideal of $\mathcal{X}_{L,S}$, using $\Theta_{L_\infty/k,S}$ (see Theorem 4.1). Theorem 4.1 gives *a more precise link* between the S-ramified Iwasawa module $\mathcal{X}_{L,S}$ and the p-adic L-function $\Theta_{L_\infty/k,S}$ than the usual main conjecture.

Received September 2, 2015; revised February 6, 2016
The second author is partially supported by JSPS Core-to-core program, "Foundation of a Global Research Cooperative Center in Mathematics focused on Number Theory and Geometry".

When we take S to be minimal, namely the set of the ramifying primes of k in L_∞, we simply write $\Theta_{L_\infty/k}$ for $\Theta_{L_\infty/k,S}$. Next we study the p-ramified Iwasawa module, namely the Galois group of $\mathcal{L}_{L_\infty,S_p}/L_\infty$ which is the maximal abelian pro-p extension unramified outside p. We write $X_L = \mathrm{Gal}(\mathcal{L}_{L_\infty,S_p}/L_\infty)$, and study the Fitting ideal of the Λ_L-module X_L, especially the problem whether $(\gamma-1)\Theta_{L_\infty/k}$ is in the Fitting ideal of X_L or not, where γ is a generator of $\mathrm{Gal}(L_\infty/L)$. Our main theorem in this direction is Theorem 5.1 in §5.

We are interested in this problem because it is equivalent to a problem on the minus class group, which we will explain in the next subsection.

1-2. For a number field F, we denote by Cl_F the class group and $A_F = \mathrm{Cl}_F \otimes \mathbf{Z}_p$. Let μ_p be the group of p-th roots of unity in an algebraic closure, and put $L' = L(\mu_p)$. Suppose that L/k is a finite abelian p-extension, for simplicity, in this subsection. Hence L is still totally real and L' is a CM-field; we keep the assumption that k is totally real all the time. Let $\omega : \mathrm{Gal}(L'/k) \longrightarrow \mathbf{Z}_p^\times$ be the Teichmüller character, which gives the action on μ_p. We denote by L'_∞/L' the cyclotomic $\mathbf{Z}_p$-extension, and define $A_{L'_\infty}$ to be the inductive limit of $A_{L'_n}$ where L'_n is the n-th layer of L'_∞/L'. Consider the ω-component $A^\omega_{L'_\infty}$. Then the Kummer pairing gives a well-known isomorphism

$$(A^\omega_{L'_\infty})^\vee(1) \simeq X_L$$

of Galois modules (see [13] Proposition 13.32), where $(A^\omega_{L'_\infty})^\vee$ is the Pontrjagin dual and (1) is the Tate twist. Put $\Lambda_{L'} = \mathbf{Z}_p[[\mathrm{Gal}(L'_\infty/k)]]$. We consider the cogredient action of the Galois group on the Pontrjagin dual $(A_{L'_\infty})^\vee$, and regard it as a $\Lambda_{L'}$-module. Let γ be a generator of $\mathrm{Gal}(L'_\infty/L')$ and κ the cyclotomic character, and $\theta_{L'_\infty/k}$ the Stickelberger element (the projective limit of $\theta_{L'_n/k}$ for $n \gg 0$; for more details, see §6). Then $(\gamma-\kappa(\gamma))\theta_{L'_\infty/k}$ is in $\Lambda_{L'}$. Using a consequence of Theorem 5.1 and the above duality isomorphism, we prove in §6 the following as a part of Theorem 6.1.

THEOREM. *Suppose that* $\mathrm{Gal}(L/k) \simeq (\mathbf{Z}/p\mathbf{Z})^{\oplus s}$ *with* $s \geq 4$. *Then we always have*

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

In previous work, see [3], it was shown: If L/k is *unramified outside* p and $\mathrm{Gal}(L/k)$ is not cyclic, then we always get this negative result. In this paper, we prove the above theorem with *no assumption on the ramification* in L'/k.

It was a surprise for us that *the above Theorem can be applied to the case* $k = \mathbf{Q}$. In our previous work, if L/k is unramified outside p and $\mathrm{Gal}(L/k)$ is not cyclic, then k cannot be $\mathbf{Q}$.

A key result in the proof of Theorems 6.1 and 5.1 is Theorem 3.1 which determines the structure of $(X_L)_{\mathrm{Gal}(L/k)}$ for elementary p-abelian $\mathrm{Gal}(L/k)$. In particular, we prove that the $\mathbf{Z}_p$-torsion part of $(X_L)_{\mathrm{Gal}(L/k)}$ is annihilated by p in this setting.

1-3. We study finite abelian extensions over $\mathbf{Q}$ in §§7 and 8. As a corollary of the above

Theorem, we prove in Corollary 7.1 a similar negative result at finite level; especially for a certain cyclotomic field $L = \mathbf{Q}(\mu_m)$ we can show that

$$(\mathrm{Ann}_{\mathbf{Z}[\mathrm{Gal}(L/\mathbf{Q})]}(\mu_m)\theta_{L/\mathbf{Q}}) \otimes \mathbf{Z}_p \not\subset \mathrm{Fitt}_{\mathbf{Z}_p[\mathrm{Gal}(L/\mathbf{Q})]}(A_L^\vee)$$

(see Corollary 7.2 and Remark 7.3). Note that the main result of [9] implies

$$(\mathrm{Ann}_{\mathbf{Z}[\mathrm{Gal}(L/\mathbf{Q})]}(\mu_m)\theta_{L/\mathbf{Q}}) \otimes \mathbf{Z}_p \subset \mathrm{Fitt}_{\mathbf{Z}_p[\mathrm{Gal}(L/\mathbf{Q})]}(A_L)$$

for any m and p. Such a negative result is surprising because people sometimes thought that the Pontrjagin dual of the class group behaved better than the class group. We also note that the above result shows that the Fitting ideal of the dual of the class group of a cyclotomic field does not coincide with the Stickelberger ideal of Iwasawa-Sinnott in [11], in general.

Combining the main results in [1] and [9], we know that

$$\mathrm{Fitt}_{\mathbf{Z}_p[\mathrm{Gal}(L/\mathbf{Q})]}((A_L^-)^\vee) = \mathrm{Fitt}_{\mathbf{Z}_p[\mathrm{Gal}(L/\mathbf{Q})]}(A_L^-)$$

for any finite abelian $L/\mathbf{Q}$ such that $\mu_p \not\subset L$. But the above negative result shows that this equality does not hold in general if $\mu_p \subset L$. We discuss this problem in §8 in the case $\mu_p \subset L$ and $s = 2$ (the latter simply meaning that the p-component of $\mathrm{Gal}(L/\mathbf{Q})$ is $(\mathbf{Z}/p\mathbf{Z})^{\oplus 2}$). We give in Proposition 8.1 a very simple criterion for this equality to hold for a certain family of abelian fields. We also study a numerical example in detail in Remark 8.4 for which

$$\mathrm{Fitt}_{\mathbf{Z}_p[\mathrm{Gal}(L/\mathbf{Q})]}((A_L^-)^\vee) \subsetneq \mathrm{Fitt}_{\mathbf{Z}_p[\mathrm{Gal}(L/\mathbf{Q})]}(A_L^-)$$

holds.

Concerning the Stickelberger ideal for cyclotomic fields, the book [6], which was based on the lectures by K. Iwasawa and W. Sinnott at Princeton in 1976, has been a well-received and widely read reference in Japan. As we see from the acknowledgement in that book, K. Shinoda suggested its publication, read the manuscript thoroughly, and gave many helpful comments. The authors believe that the importance and the arithmetical content of the Stickelberger ideal stem to a considerable extent from its beautiful relation to the Fitting ideal of the class group (cf. [7], [1]). In this sense, the theory of Stickelberger ideals has seen some new developments since the time this book was written. It is our great pleasure to dedicate this paper to K. Shinoda.

2. A fundamental exact sequence

In this paper, we fix an odd prime p. For a number field F, we denote by F_∞/F the cyclotomic $\mathbf{Z}_p$-extension.

Suppose that L/K is a finite abelian extension and put $G = \mathrm{Gal}(L/K)$. Consider the maximal abelian pro-p extension $\mathcal{L}_{L_\infty,S_p}/L_\infty$ which is unramified outside p, and put $X_L = \mathrm{Gal}(\mathcal{L}_{L_\infty,S_p}/L_\infty)$. We are interested in the Tate cohomology $\hat{H}^i(G, X_L)$. The goal of this section is to prove the following proposition, which we call the fundamental exact sequence for X_L in this paper.

PROPOSITION 2.1 (Fundamental exact sequence for X_L). *Let L/K be a finite abelian p-extension of totally real number fields such that $L \cap K_\infty = K$ and $G = \mathrm{Gal}(L/K)$. Then we have an exact sequence*

$$0 \longrightarrow \bigwedge^2 G \longrightarrow \hat{H}^{-1}(G, X_L) \longrightarrow \bigoplus_{v \in S'_{K_\infty}} I_v \longrightarrow G \longrightarrow \hat{H}^0(G, X_L) \longrightarrow 0\,,$$

where S'_{K_∞} is the set of non p-adic primes of K_∞ which are ramified in L_∞/K_∞, and I_v is the inertia subgroup of v in $G = \mathrm{Gal}(L_\infty/K_\infty)$.

REMARK 2.2. Put $K' = K(\mu_p)$ and $L' = L(\mu_p)$. We denote by L'_n the n-th layer of L'_∞/L' and by $A^\omega_{L'_n}$ the Teichmüller part of the p-component of the ideal class group of L'_n. Then, by the well-known duality (see [13] Proposition 13.32), X_L is isomorphic to the Pontrjagin dual of the direct limit $\varinjlim A^\omega_{L'_n}$ for which we write $A^\omega_{L'_\infty}$. Namely we have

$$X_L \simeq (A^\omega_{L'_\infty})^\vee(1)$$

where (1) is the Tate twist. If we use this isomorphism, Proposition 2.1 is a consequence of Lemma 1.1 in [8]. But we give here a different proof (though we use the above isomorphism to prove the following Proposition 2.3).

Before we prove Proposition 2.1, we need the following description of $\hat{H}^{-1}(G, X_L)$.

PROPOSITION 2.3. *Let L''_∞/K_∞ be the maximal subextension of L_∞/K_∞, which is unramified outside p. We put $\mathcal{G} = \mathrm{Gal}(L''_\infty/K_\infty)$. Then there is an exact sequence*

$$0 \longrightarrow \hat{H}^{-1}(G, X_L) \longrightarrow (X_L)_G \longrightarrow X_K \longrightarrow \mathcal{G} \longrightarrow 0$$

where $(X_L)_G$ is the module of G-coinvariants of X_L, and $(X_L)_G \longrightarrow X_K$ is induced by the restriction map.

