FITTING IDEALS OF IWASAWA MODULES AND
OF THE DUAL OF CLASS GROUPS

CORNELIUS GREITHER AND MASATO KURIHARA

Dedicated to Professor Ken-ichi Shinoda

Abstract. In this paper we study some problems related to a
refinement of Iwasawa theory, especially questions about the Fit-
tting 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 \( \mathbb{Z}_p(1) \