PROOF. Let L'_n be as in Remark 2.2, and define K'_n similarly. Then the cokernel of the norm map $\mathrm{Cl}_{L'_n} \longrightarrow \mathrm{Cl}_{K'_n}$ between the class groups of L'_n and K'_n is isomorphic to the Galois group of the maximal unramified subextension of L'_n/K'_n. In particular, it is a quotient of G, and independent of n when n is sufficiently large. Therefore, the cokernel of the norm map $A^\omega_{L'_\infty} \longrightarrow A^\omega_{K'_\infty}$ is finite. Using the above duality, we know that the kernel of the canonical map $X_K \longrightarrow X_L$ is finite. On the other hand, by Theorem 18 in Iwasawa [4] we know that X_K has no nontrivial finite $\mathbf{Z}_p[[\mathrm{Gal}(K_\infty/K)]]$-submodule. This shows that $X_K \longrightarrow X_L$ is injective. Therefore, $\hat{H}^{-1}(G, X_L)$ coincides with the kernel of $(X_L)_G \longrightarrow X_K$. By definition, the cokernel of this map is $\mathcal{G}$. □

Now we prove the fundamental exact sequence (Proposition 2.1). Let S_p be the set of p-adic primes of K, and S' the set of non p-adic ramifying primes of K in L. We put

$S = S_p \cup S'$. Let $\mathcal{O}_{K_\infty,S}$ be the ring of S-integers in K_∞. We denote by $H^i(\mathcal{O}_{K_\infty,S}, \mathbf{Q}_p/\mathbf{Z}_p)$ the étale cohomology $H^i_{et}(\mathrm{Spec}\, \mathcal{O}_{K_\infty,S}, \mathbf{Q}_p/\mathbf{Z}_p)$, which is the same as the Galois cohomology $H^i(\mathcal{M}/K_\infty, \mathbf{Q}_p/\mathbf{Z}_p)$ where $\mathcal{M}/K_\infty$ is the maximal extension unramified outside S. We define $H^i(\mathcal{O}_{K_\infty,S_p}, \mathbf{Q}_p/\mathbf{Z}_p)$, $H^i(\mathcal{O}_{L_\infty,S}, \mathbf{Q}_p/\mathbf{Z}_p)$, $H^i(\mathcal{O}_{L_\infty,S_p}, \mathbf{Q}_p/\mathbf{Z}_p)$, similarly. Suppose that $v_0 \in S'$ and v is a prime of K_∞ above v_0. Since v_0 is ramified in L, we must have $N(v_0) \equiv 1 \pmod{p}$ where $N(v_0)$ is the norm of the prime v_0. Therefore, the residue field $\kappa(v)$ of v contains all p-power roots of unity in an algebraic closure of $\kappa(v)$. Let $I_v(\mathcal{M}/K_\infty)$ be the inertia group of v in $\mathrm{Gal}(\mathcal{M}/K_\infty)$. Since v is prime to p, $I_v(\mathcal{M}/K_\infty)$ is isomorphic to $\mathbf{Z}_p(1)$ where (1) means the Tate twist, and

$$\begin{aligned} H^0(\kappa(v), H^1(I_v(\mathcal{M}/K_\infty), \mathbf{Q}_p/\mathbf{Z}_p)) &= H^0(\kappa(v), \mathbf{Q}_p/\mathbf{Z}_p(-1)) \\ &= \mathbf{Q}_p/\mathbf{Z}_p(-1). \end{aligned}$$

Since the weak Leopoldt conjecture is true, we know $H^2(\mathcal{O}_{K_\infty,S_p}, \mathbf{Q}_p/\mathbf{Z}_p) = 0$. Therefore, the localization sequence of étale cohomology gives a short exact sequence

$$\begin{aligned} (1) \qquad & 0 \longrightarrow H^1(\mathcal{O}_{K_\infty,S_p}, \mathbf{Q}_p/\mathbf{Z}_p) \longrightarrow H^1(\mathcal{O}_{K_\infty,S}, \mathbf{Q}_p/\mathbf{Z}_p) \\ & \longrightarrow \bigoplus_{v \in S'_{K_\infty}} \mathbf{Q}_p/\mathbf{Z}_p(-1) \longrightarrow 0\,. \end{aligned}$$

Using the same exact sequence for L_∞ and the spectral sequence, we have a commutative diagram of exact sequences

$$\begin{array}{ccccccc} & & 0 & & 0 & & 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ & & \mathcal{G}^\vee & & H^1(G, \mathbf{Q}_p/\mathbf{Z}_p) & & \bigoplus_v \mathbf{Z}/e_v\mathbf{Z}(-1) \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 \to & H^1(\mathcal{O}_{K_\infty,S_p}, \mathbf{Q}_p/\mathbf{Z}_p) & \to & H^1(\mathcal{O}_{K_\infty,S}, \mathbf{Q}_p/\mathbf{Z}_p) & \to & \bigoplus_v \mathbf{Q}_p/\mathbf{Z}_p(-1) & \to 0 \\ & \downarrow & & \downarrow & & \downarrow & \\ 0 \to & H^1(\mathcal{O}_{L_\infty,S_p}, \mathbf{Q}_p/\mathbf{Z}_p)^G & \to & H^1(\mathcal{O}_{L_\infty,S}, \mathbf{Q}_p/\mathbf{Z}_p)^G & \xrightarrow{f} & (\bigoplus_w \mathbf{Q}_p/\mathbf{Z}_p(-1))^G & \\ & \downarrow & & \downarrow & & \downarrow & \\ & \hat{H}^{-1}(G, X_L)^\vee & & H^2(G, \mathbf{Q}_p/\mathbf{Z}_p) & & 0 & \\ & \downarrow & & \downarrow & & & \\ & 0 & & 0 & & & \end{array} .$$

Here, $H^1(\mathcal{O}_{K_\infty,S_p}, \mathbf{Q}_p/\mathbf{Z}_p)$, $H^1(\mathcal{O}_{L_\infty,S_p}, \mathbf{Q}_p/\mathbf{Z}_p)^G$ are the Pontrjagin duals of X_K and $(X_L)_G$, respectively, so Proposition 2.3 assures the exactness of the first vertical sequence. The second vertical sequence is exact by the Serre-Hochschild spectral sequence. We note that S contains all primes which ramify in L_∞/K_∞. We also note that $H^1(G, \mathbf{Q}_p/\mathbf{Z}_p)$, $H^2(G, \mathbf{Q}_p/\mathbf{Z}_p)$ are the Pontrjagin duals of G and $\bigwedge^2 G$, respectively. In the third vertical sequence, v runs over S'_{K_∞} and w runs over S'_{L_∞} which is the set of primes of L_∞ above S'.

We have $(\bigoplus_w \mathbf{Q}_p/\mathbf{Z}_p(-1))^G \simeq \bigoplus_v \mathbf{Q}_p/\mathbf{Z}_p(-1)$ and the third vertical map is the multiplication by e_v for the v-component. This shows that the third map in the third vertical sequence is surjective. This implies that f (which is the third horizontal map in the second horizontal sequence) is surjective. Therefore by the snake lemma and dualization, we obtain an exact sequence

$$0 \longrightarrow \bigwedge^2 G \longrightarrow \hat{H}^{-1}(G, X_L) \longrightarrow \bigoplus_{v \in S'_{K_\infty}} \mathbf{Z}/e_v\mathbf{Z}(1) \longrightarrow G \longrightarrow \mathcal{G} \longrightarrow 0\,.$$

We note that the inertia group I_v of v in G is isomorphic to $\mathbf{Z}/e_v\mathbf{Z}(1)$. Hence, in order to prove Proposition 2.1, we have only to prove

$$\hat{H}^0(G, X_L) \simeq \mathcal{G}\,. \tag{2}$$

We need the following lemma.

LEMMA 2.4. *We have an isomorphism*

$$X_K \xrightarrow{\simeq} X_L^G$$

where the right hand side is the G-invariant part of X_L.

PROOF. By induction on $\#G$, we may assume that $\#G = p$, namely $G \simeq \mathbf{Z}/p\mathbf{Z}$. Let $\mathcal{X}_{K,S}$ be the Galois group of $\mathcal{L}_{K_\infty,S}/K_\infty$ which is the maximal abelian pro-p extension unramified outside S. Taking the dual of the exact sequence (1), we have an exact sequence

$$0 \longrightarrow \bigoplus_{v \in S'_{K_\infty}} I_v(\mathcal{M}_S/K_\infty) \longrightarrow \mathcal{X}_{K,S} \longrightarrow X_K \longrightarrow 0$$

where $I_v(\mathcal{M}_S/K_\infty) \simeq \mathbf{Z}_p(1)$ is the inertia group of v in $\mathcal{X}_{K,S}$. As we proved in the proof of Proposition 2.3, $X_K \longrightarrow X_L$ is injective. We define $\mathcal{X}_{L,S}$ similarly. Then the above injectivity implies that the canonical map $\mathcal{X}_{K,S} \longrightarrow \mathcal{X}_{L,S}$ is also injective. Taking the dual, we know that the corestriction map $H^1(\mathcal{O}_{L_\infty,S}, \mathbf{Q}_p/\mathbf{Z}_p) \xrightarrow{\mathrm{Cor}} H^1(\mathcal{O}_{K_\infty,S}, \mathbf{Q}_p/\mathbf{Z}_p)$ is surjective.

By the Serre-Hochschild spectral sequence, we have an isomorphism

$$H^1(G, H^1(\mathcal{O}_{L_\infty,S}, \mathbf{Q}_p/\mathbf{Z}_p)) \simeq H^3(G, \mathbf{Q}_p/\mathbf{Z}_p)\,.$$

The latter group is isomorphic to $H^1(G, \mathbf{Q}_p/\mathbf{Z}_p)$ because G is cyclic. Therefore, we have

$$H^1(G, H^1(\mathcal{O}_{L_\infty,S}, \mathbf{Q}_p/\mathbf{Z}_p)) \simeq \mathbf{Z}/p\mathbf{Z}\,.$$

This shows that the kernel of

$$H^1(\mathcal{O}_{L_\infty,S}, \mathbf{Q}_p/\mathbf{Z}_p)_G \xrightarrow{\mathrm{Cor}} H^1(\mathcal{O}_{K_\infty,S}, \mathbf{Q}_p/\mathbf{Z}_p) \xrightarrow{\mathrm{Res}} H^1(\mathcal{O}_{L_\infty,S}, \mathbf{Q}_p/\mathbf{Z}_p)$$

is of order p where M_G means the module of G-coinvariants of M. Since the kernel of the restriction map $H^1(\mathcal{O}_{K_\infty,S}, \mathbf{Q}_p/\mathbf{Z}_p) \longrightarrow H^1(\mathcal{O}_{L_\infty,S}, \mathbf{Q}_p/\mathbf{Z}_p)$ is $H^1(G, \mathbf{Q}_p/\mathbf{Z}_p)$ which is of order p, we know that the corestriction map gives an isomorphism

$$H^1(\mathcal{O}_{L_\infty,S}, \mathbf{Q}_p/\mathbf{Z}_p)_G \simeq H^1(\mathcal{O}_{K_\infty,S}, \mathbf{Q}_p/\mathbf{Z}_p)\,.$$

Consider the commutative diagram

$$\begin{array}{ccc} H^1(\mathcal{O}_{L_\infty,S_p}, \mathbf{Q}_p/\mathbf{Z}_p)_G & \longrightarrow & H^1(\mathcal{O}_{L_\infty,S}, \mathbf{Q}_p/\mathbf{Z}_p)_G \\ \downarrow & & \downarrow \\ H^1(\mathcal{O}_{K_\infty,S_p}, \mathbf{Q}_p/\mathbf{Z}_p) & \longrightarrow & H^1(\mathcal{O}_{K_\infty,S}, \mathbf{Q}_p/\mathbf{Z}_p)\,. \end{array}$$

We have just seen that the right vertical arrow is bijective. The lower horizontal arrow is injective by definition. The upper horizontal arrow is also injective because of the surjectivity of f in the previous commutative diagram and of the cyclicity of G. Therefore, we get the injectivity of the left vertical arrow. Taking the dual, we know that $X_K \longrightarrow X_L^G$ is surjective.

As we have mentioned, we proved the injectivity of $X_K \longrightarrow X_L$ in the proof of Proposition 2.3. Therefore, we get the bijectivity of $X_K \longrightarrow X_L^G$. □

We go back to the proof of (2). By Lemma 2.4, we have

$$\hat{H}^0(G, X_L) \simeq \mathrm{Coker}(X_L \longrightarrow X_K)\,.$$

Therefore, Proposition 2.3 implies (2). This completes the proof of (2) and Proposition 2.1.

REMARK 2.5. We note that we did not assume the vanishing of the μ-invariant of L to prove the fundamental exact sequence in Proposition 2.1. The argument becomes much simpler if one is willing to assume $\mu = 0$.

3. The torsion submodule of $(X_L)_G$

In this section, we assume the same condition as in Proposition 2.1. Namely, L/K is a finite abelian p-extension of totally real number fields such that $L \cap K_\infty = K$. Recall that X_K, X_L are the Galois groups of the maximal abelian pro-p extensions unramified outside p over K_∞, L_∞, respectively. We also use the notation $\mathcal{G} = \mathrm{Gal}(L''_\infty/K_\infty)$ in the previous section where L''_∞/K_∞ is the maximal subextension of L_∞/K_∞, which is unramified outside p.

THEOREM 3.1. *Let L/K be as above and $G = \mathrm{Gal}(L/K)$. We assume that G is elementary abelian and $G \simeq (\mathbf{Z}/p\mathbf{Z})^{\oplus s}$ for some $s \in \mathbf{Z}_{>0}$. We assume that the μ-invariant of X_K is zero, and denote the λ-invariant by λ_K. Let S'_{K_∞} be the set of primes of non p-adic primes of K_∞ that are ramified in L_∞, $n(L/K) = \#S'_{K_\infty}$, and $\varepsilon(L/K) = \dim_{\mathbf{F}_p} \mathcal{G}$. Then the structure of the module $(X_L)_G$ of Galois coinvariants as a $\mathbf{Z}_p$-module is as follows*:

$$(X_L)_G \simeq (\mathbf{Z}/p\mathbf{Z})^{\oplus t} \oplus \mathbf{Z}_p^{\oplus \lambda_K},$$

where

$$t = \frac{s(s-3)}{2} + n(L/K) + \varepsilon(L/K)\,.$$

In particular, the $\mathbf{Z}_p$-torsion subgroup of $(X_L)_G$ is annihilated by p.

PROOF. Since we assumed the vanishing of the μ-invariant of X_K, it is a free $\mathbf{Z}_p$-module by Theorem 18 in [4], and $X_K \simeq \mathbf{Z}_p^{\oplus \lambda_K}$ as $\mathbf{Z}_p$-modules. By Proposition 2.3, $(X_L)_G$ is a finitely generated $\mathbf{Z}_p$-module with rank λ_K, and the $\mathbf{Z}_p$-torsion part of $(X_L)_G$ is $\hat{H}^{-1}(G, X_L)$. Thus our aim is to determine $\hat{H}^{-1}(G, X_L)$. By the fundamental exact sequence (Proposition 2.1) and the isomorphism (2), we know that the order of $\hat{H}^{-1}(G, X_L)$ is p^t where

$$t = \frac{s(s-1)}{2} + n(L/K) + \varepsilon(L/K) - s = \frac{s(s-3)}{2} + n(L/K) + \varepsilon(L/K)\,.$$

Therefore, it suffices to prove that $\hat{H}^{-1}(G, X_L)$ is killed by p, or that it needs t elements as its minimal generators as a $\mathbf{Z}_p$-module.

Step 1 (the case $s = 1$). Suppose that $G = \mathbf{Z}/p\mathbf{Z}$. In this case, since the order of G is p, we have $p\hat{H}^{-1}(G, X_L) = 0$, which implies the conclusion of Theorem 3.1.

Step 2 (the case $s = 2$). Suppose that $G = \mathbf{Z}/p\mathbf{Z} \oplus \mathbf{Z}/p\mathbf{Z}$. At first, we assume that L_∞/K_∞ is unramified outside p, namely $n(L/K) = 0$. Then the fundamental exact sequence implies $\hat{H}^{-1}(G, X_L) = \mathbf{Z}/p\mathbf{Z}$. Therefore, we get the theorem in this case. So we may assume $n(L/K) > 0$. This implies $\varepsilon(L/K) = 0$, or 1.
(i) We first assume that $\varepsilon(L/K) = 1$. We take an intermediate field M with $[L : M] = p$ and L_∞/M_∞ is unramified outside p. Put $G_1 = \mathrm{Gal}(L/M)$ and write $G = G_1 \oplus G_2$. We identify $\mathrm{Gal}(M/K)$ with G_2.

By the fundamental exact sequence, we have $\hat{H}^{-1}(G_1, X_L) = 0$. This shows that $(X_L)_{G_1}$ is a submodule of X_M with index p by Proposition 2.3. In particular, $(X_L)_{G_1}$ is a free $\mathbf{Z}_p$-module, so we can write

$$(X_L)_{G_1} \simeq \mathbf{Z}_p[G_2]^{\oplus a} \oplus \mathbf{Z}_p^{\oplus b} \oplus (\mathbf{Z}_p[G_2]/(N_{G_2}))^{\oplus c}$$

as $\mathbf{Z}_p[G_2]$-modules for some integers a, b, c where $N_{G_2} = \Sigma_{\sigma \in G_2} \sigma$. Taking the G_2-coinvariant, we have

$$(X_L)_G = ((X_L)_{G_1})_{G_2} \simeq \mathbf{Z}_p^{\oplus(a+b)} \oplus (\mathbf{Z}/p\mathbf{Z})^{\oplus c}\,.$$

Therefore, $p\hat{H}^{-1}(G, X_L) = 0$. This implies the conclusion as we explained.

By the way, we can determine a, b, c. We have proved that $\hat{H}^{-1}(G, X_L) = (\mathbf{Z}/p\mathbf{Z})^{\oplus n(L/K)}$, which implies $c = n(L/K)$. By the fundamental exact sequence for M/K, we get $\hat{H}^{-1}(G_2, X_M) = (\mathbf{Z}/p\mathbf{Z})^{\oplus n(M/K)-1} = (\mathbf{Z}/p\mathbf{Z})^{\oplus n(L/K)-1}$ and $\hat{H}^0(G_2, X_M) = 0$,

which imply

$$X_M = \mathbf{Z}_p[G_2]^{\oplus\lambda_K} \oplus (\mathbf{Z}_p[G_2]/(N_{G_2}))^{\oplus(n(L/K)-1)}.$$

(This procedure is the same as the proof of Kida's formula in Iwasawa [5].) Comparing the $\mathbf{Z}_p$-ranks of X_M and $(X_L)_{G_1}$ together with $a+b=\lambda_K$, we get $b=1$ and $a=\lambda_K-1$.

(ii) We next assume that $\varepsilon(L/K)=0$. We take an intermediate field M such that $[M:K]=p$, $S'(M_\infty/K_\infty)\neq\emptyset$, and $S'(L_\infty/M_\infty)\neq\emptyset$ where $S'(M_\infty/K_\infty)$ is the set of non p-adic ramifying primes of K_∞ in M_∞, and $S'(L_\infty/M_\infty)$ is the set of non p-adic ramifying primes of M_∞ in L_∞. Put $n(M/K)=\#S'(M_\infty/K_\infty)$ and $n(L/M)=\#S'(L_\infty/M_\infty)$. If v is in $S'(M_\infty/K_\infty)$, v is not a p-adic prime and the inertia group in G is cyclic. So the prime of M_∞ above v is not in $S'(L_\infty/M_\infty)$. If w is in $S'(L_\infty/M_\infty)$ and v is the prime of K_∞ below w, then v is not in $S'(M_\infty/K_\infty)$ and it splits completely in M_∞. Thus we have

$$n(L/K)=n(M/K)+\frac{1}{p}n(L/M)\,.$$

We again write $G=G_1\oplus G_2$ with $G_1=\mathrm{Gal}(L/M)$. By the fundamental exact sequence for L/M, we have an exact sequence

$$0\longrightarrow \hat{H}^{-1}(G_1,X_L)\longrightarrow \mathbf{F}_p[G_2]^{\oplus n(L/M)/p}\longrightarrow G_1\longrightarrow 0\,.$$

Therefore, we have an isomorphism

$$\hat{H}^{-1}(G_1,X_L)\simeq \mathbf{F}_p[G_2]^{\oplus(n(L/M)/p)-1}\oplus \mathbf{F}_p[G_2]/(N_{G_2})$$

as G_2-modules. As we saw in the case (i), we have an isomorphism

$$X_M=\mathbf{Z}_p[G_2]^{\oplus\lambda_K}\oplus(\mathbf{Z}_p[G_2]/(N_{G_2}))^{\oplus(n(M/K)-1)}$$

as G_2-modules by the fundamental exact sequence for M/K. From the exact sequence

$$0\longrightarrow \hat{H}^{-1}(G_1,X_L)\longrightarrow (X_L)_{G_1}\longrightarrow X_M\longrightarrow 0\,,$$

we have an exact sequence

$$\begin{aligned}0\longrightarrow \mathbf{F}_p[G_2]^{\oplus(n(L/M)/p)-1}\oplus \mathbf{F}_p[G_2]/(N_{G_2})\longrightarrow ((X_L)_{G_1})\otimes\mathbf{F}_p\\ \longrightarrow \mathbf{F}_p[G_2]^{\oplus\lambda_K}\oplus(\mathbf{F}_p[G_2]/(N_{G_2}))^{\oplus(n(M/K)-1)}\longrightarrow 0\,.\end{aligned}$$

We take a generator σ of G_2 and put $S=\sigma-1$. We identify $\mathbf{F}_p[G_2]$ with $\mathbf{F}_p[[S]]/(S^p)$. The above exact sequence is a sequence of $\mathbf{F}_p[[S]]/(S^p)$-modules. We put $R=\mathbf{F}_p[[\pi]]$ in the following Lemma 3.2, where π is an indeterminate. Then $\mathbf{F}_p[G_2]\cong R/(\pi^p)$ and $\mathbf{F}_p[G_2]/(N_{G_2})\cong R/(\pi^{p-1})$. From the lemma we obtain that the minimal number of generators of the $\mathbf{F}_p[G_2]$-module $((X_L)_{G_1})\otimes\mathbf{F}_p$ is exactly

$$n(M/K)+(n(L/M)/p)+\lambda_K-1=n(L/K)+\lambda_K-1\,.$$

Now we take G_2-coinvariants of $((X_L)_{G_1}) \otimes \mathbf{F}_p$, which of course gives $((X_L)_G) \otimes \mathbf{F}_p$. On the other hand, taking G_2-coinvariants simply means factoring out by π. Therefore, we obtain

$$\begin{aligned}((X_L)_G) \otimes \mathbf{F}_p &= ((X_L)_{G_1} \otimes \mathbf{F}_p)_{G_2} \\ &\simeq (\mathbf{Z}/p\mathbf{Z})^{\oplus n(L/K)+\lambda_K-1}.\end{aligned}$$

This shows that the minimal number of generators of the torsion part of $(X_L)_G$ (which is $\hat{H}^{-1}(G, X_L)$) as a $\mathbf{Z}_p$-module is exactly $n(L/K) - 1$ by Nakayama's lemma. This completes the proof in this case.

LEMMA 3.2. *Let R be a discrete valuation ring and π a uniformizing element. Suppose that M is an $R/(\pi^n)$-module with $n \geq 3$, and that there is an exact sequence*

$$0 \longrightarrow (R/(\pi^n))^{\oplus a} \oplus R/(\pi^{n-1}) \longrightarrow M \longrightarrow (R/(\pi^n))^{\oplus b} \oplus (R/(\pi^{n-1}))^{\oplus c} \longrightarrow 0$$

for some nonnegative integers a, b, c. Then the minimal number of generators of M over R is $a + b + c + 1$. In more detail, we have

$$M \simeq (R/(\pi^n))^{\oplus(a+b+\delta)} \oplus (R/(\pi^{n-1}))^{\oplus(c+1-2\delta)} \oplus (R/(\pi^{n-2}))^{\oplus\delta}$$

with $\delta = 0$ or 1.

We only sketch the idea of the *proof* of this lemma. First one uses that $R/(\pi^n)$ is projective and injective as a module over itself. This allows to reduce the situation to $a = b = 0$. The essential case is $c = 1$. One shows that an extension of $R/(\pi^{n-1})$ by itself which is annihilated by π^n is either split or isomorphic to $R/(\pi^n) \oplus R/(\pi^{n-2})$. Since $n - 2$ is still positive, the claim follows. Let us remark that (as the reader may have noticed) this lemma can be stated and proved more generally, but we will not go into it since it is not needed here.

Step 3 (general case). Now we assume $G = (\mathbf{Z}/p\mathbf{Z})^{\oplus s}$ with $s > 2$. Let H be a subgroup of G, and $M(H)$ the intermediate field of L/K corresponding to H. The restriction map $X_L \longrightarrow X_{M(H)}$ on the Galois groups induces the canonical homomorphism $\hat{H}^{-1}(G, X_L) \longrightarrow \hat{H}^{-1}(G/H, X_{M(H)})$ on the cohomology groups by the commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \hat{H}^{-1}(G, X_L) & \longrightarrow & (X_L)_G & \longrightarrow & X_K \\ & & \downarrow{\scriptstyle can} & & \downarrow{\scriptstyle Res} & & \downarrow{\scriptstyle id} \\ 0 & \longrightarrow & \hat{H}^{-1}(G/H, X_{M(H)}) & \longrightarrow & (X_{M(H)})_{G/H} & \longrightarrow & X_K \end{array}$$

where the horizontal exact sequences are the sequences obtained from Proposition 2.3, the right vertical arrow is the identity map, the middle vertical arrow is the restriction map, and the left vertical arrow is induced by the middle vertical arrow. We call the left vertical arrow

can. The fundamental exact sequences for L/K and $M(H)/K$ give a commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \bigwedge^2 G & \longrightarrow & \hat{H}^{-1}(G, X_L) & \longrightarrow & \bigoplus_v I_v(L/K) \\ & & \downarrow & & \downarrow \, can & & \downarrow \, Res \\ 0 & \longrightarrow & \bigwedge^2 G/H & \longrightarrow & \hat{H}^{-1}(G/H, X_{M(H)}) & \longrightarrow & \bigoplus_v I_v(M(H)/K) \end{array}$$

where $I_v(L/K)$, $I_v(M(H)/K)$ are the inertia subgroups of v in G, G/H, respectively, the left vertical arrow is induced by the natural map $G \longrightarrow G/H$, and the right vertical is defined by the restriction maps.

Let $\mathcal{H}$ be the set of subgroups of G with index p^2. Considering all $H \in \mathcal{H}$, we get a commutative diagram of exact sequences:

$$\begin{array}{ccccccc} 0 & \to & \bigwedge^2 G & \longrightarrow & \hat{H}^{-1}(G, X_L) & \longrightarrow & \bigoplus_v I_v(L/K) \\ & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma \\ 0 & \to & \bigoplus_{H\in\mathcal{H}} \bigwedge^2 G/H & \longrightarrow & \bigoplus_{H\in\mathcal{H}} \hat{H}^{-1}(G/H, X_{M(H)}) & \longrightarrow & \bigoplus_{H\in\mathcal{H}} \bigoplus_v I_v(M(H)/K). \end{array}$$

Since G is elementary abelian, α is injective. It is also easy to see that γ is injective. Therefore, β is also injective. Since $G/H \simeq (\mathbf{Z}/p\mathbf{Z})^{\oplus 2}$, we have shown in Step 2 that the range of β is annihilated by p. This shows that $\hat{H}^{-1}(G, X_L)$ is annihilated by p. Therefore, by the fundamental exact sequence and the isomorphism (2), we have $\hat{H}^{-1}(G, X_L) \simeq (\mathbf{Z}/p\mathbf{Z})^{\oplus t}$ with t as in Theorem 3.1. This completes the proof of Theorem 3.1. □

4. *S*-ramified Iwasawa modules and the main conjecture

In this section, we assume that L/k is a finite abelian extension of totally real number fields such that $L \cap k_\infty = k$.

We first introduce the p-adic L-function of Deligne-Ribet. We put $\Lambda_L = \mathbf{Z}_p[[\mathrm{Gal}(L_\infty/k)]]$. We fix a generator γ of $\mathrm{Gal}(L_\infty/L) \simeq \mathbf{Z}_p$ and put $T = \gamma - 1$. Then we have $\Lambda_L = \mathbf{Z}_p[\mathrm{Gal}(L/k)][[T]]$.

Suppose that S is a finite set of primes of k which contains all ramifying primes in L_∞. For simplicity, we assume that $L(\mu_p)^+ = L$. We denote the cyclotomic character by $\kappa : \mathrm{Gal}(L(\mu_p)_\infty/k) \longrightarrow \mathbf{Z}_p^\times$. For a character χ of $\mathrm{Gal}(L/k)$ and $n \in \mathbf{Z}_{>0}$ we regard $\chi\kappa^n$ as a p-adic character of $\mathrm{Gal}(L(\mu_p)_\infty/k)$. The group homomorphism $\chi\kappa^n$ extends to a ring homomorphism $\Lambda_{L(\mu_p)} \longrightarrow \overline{\mathbf{Q}}_p$. Furthermore, we can extend it to the total quotient ring of $\Lambda_{L(\mu_p)}$ and denote it also by $\chi\kappa^n$. Then the p-adic L-function of Deligne-Ribet is the unique element

$$\Theta_{L_\infty/k,S} \in \frac{1}{T}\Lambda_{L(\mu_p)}$$

satisfying

$$\chi\kappa^n(\Theta_{L_\infty/k,S}) = L_S(1-n,\chi)$$

for all positive integers $n \in \mathbf{Z}_{>0}$ and all characters χ of $\mathrm{Gal}(L/k)$ where $L_S(s,\chi)$ is defined by $L_S(s,\chi) = \prod_{v\in S}(1-\chi(v)N(v)^{-s})L(s,\chi)$. Since χ is even, $L_S(1-n,\chi) = 0$ for odd positive n, so the complex conjugation acts on $\Theta_{L_\infty/k,S}$ trivially. Thus we know

$$\Theta_{L_\infty/k,S} \in \frac{1}{T}\Lambda_L\,.$$

Next we study the algebraic object. Let $\mathcal{X}_{L,S}$ be the Galois group of $\mathcal{L}_{L_\infty,S}/L_\infty$, the maximal abelian pro-p extension which are unramified outside S. Therefore, $\mathcal{X}_{L,S}$ is the Pontrjagin dual of the étale cohomology $H^1(\mathcal{O}_{L_\infty,S}, \mathbf{Q}_p/\mathbf{Z}_p)$ (see the proof of Proposition 2.1). Let χ be a character of $\mathrm{Gal}(L/k)$, and $\mathcal{O}_\chi = \mathbf{Z}_p[\mathrm{Image}(\chi)]$ on which $\mathrm{Gal}(L/k)$ acts via χ. For a $\mathbf{Z}_p[\mathrm{Gal}(L/k)]$-module M, we define the χ-quotient by $M_\chi = M \otimes_{\mathbf{Z}_p[\mathrm{Gal}(L/k)]} \mathcal{O}_\chi$. Then $(\mathcal{X}_{L,S})_\chi$ is a finitely generated torsion $(\Lambda_L)_\chi = \mathcal{O}_\chi[[T]]$-module. Let $\tilde{\chi} : \Lambda_L \longrightarrow (\Lambda_L)_\chi$ be the ring homomorphism induced by χ. The main conjecture which was proved by Wiles in [14] Theorem 1.3 (at least assuming the vanishing of the μ-invariant) is

$$\mathrm{char}_{(\Lambda_L)_\chi}((\mathcal{X}_{L,S})_\chi) = \begin{cases} (\tilde{\chi}(\Theta_{L_\infty/k,S})) & \text{if } \chi \neq 1 \\ (T\tilde{\chi}(\Theta_{L_\infty/k,S})) & \text{if } \chi = 1 \end{cases}$$

as ideals of $(\Lambda_L)_\chi$ where the left hand side is the characteristic ideal. If M is a finitely generated torsion $(\Lambda_L)_\chi$-module with no nontrivial finite submodule, we know $\mathrm{char}_{(\Lambda_L)_\chi}(M) = \mathrm{Fitt}_{(\Lambda_L)_\chi}(M)$ where the latter is the (initial) Fitting ideal of M (cf. [10]). Thus the question arises naturally whether $T\Theta_{L_\infty/k,S}$ is in $\mathrm{Fitt}_{\Lambda_L}(\mathcal{X}_{L,S})$ or not. The answer is No if $\mathrm{Gal}(L/k) \otimes \mathbf{Z}_p$ is not cyclic. But using $\Theta_{L_\infty/k,S}$, we can describe the Fitting ideal in the following theorem.

THEOREM 4.1. *We assume the vanishing of the μ-invariant of X_L. Suppose that the p-Sylow subgroup of* $\mathrm{Gal}(L/k)$ *is generated by exactly s elements. Then we have*

$$\mathrm{Fitt}_{\Lambda_L}(\mathcal{X}_{L,S}) = T^{1-s}\mathfrak{A}_{\mathrm{Gal}(L/k)}\Theta_{L_\infty/k,S}$$

where $\mathfrak{A}_{\mathrm{Gal}(L/k)}$ is the ideal of Λ_L defined in our previous paper [3] *as the Fitting ideal of a certain second syzygy module, which is determined only by the p-Sylow subgroup of* $\mathrm{Gal}(L/k)$.

PROOF. This can be proved by the same method as Theorem 3.3 in [3]. In that paper we assumed that $S = S_p$, so that $\mathcal{X}_{L,S}$ agrees with X_L. But this is the only difference; all the arguments carry over unchanged to general $S \supset S_p$.

We cannot reproduce the proof of the quoted theorem here, but let us at least say something on the ideal $T^{1-s}\mathfrak{A}_{\mathrm{Gal}(L/k)}$. The precise definition is to be found in §1 of loc. cit. Let Δ be the non-p-part of $\mathrm{Gal}(L/k)$ and G be the p-part, in particular, $\mathrm{Gal}(L/k) \simeq \Delta \times G$. The ideal $\mathfrak{A}_{\mathrm{Gal}(L/k)}$ is a purely algebraic invariant that depends only on G. For every character

ξ of Δ except for the trivial character, the ξ-component of $T^{1-s}\mathfrak{A}_{\mathrm{Gal}(L/k)}$ is the unit ideal. We regard the trivial character component $(T^{1-s}\mathfrak{A}_{\mathrm{Gal}(L/k)})^1 = T^{1-s}(\mathfrak{A}_{\mathrm{Gal}(L/k)})^1$ as an ideal of $\Lambda[G]$. The ideal $(\mathfrak{A}_{\mathrm{Gal}(L/k)})^1$ is defined by $(\mathfrak{A}_{\mathrm{Gal}(L/k)})^1 = \mathrm{Fitt}_{\Lambda[G]}(\Omega^2)$ with a certain explicit second syzygy Ω^2 of the module $\mathbf{Z}$ over G with trivial $\mathrm{Gal}(k_\infty/k)$-action. □

We explain the ideal $(\mathfrak{A}_{\mathrm{Gal}(L/k)})^1$ a little more. Let $I_{\Lambda[G]} = \mathrm{Ker}(\Lambda[G] = \mathbf{Z}_p[[\mathrm{Gal}(k_\infty/k) \times G]] \longrightarrow \mathbf{Z}_p)$ be the augmentation ideal of $\mathrm{Gal}(k_\infty/k) \times G$. Write $G = \mathbf{Z}/p^{n_1} \times \ldots \times \mathbf{Z}/p^{n_s}$ with $n_1 \leq \ldots \leq n_s$. Define $J_{\Lambda[G]}$ to be the ideal generated by $I_{\Lambda[G]}$ and p^{n_1}. Then $(T^{1-s}\mathfrak{A}_{\mathrm{Gal}(L/k)})^1$ is contained, with finite index, in the ideal $I_{\Lambda[G]}$ of $\Lambda[G]$. We also have

$$(T^{1-s}\mathfrak{A}_{\mathrm{Gal}(L/k)})^1 \subset I_{\Lambda[G]} J_{\Lambda[G]}^{s(s-1)/2}$$

(see Propositions 1.6 and 1.5 in [3]); one can check this in the following way. Let I_G be the augmentation ideal of $\mathbf{Z}_p[G]$ and J_G the ideal of $\mathbf{Z}_p[G]$ generated by I_G and p^{n_1}. Then $\mathfrak{n}_d$ in [3] §1 satisfies $\mathfrak{n}_d \subset J_G^d$, which implies $\mathfrak{m}_d \subset J_G^d$ by Proposition 1.5 in [3] where $\mathfrak{m}_d$ is the ideal of $\mathbf{Z}_p[G]$ appearing in Proposition 1.6 in [3]. We also note $\mathfrak{m}_{t+1} \subset I_G J_G^t$ for $t = s(s-1)/2$, since any monomial appearing in a $(t+1)$-minor of $\tilde{M}_s$ can only have t factors of type ν and therefore must have at least one factor of type τ. Thus Proposition 1.6 in [3] implies the above inclusion.

5. The Fitting ideal of the p-ramified Iwasawa module over a totally real number field

In this section, L/k is as in the previous section, but we do not assume $L = L(\mu_p)^+$. We put $\Lambda_L = \mathbf{Z}_p[[\mathrm{Gal}(L_\infty/k)]]$. As in §2 let X_L be the Galois group of the maximal abelian pro-p extension $\mathcal{L}_{L_\infty, S_p}/L_\infty$, which is unramified outside p. We call X_L the p-ramified Iwasawa module of L_∞; it is a module over Λ_L.

For $L(\mu_p)^+$, consider $\Theta_{L(\mu_p)^+_\infty/k,S}$ defined in the previous section. When we take S to be minimal, namely the set of ramifying primes of k in $L(\mu_p)^+_\infty$, we simply write $\Theta_{L(\mu_p)^+_\infty/k}$ for $\Theta_{L(\mu_p)^+_\infty/k,S}$. We note that $[L(\mu_p)^+ : L]$ is prime to p, which implies that Λ_L can be regarded as a direct summand of $\Lambda_{L(\mu_p)^+}$. We denote by $\Theta_{L_\infty/k} \in \Lambda_L$ the Λ_L-component of $\Theta_{L(\mu_p)^+_\infty/k}$. We are interested in whether $T\Theta_{L_\infty/k}$ is in the Fitting ideal $\mathrm{Fitt}_{\Lambda_L}(X_L)$ or not.

THEOREM 5.1. *Suppose that L/k is a finite abelian extension of totally real number fields such that $L \cap k_\infty = k$. We assume that L/k contains an intermediate field K such that $K \subset k(\mu_p)^+$ and $\mathrm{Gal}(L/K)$ is elementary p-abelian. We write $\mathrm{Gal}(L/K) = (\mathbf{Z}/p\mathbf{Z})^{\oplus s}$ for some $s \geq 0$. We also assume the vanishing of the μ-invariant of X_L and one of the following conditions.*

(i) *$s = 2$ and L_∞/K_∞ is unramified outside p.*

(ii) $s = 3$ *and* L_∞/K_∞ *contains an intermediate field* L''_∞ *which is unramified outside* p *and* $[L''_\infty : K_\infty] = p$.

(iii) $s \geq 4$.

Then we have

$$T\Theta_{L_\infty/k} = (\gamma - 1)\Theta_{L_\infty/k} \notin \mathrm{Fitt}_{\Lambda_L}(X_L)\,.$$

REMARK 5.2. When $k = \mathbf{Q}$, then (i) and (ii) never occur. This is because if $L/\mathbf{Q}$ is a finite abelian p-extension which is unramified outside p, then L is contained in $\mathbf{Q}_\infty$. But, of course, (iii) does occur.

PROOF OF THEOREM 5.1. We may assume that $K = k$. In fact, put $\Delta = \mathrm{Gal}(K/k)$, and regard it as a subgroup of $\mathrm{Gal}(L/k)$. Let $L(\Delta)$ be the intermediate field of L/k such that $\mathrm{Gal}(L/L(\Delta)) = \Delta$, so $L(\Delta)/k$ is a p-extension. Then, since $\#\Delta$ is prime to p, $\Lambda_{L(\Delta)}$ is a direct summand of Λ_L. The $\Lambda_{L(\Delta)}$-component of $\Theta_{L_\infty/k}$ is $\Theta_{L(\Delta)_\infty/k}$ because the set of primes of k ramifying in L_∞ coincides with the set of primes of k ramifying in $L(\Delta)_\infty$. Since $H^1(\mathcal{O}_{L(\Delta)_\infty,S_p}, \mathbf{Q}_p/\mathbf{Z}_p) \longrightarrow H^1(\mathcal{O}_{L_\infty,S_p}, \mathbf{Q}_p/\mathbf{Z}_p)^\Delta$ is bijective, the $\Lambda_{L(\Delta)}$-component of X_L is $X_{L(\Delta)}$. Therefore the conclusion of Theorem 5.1 for the extension $L(\Delta)/k$ implies the conclusion of Theorem 5.1 for L/k.

We suppose $K = k$ from now on. We put $\Lambda = \Lambda_k = \mathbf{Z}_p[[\mathrm{Gal}(k_\infty/k)]] \simeq \mathbf{Z}_p[[T]]$. We first consider the restriction homomorphism $c_{L_\infty/k_\infty} : \Lambda_L \longrightarrow \Lambda$. Let S' be the set of non p-adic ramifying primes of k in L_∞. Since only p-adic primes are ramified in k_∞/k, we have

$$c_{L_\infty/k_\infty}(T\Theta_{L_\infty/k}) = \left(\prod_{v\in S'}(1 - N(v)^{-1}\varphi_v)\right) T\Theta_{k_\infty/k} \in \Lambda$$

where φ_v is the Frobenius of v in $\mathrm{Gal}(k_\infty/k)$. By the main conjecture proved by Wiles [14] (see §4), $T\Theta_{k_\infty/k}$ generates the characteristic ideal of X_k. Therefore, its image modulo p $\in \Lambda/p = \mathbf{F}_p[[T]]$ satisfies

$$\mathrm{ord}_T(T\Theta_{k_\infty/k} \bmod p) = \lambda_k\,,$$

where λ_k is the λ-invariant of X_k and ord_T is the normalized additive valuation of $\mathbf{F}_p[[T]]$, because we are assuming the vanishing of the μ-invariant.

Since v is ramified in L, we know $N(v) \equiv 1 \pmod p$. Therefore, we have

$$\begin{aligned}\mathrm{ord}_T\left(\prod_{v\in S'}(1 - N(v)^{-1}\varphi_v) \bmod p\right) &= \mathrm{ord}_T\left(\prod_{v\in S'}(1 - \varphi_v) \bmod p\right)\\ &= \sum_{v\in S'}\mathrm{ord}_T((1 - \varphi_v) \bmod p)\\ &= \#S'_{k_\infty}\end{aligned}$$

where S'_{k_∞} is the set of primes of k_∞ above S'. Thus the image of $T\Theta_{L_\infty/k}$ in $\Lambda_k \otimes \mathbf{F}_p$ satisfies

$$\mathrm{ord}_T(c_{L_\infty/k_\infty}(T\Theta_{L_\infty/k}) \bmod p) = \lambda_k + \#S'_{k_\infty}\,. \tag{3}$$

Next applying Theorem 3.1 to L/k, we have $((X_L)_{\mathrm{Gal}(L/k)}) \otimes \mathbf{F}_p \simeq (\mathbf{Z}/p\mathbf{Z})^{\oplus t}$ with

$$t = \frac{s(s-3)}{2} + \#S'_{k_\infty} + \varepsilon + \lambda_k\,, \tag{4}$$

where $\varepsilon = \dim_{\mathbf{F}_p} \mathrm{Gal}(L''_\infty/k_\infty)$ with L'' as in (ii). If (i) is satisfied, then $\varepsilon = 2$ and $s(s-3)/2 + \varepsilon = 1 > 0$. If (ii) is satisfied, then $\varepsilon \geq 1$, and $s(s-3)/2 + \varepsilon \geq 1 > 0$. If (iii) is satisfied, then $s(s-3)/2 + \varepsilon \geq s(s-3)/2 > 0$. In any case, by the equations (3), (4), we have

$$t > \mathrm{ord}_T(c_{L_\infty/k_\infty}(T\Theta_{L_\infty/k}) \bmod p)\,.$$

After these preparations, suppose now that $T\Theta_{L_\infty/k}$ is in $\mathrm{Fitt}_{\Lambda_L}(X_L)$. This would imply

$$c_{L_\infty/k_\infty}(T\Theta_{L_\infty/k}) \bmod p \in \mathrm{Fitt}_{\mathbf{F}_p[[T]]}((X_L)_{\mathrm{Gal}(L/k)} \otimes \mathbf{F}_p) = (T^t)\,.$$

This contradicts the above inequality. Therefore, we have $T\Theta_{L_\infty/k} \notin \mathrm{Fitt}_{\Lambda_L}(X_L)$. □

6. The Fitting ideal of the dualized Iwasawa module

By the duality we mentioned in Remark 2.2, Theorem 5.1 implies the result on the minus class group that we explained in the Introduction. We now give the details of this implication.

For the ideal class group of a number field F, the p-component of the class group is denoted by A_F, namely $A_F = \mathrm{Cl}_F \otimes \mathbf{Z}_p$. For a CM-field L and the cyclotomic $\mathbf{Z}_p$-extension L_∞/L and the n-th layer L_n, we define $A_{L_\infty} = \varinjlim A_{L_n}$, which is a discrete $\Lambda_L = \mathbf{Z}_p[[\mathrm{Gal}(L_\infty/k)]]$-module. We consider the Pontrjagin dual $(A_{L_\infty})^\vee$ with the cogredient action of $\mathrm{Gal}(L_\infty/k)$. So it is a compact Λ_L-module.

For a finite abelian extension L/k where k is totally real and L is a CM-field, the Stickelberger element $\theta_{L/k} \in \mathbf{Q}[\mathrm{Gal}(L/k)]$ is the unique element which satisfies

$$\chi(\theta_{L/k}) = L_{S_L}(0, \chi^{-1})$$

for all characters χ of $\mathrm{Gal}(L/k)$ where we extended χ to the ring homomorphism $\chi : \mathbf{Q}[\mathrm{Gal}(L/k)] \longrightarrow \mathbf{Q}(\mathrm{Image}(\chi))$ and S_L is the set of ramifying primes of k in L. Let L, L_n be as in the previous paragraph. Then $\theta_{L_n/k}$ becomes a projective system for $n \gg 0$. Let γ be the generator we fixed and κ the cyclotomic character. We know $(\gamma - \kappa(\gamma))\theta_{L_n/k} \in \mathbf{Z}_p[\mathrm{Gal}(L_n/k)]$ and denote the projective limit by $(\gamma - \kappa(\gamma))\theta_{L_\infty/k} \in \Lambda_L$.

THEOREM 6.1. *Assume exactly the same conditions as in Theorem* 5.1, *including the list of conditions* (i), (ii), (iii), *with the exception that now* $K = k(\mu_p)$ *instead of* $K \subset k(\mu_p)^+$,

and "L is CM" instead of "L is totally real". Then we have

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

REMARK 6.2. (1) When L/K is unramified outside p (and in particular when we assume (i)), the above result was already obtained in our previous papers [8], [3].

(2) It is somewhat surprising that this corollary also applies in the case $k = \mathbf{Q}$ and suitable abelian fields L. Indeed, the paper [7] determines the Fitting ideal of the non-dualised class group over L_∞, and it contains the left hand side of the non-inclusion displayed in the theorem. In particular, in many cases the Fitting ideals of the class group of an abelian number field and of its dual cannot be equal. We will see such cases in §§7,8.

PROOF OF THEOREM 6.1. Suppose that $\kappa : \mathrm{Gal}(L_\infty/k) \longrightarrow \mathbf{Z}_p^\times$ is the cyclotomic character. Let τ, ι be the automorphisms of the total quotient ring of Λ_L induced by $\sigma \mapsto \kappa(\sigma)\sigma$, $\sigma \mapsto \sigma^{-1}$, respectively, for any $\sigma \in \mathrm{Gal}(L_\infty/k)$. Then we know

$$\iota\tau(\Theta_{L_\infty/k}) = \theta_{L_\infty/k}$$

and $\iota\tau(T) = \kappa(\gamma)\gamma^{-1} - 1$. Let $A_{L_\infty}^-$ be the minus part of A_{L_∞} (the part on which the complex conjugation acts as -1). The Kummer pairing gives a natural isomorphism

$$(A_{L_\infty}^-)^\vee(1) \simeq X_{L^+}$$

(see [13] Proposition 13.32). Therefore, Theorem 5.1 implies

$$(\kappa(\gamma)\gamma^{-1} - 1)\theta_{L_\infty/k} \notin \mathrm{Fitt}_{\Lambda_L}((A_{L_\infty}^-)^\vee)\,,$$

which completes the proof. □

REMARK 6.3. Put $\Delta = \mathrm{Gal}(K/k)$ and let $\omega : \Delta \longrightarrow \mathbf{Z}_p^\times$ be the Teichmüller character. Since the order of Δ is prime to p, $\mathbf{Z}_p[\Delta]$ is decomposed into character components, so any $\mathbf{Z}_p[\Delta]$-module M is decomposed into character components, $M = \bigoplus_\xi M^\xi$ where ξ runs over $\mathbf{Q}_p$-conjugacy classes of characters of Δ. By the same method as the proof of Theorem 6.1, we see that

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

where the left hand side is the ω-component of the element $(\gamma - \kappa(\gamma))\theta_{L_\infty/k}$. In fact, taking the ω-component of the isomorphism of the Kummer pairing in the proof of Theorem 6.1, we have

$$(A_{L_\infty}^\omega)^\vee(1) \simeq X_{L(\Delta)}$$

where $L(\Delta)$ is the intermediate field of L/k such that $\mathrm{Gal}(L/L(\Delta)) = \Delta$. Since $T\Theta_{L(\Delta)_\infty/k} \notin \mathrm{Fitt}_{\Lambda_{L(\Delta)}}(X_{L(\Delta)})$ by Theorem 5.1, we get the above statement on the ω-component.

7. Results at number field level

In this section, we study some consequences of Theorem 6.1 over number fields of finite degree. For simplicity, we assume $k = \mathbf{Q}$. We note that the vanishing of the μ-invariant is proved by Ferrero and Washington. We repeat that the cases (i) and (ii) in Theorem 6.1 never happen over $k = \mathbf{Q}$, and so we may concentrate on the case (iii).

COROLLARY 7.1. *Suppose that $L/\mathbf{Q}$ is a finite abelian extension such that $\mu_p \subset L$, $\mu_{p^2} \not\subset L$, and $\mathrm{Gal}(L/\mathbf{Q}(\mu_p)) \simeq (\mathbf{Z}/p\mathbf{Z})^{\oplus s}$ for some $s \geq 4$. Let S be the set of prime numbers ramifying in L, and $S' = S \setminus \{p\}$. We take $n \in \mathbf{Z}_{>0}$ such that*

$$p^n > \sum_{\ell \in S'} p^{\mathrm{ord}_p(\ell-1)-1}.$$

Let L_n be the n-th layer of L_∞/L (so $L_n = L(\mu_{p^{n+1}})$), and $R_n = \mathbf{Z}_p[\mathrm{Gal}(L_n/\mathbf{Q})]$. Then we have

$$\mathrm{Ann}_{R_n}(\mu_{p^{n+1}})\theta_{L_n/\mathbf{Q}} \not\subset \mathrm{Fitt}_{R_n}((A_{L_n})^\vee),$$

where $\mathrm{Ann}_{R_n}(\mu_{p^{n+1}})$ is the annihilator ideal of $\mu_{p^{n+1}}$ in R_n. More precisely,

$$(\mathrm{Ann}_{R_n}(\mu_{p^{n+1}})\theta_{L_n/\mathbf{Q}})^\omega \not\subset \mathrm{Fitt}_{R_n^\omega}((A_{L_n}^\omega)^\vee)$$

holds.

PROOF. As in the previous sections, suppose that γ is a generator of $\mathrm{Gal}(L_\infty/L)$. We regard γ as a generator of $\mathrm{Gal}(L_n/L)$. It is well-known that $(\gamma - \kappa(\gamma))\theta_{L_n/\mathbf{Q}} \in R_n$, and is, of course, in $\mathrm{Ann}_{R_n}(\mu_{p^{n+1}})\theta_{L_n/\mathbf{Q}}$. We will show that

$$((\gamma - \kappa(\gamma))\theta_{L_n/\mathbf{Q}})^\omega \notin \mathrm{Fitt}_{R_n^\omega}((A_{L_n}^\omega)^\vee).$$

Put $K = \mathbf{Q}(\mu_p)$, $\Delta = \mathrm{Gal}(K/\mathbf{Q})$, and $G = \mathrm{Gal}(L/K)$. As in Remark 6.3, we denote by $L(\Delta)$ the intermediate field of $L/\mathbf{Q}$ such that $\mathrm{Gal}(L/L(\Delta)) = \Delta$. Put $G = \mathrm{Gal}(L(\Delta)/\mathbf{Q}) = \mathrm{Gal}(L/\mathbf{Q}(\mu_p)) \simeq (\mathbf{Z}/p\mathbf{Z})^{\oplus s}$. It is well-known that $X_{\mathbf{Q}} = 0$. Therefore, applying Theorem 3.1 for $L(\Delta)/\mathbf{Q}$, we have

$$(X_{L(\Delta)})_G = \hat{H}^{-1}(G, X_{L(\Delta)}) \simeq (\mathbf{Z}/p\mathbf{Z})^{\oplus t}$$

where

$$t = \frac{s(s-3)}{2} + \#S'_{\mathbf{Q}_\infty}.$$

In particular, $(X_{L(\Delta)})_G$ is an $\mathbf{F}_p$-vector space. More precisely, consider the fundamental exact sequence

$$0 \longrightarrow \bigwedge^2 G \longrightarrow \hat{H}^{-1}(G, X_{L(\Delta)}) \longrightarrow \bigoplus_{v \in S'_{\mathbf{Q}_\infty}} \mathbf{F}_p \longrightarrow G \longrightarrow 0.$$

We regard γ as a generator of $\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})$, and put $T = \gamma - 1$ as before. Then γ acts on G trivially, and $\bigoplus_{v\in S'_{\mathbf{Q}_\infty}, v|\ell}\mathbf{F}_p \simeq \mathbf{F}_p[[T]]/(T^{p^r})$ where $r = \mathrm{ord}_p(\ell-1)-1$ (note that $\mathrm{ord}_p(\ell-1)\geq 1$). By our assumption, $n > r$ holds. Therefore, $T^{p^{n-1}}$ annihilates $\bigoplus_{v\in S'_{\mathbf{Q}_\infty}}\mathbf{F}_p$. Since T annihilates $\bigwedge^2 G$, we know that (p, T^{p^n}) annihilates $\hat{H}^{-1}(G, X_{L(\Delta)})$.

By the isomorphism $(A^\omega_{L_\infty})^\vee \simeq X_{L(\Delta)}(-1)$, we have isomorphisms of $\Lambda = \Lambda_{\mathbf{Q}_\infty}$-modules

$$\begin{aligned}((A^\omega_{L_\infty})^G)^\vee &\simeq (X_{L(\Delta)})_G(-1) = \hat{H}^{-1}(G, X_{L(\Delta)})(-1)\\ &\simeq \hat{H}^{-1}(G, X_{L(\Delta)})\,.\end{aligned}$$

Here, we used $p\hat{H}^{-1}(G, X_{L(\Delta)}) = 0$ to get the second isomorphism. Put $\Gamma_n = \mathrm{Gal}(L_\infty/L_n)$, which is generated by γ^{p^n}. Since (p, T^{p^n}) annihilates $\hat{H}^{-1}(G, X_{L(\Delta)})$, we have

$$((A^\omega_{L_\infty})^{G\times\Gamma_n})^\vee \simeq \hat{H}^{-1}(G, X_{L(\Delta)})_{\Gamma_n} = \hat{H}^{-1}(G, X_{L(\Delta)})\,.$$

Since the p-adic primes of L_n^+ are ramified in L_n, the natural map $A^-_{L_n} \longrightarrow (A^-_{L_\infty})^{\Gamma_n}$ is bijective. Therefore, we get

$$((A^\omega_{L_n})^\vee)_G \simeq \hat{H}^{-1}(G, X_{L(\Delta)})\,.$$

Now we can proceed in the same way as in the proof of Theorem 5.1. Suppose that $((\gamma-\kappa(\gamma))\theta_{L_n/\mathbf{Q}})^\omega$ is in $\mathrm{Fitt}_{R_n^\omega}((A^\omega_{L_n})^\vee)$. This would imply

$$T^{\#S'_{\mathbf{Q}_\infty}+1}\theta^\omega_{K_n} \in \mathrm{Fitt}_{\mathbf{F}_p[[T]]/(T^{p^n})}(\hat{H}^{-1}(G, X_{L(\Delta)})) = (T^t)$$

where t is as above and satisfies $t > \#S'_{\mathbf{Q}_\infty}$ because of our assumption $s \geq 4$. This is a contradiction because $T\theta^\omega_{K_n}$ is a unit of $\mathbf{Z}_p[\mathrm{Gal}(K_n/\mathbf{Q})]^\omega$ and $p^n > \sum_{\ell\in S'} p^{\mathrm{ord}_p(\ell-1)-1} = \#S'_{\mathbf{Q}_\infty}$. □

COROLLARY 7.2. *Suppose that p is an odd prime and*

$$m = p^n\prod_{i=1}^{s}\ell_i$$

satisfying

(i) $s \geq 4$,
(ii) $\ell_i \equiv 1 \pmod p$ *for all* $i = 1, \ldots, s$,
(iii) $p^{n-1} > \sum_{i=1}^{s} p^{\mathrm{ord}_p(\ell_i-1)-1}$.

We put $L = \mathbf{Q}(\mu_m)$. Then we have

$$(\mathrm{Ann}_{\mathbf{Z}[\mathrm{Gal}(L/\mathbf{Q})]}(\mu_m)\theta_{L/\mathbf{Q}}) \otimes \mathbf{Z}_p \not\subset \mathrm{Fitt}_{\mathbf{Z}_p[\mathrm{Gal}(L/\mathbf{Q})]}(A_L^\vee)\,.$$

In particular, the classical Stickelberger ideal of L by Iwasawa and Sinnott which contains $\mathrm{Ann}_{\mathbf{Z}[\mathrm{Gal}(L/\mathbf{Q})]}(\mu_m)\theta_{L/\mathbf{Q}}$ *does not coincide with* $\mathrm{Fitt}_{\mathbf{Z}[\mathrm{Gal}(L/\mathbf{Q})]}(\mathrm{Cl}_L^\vee)$.

PROOF. Clearly, L has a unique subfield L' such that the conductor of L' is m/p^{n-1}, L' contains $\mathbf{Q}(\mu_p)$, and $\mathrm{Gal}(L'/\mathbf{Q}(\mu_p)) \simeq (\mathbf{Z}/p\mathbf{Z})^{\oplus s}$. Put $F = L'(\mu_{p^n})$. By Corollary 7.1, we have

$$(\mathrm{Ann}_{\mathbf{Z}_p[\mathrm{Gal}(F/\mathbf{Q})]}(\mu_{p^n})\theta_{F/\mathbf{Q}})^\omega \not\subset \mathrm{Fitt}_{\mathbf{Z}_p[\mathrm{Gal}(F/\mathbf{Q})]^\omega}((A_F^\omega)^\vee)\,.$$

Since the conductor of F is m, the image of $\theta_{L/\mathbf{Q}}$ in $\mathbf{Q}[\mathrm{Gal}(F/\mathbf{Q})]$ is $\theta_{F/\mathbf{Q}}$. Since $\mathrm{Gal}(L/F)$ is generated by the inertia subgroups of the ramified primes, the natural map $A_F^- \longrightarrow A_L^-$ is injective. Therefore,

$$c_{L/F}(\mathrm{Fitt}_{\mathbf{Z}_p[\mathrm{Gal}(L/\mathbf{Q})]^\omega}((A_L^\omega)^\vee)) \subset \mathrm{Fitt}_{\mathbf{Z}_p[\mathrm{Gal}(L/\mathbf{Q})]^\omega}((A_F^\omega)^\vee)\,,$$

where $c_{L/F} : \mathbf{Z}_p[\mathrm{Gal}(L/\mathbf{Q})]^\omega \longrightarrow \mathbf{Z}_p[\mathrm{Gal}(F/\mathbf{Q})]^\omega$ is the restriction map. This implies that

$$(\mathrm{Ann}_{\mathbf{Z}_p[\mathrm{Gal}(L/\mathbf{Q})]}(\mu_{p^n})\theta_{L/\mathbf{Q}})^\omega \not\subset \mathrm{Fitt}_{\mathbf{Z}_p[\mathrm{Gal}(L/\mathbf{Q})]^\omega}((A_L^\omega)^\vee)\,,$$

which implies the conclusion. □

REMARK 7.3. For example, $m = 27\cdot 7\cdot 13\cdot 19\cdot 31$ satisfies the conditions of Corollary 7.2 for $p = 3$.

8. The case $s = 2$

We have studied the Fitting ideal of the minus class group of an abelian field L whose Galois group over $\mathbf{Q}$ has p-rank ≥ 4 (namely, $s = \dim_{\mathbf{F}_p} \mathrm{Gal}(L/\mathbf{Q}) \otimes \mathbf{F}_p \geq 4$). In this section, let us examine several examples in the case $s = 2$ for $k = \mathbf{Q}$.

Consider the subset $P = \{\ell \mid \ell \equiv 1 (\mathrm{mod}\ p)\}$ of the set of prime numbers. For $\ell \in P$, we denote by $F(\ell)$ the subfield of $\mathbf{Q}(\mu_\ell)$ of degree p. For two primes ℓ_1,$\ell_2 \in P$, we define $F(\ell_1, \ell_2)$ to be the composite field of $F(\ell_1)$ and $F(\ell_2)$, $L(\ell_1) = F(\ell_1)(\mu_p)$ and $L(\ell_1, \ell_2) = F(\ell_1, \ell_2)(\mu_p)$.

PROPOSITION 8.1. *Let ℓ_1, ℓ_2 be two primes in P, and assume $\ell_1 \not\equiv 1 \pmod{p^2}$. Put $L = L(\ell_1, \ell_2)$, and $G = \mathrm{Gal}(L/\mathbf{Q}(\mu_p)) = \mathrm{Gal}(F(\ell_1, \ell_2)/\mathbf{Q})$.*

(1) *We have $A^\omega_{L(\ell_1)} = 0$.*
(2) *For any $\ell_2 \in P$, A_L^ω is generated by one element as a $\mathbf{Z}_p[G]$-module.*
(3) *Suppose that ℓ_2 satisfies at least one of the following conditions*:

(i) $\ell_2 \not\equiv 1 \pmod{p^2}$;

(ii) *ℓ_2 does not split completely in $F(\ell_1)$.*

Then we have

$$\mathrm{Fitt}_{\mathbf{Z}_p[G]}((A_L^\omega)^\vee) = \mathrm{Fitt}_{\mathbf{Z}_p[G]}(A_L^\omega).$$

(4) *Suppose that ℓ_2 satisfies neither* (i) *nor* (ii) *above. Then N_{G_2} is in* $\mathrm{Fitt}_{\mathbf{Z}_p[G]}(A_L^\omega)$, *but not in* $\mathrm{Fitt}_{\mathbf{Z}_p[G]}((A_L^\omega)^\vee)$ *where $G_2 = \mathrm{Gal}(L/L(\ell_1))$ and N_{G_2} is the norm element of G_2 in $\mathbf{Z}_p[G]$. In particular, we have*

$$\mathrm{Fitt}_{\mathbf{Z}_p[G]}((A_L^\omega)^\vee) \neq \mathrm{Fitt}_{\mathbf{Z}_p[G]}(A_L^\omega)\,.$$

PROOF. We first note that the natural maps $A^\omega_{L(\ell_i)} \longrightarrow A^\omega_L$, $A^\omega_{L(\ell_i)} \longrightarrow A^\omega_{L(\ell_i)_\infty}$, $A^\omega_L \longrightarrow A^\omega_{L_\infty}$ are all injective.

(1) Put $G_1 = \mathrm{Gal}(F(\ell_1)/\mathbf{Q})$. By our assumption $\ell_1 \not\equiv 1 \pmod{p^2}$, there is only one prime of $F(\ell_1)_\infty$ above ℓ_1. It follows from the fundamental exact sequence for $F(\ell_1)/\mathbf{Q}$ that $\hat{H}^{-1}(G_1, X_{F(\ell_1)}) = 0$. Since $X_{\mathbf{Q}} = 0$, this implies that $X_{F(\ell_1)} = 0$ by Proposition 2.3. Since $(A^\omega_{L(\ell_1)_\infty})^\vee(1) \simeq X_{F(\ell_1)}$, we also have $A^\omega_{L(\ell_1)} = 0$.

(2) Let w_i be a prime of $L(\ell_1, \ell_2)$ above ℓ_i. We denote by $\kappa(w_i)$ the residue field of w_i, and by D_{ℓ_i} the decomposition group of w_i in G. We need the following lemma.

LEMMA 8.2. *We have an exact sequence*

$$\hat{H}^0(G, \mu_p) \longrightarrow \hat{H}^0(D_{\ell_1}, \kappa(w_1)^\times) \oplus \hat{H}^0(D_{\ell_2}, \kappa(w_2)^\times) \longrightarrow \hat{H}^{-1}(G, A_L^\omega)$$

$$\longrightarrow H^1(G, \mu_p) \xrightarrow{f_1} H^1(D_{\ell_1}, \kappa(w_1)^\times) \oplus H^1(D_{\ell_2}, \kappa(w_2)^\times) \longrightarrow \hat{H}^0(G, A_L^\omega)$$

$$\longrightarrow H^2(G, \mu_p) \xrightarrow{f_2} H^2(D_{\ell_1}, \kappa(w_1)^\times) \oplus H^2(D_{\ell_2}, \kappa(w_2)^\times)\,.$$

where G acts on μ_p trivially. The map f_1 is bijective. The group $\hat{H}^j(D_{\ell_i}, \kappa(w_i)^\times)$ is of order p for any $i, j \in \{0, 1, 2\}$.

PROOF OF LEMMA 8.2. This exact sequence is obtained from the exact sequence in the last line on page 411 in [8]. We know $H^1(D_{\ell_i}, \kappa(w_i)^\times) = H^1(D_{\ell_i}, U_{L_{w_i}}) \simeq \mathbf{Z}/e_{w_i}\mathbf{Z} = \mathbf{Z}/p\mathbf{Z}$ where $U_{L_{w_i}}$ is the unit group of the integer ring of L_{w_i}, and e_{w_i} is the ramification index of w_i in $L/\mathbf{Q}(\mu_p)$. It is well-known that the kernel of f_1 is isomorphic to the kernel of $A^\omega_{\mathbf{Q}(\mu_p)} \longrightarrow A^\omega_{L(\ell_1,\ell_2)}$. But $A^\omega_{\mathbf{Q}(\mu_p)} = 0$, so the kernel of f_1 is zero. Since both the source and the range of f_1 have order p^2, the injectivity of f_1 implies the bijectivity of f_1. Finally, $\hat{H}^0(D_{\ell_i}, \kappa(w_i)^\times)$ is isomorphic to the inertia group of ℓ_i in G by local class field theory, so it has order p. This completes the proof of Lemma 8.2.

We go back to the proof of Proposition 8.1. In the exact sequence in Lemma 8.2, since $\ell_1 \not\equiv 1 \pmod{p^2}$, we have $\hat{H}^0(D_{\ell_1}, \kappa(w_1)^\times) = \mathbf{F}_{\ell_1}^\times \otimes \mathbf{Z}/p\mathbf{Z} \simeq \mu_p$, and the natural map $\hat{H}^0(G, \mu_p) = \mu_p \longrightarrow \hat{H}^0(D_{\ell_1}, \kappa(w_1)^\times) = \mu_p$ is bijective. Therefore, it follows from Lemma 8.2 that $\hat{H}^{-1}(G, A_L^\omega)$ is isomorphic to $\mathbf{Z}/p\mathbf{Z}$. Since $A^\omega_{\mathbf{Q}(\mu_p)} = 0$, we know that A_L^ω is generated by one element as a G-module.

(3) We prove that $(A_L^\omega)^\vee$ is generated by one element as a G-module under the assumption in (3). Let us first assume that the condition (i) holds. By the fundamental exact sequence for $F(\ell_1, \ell_2)/\mathbf{Q}$,

$$0 \longrightarrow \bigwedge^2 G \longrightarrow \hat{H}^{-1}(G, X_{F(\ell_1,\ell_2)}) \longrightarrow \bigoplus_{v|\ell_1\ell_2} \mathbf{Z}/p\mathbf{Z} \longrightarrow G \longrightarrow 0$$

is exact. Since neither ℓ_1 nor ℓ_2 splits in $\mathbf{Q}_\infty$ by our assumption (i), we know $\bigoplus_{v|\ell_1\ell_2} \mathbf{Z}/p\mathbf{Z} \simeq (\mathbf{Z}/p\mathbf{Z})^{\oplus 2}$, which implies $\hat{H}^{-1}(G, X_{F(\ell_1,\ell_2)}) \simeq \mathbf{Z}/p\mathbf{Z}$ by the above exact sequence. Since $X_{\mathbf{Q}} = 0$, $X_{F(\ell_1,\ell_2)}$ is generated by one element as a G-module by Nakayama's lemma. Therefore, using the duality isomorphism as in (1), we get the cyclicity of $(A_L^\omega)^\vee$.

Next, we assume the condition (ii). Put $G_2 = \mathrm{Gal}(F(\ell_1, \ell_2)/F(\ell_1))$. By the fundamental exact sequence for $F(\ell_1, \ell_2)/F(\ell_1)$,

$$0 \longrightarrow \hat{H}^{-1}(G_2, X_{F(\ell_1,\ell_2)}) \longrightarrow \bigoplus_{v|\ell_2} \mathbf{Z}/p\mathbf{Z} \longrightarrow G_2 \longrightarrow 0$$

is exact where v runs over primes of $F(\ell_1)_\infty$ above ℓ_2. By our assumption (ii), $\bigoplus_{v|\ell_2} \mathbf{Z}/p\mathbf{Z}$ is a quotient of $\mathbf{F}_p[[\mathrm{Gal}(F(\ell_1)_\infty/F(\ell_1))]] = \mathbf{F}_p[[\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})]]$ and the third map in the exact sequence is induced by the augmentation map $\mathbf{F}_p[[\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q})]] \longrightarrow \mathbf{F}_p$. It follows that $\hat{H}^{-1}(G_2, X_{F(\ell_1,\ell_2)})$ is cyclic as a $\Lambda_{\mathbf{Q}}$-module. Since $X_{F(\ell_1)} = 0$ by (1), we have $(X_{F(\ell_1,\ell_2)})_{G_2} = \hat{H}^{-1}(G_2, X_{F(\ell_1,\ell_2)})$ by Proposition 2.3. Therefore, by Nakayama's lemma, $X_{F(\ell_1,\ell_2)}$ is generated by one element as a $\Lambda_{F(\ell_1,\ell_2)}$-module. Thus, by the same method as above, we get the cyclicity of $(A_L^\omega)^\vee$.

By (2) and the above, both A_L^ω and $(A_L^\omega)^\vee$ are cyclic as $\mathbf{Z}_p[G]$-modules. Therefore, we obtain

$$\mathrm{Fitt}_{\mathbf{Z}_p[G]}(A_L^\omega) = \mathrm{Fitt}_{\mathbf{Z}_p[G]}((A_L^\omega)^\vee) = \mathrm{Ann}_{\mathbf{Z}_p[G]}(A_L^\omega)\,.$$

This completes the proof of (3).

(4) Since $A_{L(\ell_1)}^\omega = 0$ by (1), N_{G_2} is in $\mathrm{Ann}_{\mathbf{Z}_p[G]}(A_L^\omega)$. Therefore, it is also in $\mathrm{Fitt}_{\mathbf{Z}_p[G]}(A_L^\omega)$ because A_L^ω is cyclic by (2).

Consider the homomorphism $H^2(G, \mu_p) \longrightarrow H^2(D_{\ell_2}, \kappa(w_2)^\times)$, which is obtained by the composition of f_2 in Lemma 8.2 and the second projection. Since ℓ_2 splits completely in $L(\ell_1)$ and ramifies in $L/L(\ell_1)$, $\kappa(w_2) = \mathbf{F}_{\ell_2}$. Put $r_2 = \mathrm{ord}_p(\ell_2 - 1)$. By our assumption $\ell_2 \equiv 1 \pmod{p^2}$, we have $r_2 > 1$. Then $H^2(D_{\ell_2}, \kappa(w_2)^\times) = H^2(D_{\ell_2}, \mu_{p^{r_2}})$ and the above map

$$H^2(G, \mu_p) \longrightarrow H^2(D_{\ell_2}, \kappa(w_2)^\times) = H^2(D_{\ell_2}, \mu_{p^{r_2}})$$

is induced by the natural homomorphisms $D_{\ell_2} \longrightarrow G$, $\mu_p \longrightarrow \mu_{p^{r_2}}$. In particular, it factors through $H^2(D_{\ell_2}, \mu_p)$. Recall that D_{ℓ_2} is cyclic of order p. Therefore, $H^2(D_{\ell_2}, \mu_p) \longrightarrow$

$H^2(D_{\ell_2}, \mu_{p^{r_2}})$ is the zero map. It follows that the $\mathbf{F}_p$-dimension of the image of f_2 in Lemma 8.2 is equal to or smaller than 1. By Lemma 8.2, we have

$$\dim_{\mathbf{F}_p}((A_L^{\omega})^G) \geq \dim_{\mathbf{F}_p} H^2(G, \mu_p) - 1 = 3 - 1 = 2\,.$$

Suppose that $\alpha \in \mathbf{Z}_p[G]$ is in $\mathrm{Fitt}_{\mathbf{Z}_p[G]}((A_L^{\omega})^{\vee})$. Let $c : \mathbf{Z}_p[G] \longrightarrow \mathbf{Z}_p$ be the augmentation map. We have $c(\alpha) \in \mathrm{Fitt}_{\mathbf{Z}_p}(((A_L^{\omega})^G)^{\vee})$, so p^2 divides $c(\alpha)$ because $\dim_{\mathbf{F}_p}((A_L^{\omega})^G) \geq 2$. Namely, we get

$$\alpha \in \mathrm{Fitt}_{\mathbf{Z}_p[G]}((A_L^{\omega})^{\vee}) \Longrightarrow p^2 | c(\alpha)\,.$$

This shows that N_{G_2} is not in $\mathrm{Fitt}_{\mathbf{Z}_p[G]}((A_L^{\omega})^{\vee})$ because $c(N_{G_2}) = p$. This completes the proof of Proposition 8.1.

□

REMARK 8.3. Suppose that n is a product of primes in P. We define $\eta_{\mathbf{Q}(\mu_{np})}$ by

$$\eta_{\mathbf{Q}(\mu_{np})} = \theta_{\mathbf{Q}(\mu_{np})/\mathbf{Q}} - \nu\theta_{\mathbf{Q}(\mu_p)/\mathbf{Q}}\,,$$

where ν is the corestriction map. It is easy to see that $\eta_{\mathbf{Q}(\mu_{np})} \in \mathbf{Z}_p[\mathrm{Gal}(\mathbf{Q}(\mu_{np})/\mathbf{Q})]$. For any field F with conductor np, we define η_F by the image of $\eta_{\mathbf{Q}(\mu_{np})}$. Let $\Theta(L) \subset \mathbf{Z}_p[\mathrm{Gal}(L/\mathbf{Q})]$ be the Stickelberger ideal in the sense of Sinnott [12] (or in the sense of the second author [7]). We regard $\Theta(L)$ as an ideal of the minus part $\mathbf{Z}_p[\mathrm{Gal}(L/\mathbf{Q})]^-$. We can check that $\Theta(L)$ of $L = L(\ell_1, \ell_2)$ is generated by four elements, to wit, η_L, $\nu\eta_{L(\ell_i)}$ with $i = 1, 2$, and $p\nu\theta_{\mathbf{Q}(\mu_p)/\mathbf{Q}}$ with suitable corestriction maps ν. By the main theorem in [9] (or Theorem 0.6 in [7]) we have

$$\mathrm{Fitt}_{\mathbf{Z}_p[\mathrm{Gal}(L/\mathbf{Q})]^-}(A_L^-) = \Theta(L)\,.$$

We have seen in Proposition 8.1 that

$$\mathrm{Fitt}_{\mathbf{Z}_p[\mathrm{Gal}(L/\mathbf{Q})]^-}((A_L^{\vee})^-) \neq \Theta(L)$$

if L satisfies the condition of Proposition 8.1 (4).

REMARK 8.4. We give numerical examples. Take $p = 3$ and $\ell_1 = 7$. Then all $\ell_2 \in P$ with $\ell_2 < 127$ satisfy the condition of Proposition 8.1 (3) (more precisely, $\ell_2 = 13, 19, 31, 43, 61, 67, 73, 79, 97, 103, 109$ satisfy the condition).

The first prime which does not satisfy the condition is $\ell_2 = 127$. Let us examine this case in detail. For $L = L(7, 127)$, take a generator σ of $\mathrm{Gal}(F(7)/\mathbf{Q})$ and $\tau \in \mathrm{Gal}(F(127)/\mathbf{Q})$ such that $\sigma(\zeta_7) = \zeta_7^3$ and $\tau(\zeta_{127}) = \zeta_{127}^3$. We write $\sigma = 1 + S$ and $\tau = 1 + T$, and

$$\mathbf{Z}_p[G] = \mathbf{Z}_p[S, T]/((1+S)^3 - 1, (1+T)^3 - 1)$$

where G is as in Proposition 8.1. (Note: the above T has no relation with T in the previous sections.) Let η_L be as in Remark 8.3. We regard η_L as an element of $\mathbf{Z}_p[\mathrm{Gal}(L/\mathbf{Q})]^- =$

$\mathbf{Z}_p[G]$. One can compute

$$\eta_L = -2(126 + 126S + 42S^2 + 123T + 123ST + 44S^2T + 40T^2 + 39ST^2 + 15S^2T^2)\,.$$

Let us not write out the others, but note that $\nu\eta_{L(7)}$ is $1+\tau+\tau^2$ times a unit since $A_{\mathbf{Q}(\mu_7)} = 0$. Then we can compute numerically the Stickelberger ideal $\Theta(L)$ of L. The result is

$$\Theta(L) = (3, S^2T, T^2) \subset \mathbf{Z}_p[G]\,. \tag{5}$$

We know $A_{L^+} = 0$, so we have $A_L = A_L^- = A_L^\omega$. Since A_L is cyclic by Proposition 8.1 (2), we have

$$\begin{aligned} A_L \simeq \mathbf{Z}_p[G]/\Theta(L) &= \mathbf{Z}_p[G]/(3, S^2T, T^2) \\ &= \mathbf{F}_p[S,T]/(S^3, S^2T, T^2)\,. \end{aligned} \tag{6}$$

In particular, as an abelian group, we have $A_L \simeq (\mathbf{Z}/p\mathbf{Z})^{\oplus 5}$. The structure of A_L as an abelian group can be also checked by direct computation. We thank Jiro Nomura very much for his computing the structure as an abelian group of $A_{L(\ell_1,\ell_2)}$ for several ℓ_1, ℓ_2 by Pari-GP.

By the isomorphism (6), we can also compute generators and relations of $A_L^\vee$. We find that $A_L^\vee$ is generated by two elements and its Fitting ideal is

$$\mathrm{Fitt}_{\mathbf{Z}_p[G]}(A_L^\vee) = (9, 3T, 3S, S^2T, T^2)\,. \tag{7}$$

It follows from (6) and (7) that

$$\mathrm{Fitt}_{\mathbf{Z}_p[G]}(A_L^\vee) \subsetneq \mathrm{Fitt}_{\mathbf{Z}_p[G]}(A_L) = (3, S^2T, T^2)\,.$$

By (7) we also see

$$\eta_L \in \mathrm{Fitt}_{\mathbf{Z}_p[G]}(A_L^\vee)\,,$$

but

$$\nu\eta_{L(7)} \notin \mathrm{Fitt}_{\mathbf{Z}_p[G]}(A_L^\vee)$$

because $\nu\eta_{L(7)}$ is $1+\tau+\tau^2 = 3+3T+T^2$ up to a unit factor.

References

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

[2] C. GREITHER and R. KUČERA, Annihilators of minus class groups of imaginary abelian fields, Ann. Inst. Fourier **57** (2007), 1623–1653.

[3] C. GREITHER and M. KURIHARA, Tate sequences and Fitting ideals of Iwasawa modules, to appear in the "Vostokov volume," Algebra i Analiz (St. Petersburg Math. J.) (2016).

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

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

[6] T. KIMURA, Algebraic class number formulae for cyclotomic fields (in Japanese), Sophia Kôkyûroku in Math. **22**, Sophia University Tokyo, 1985.
[7] M. KURIHARA, Iwasawa theory and Fitting ideals, J. reine angew. Math. **561** (2003), 39–86.
[8] M. KURIHARA, On stronger versions of Brumer's conjecture, Tokyo J. Math. **34** (2011), 407–428.
[9] M. KURIHARA and T. MIURA, Stickelberger ideals and Fitting ideals of class groups for abelian number fields, Math. Annalen **350** (2011), 549–575.
[10] D. G. NORTHCOTT, *Finite free resolutions*, Cambridge Tracts in Math. **71**, Cambridge Univ. Press, Cambridge New York, 1976.
[11] W. SINNOTT, On the Stickelberger ideal and the circular units of a cyclotomic field, Ann. Math. **108** (1978), 107–134.
[12] W. SINNOTT, On the Stickelberger ideal and the circular units of an abelian field, Invent. Math. **62** (1980), 181–234.
[13] L. WASHINGTON, *Introduction to cyclotomic fields*, Graduate Texts in Math. **83**, Springer-Verlag, 1982.
[14] A. WILES, The Iwasawa conjecture for totally real fields, Ann. Math. **131** (1990), 493–540.

Present Addresses:
CORNELIUS GREITHER
INSTITUT FÜR THEORETISCHE INFORMATIK UND MATHEMATIK,
UNIVERSITÄT DER BUNDESWEHR, MÜNCHEN,
85577 NEUBIBERG, GERMANY.
e-mail: cornelius.greither@unibw.de

MASATO KURIHARA
DEPARTMENT OF MATHEMATICS, FACULTY OF SCIENCE AND TECHNOLOGY,
KEIO UNIVERSITY,
3–14–1 HIYOSHI, KOHOKU-KU, YOKOHAMA 223–8522, JAPAN.
e-mail: kurihara@math.keio.ac.jp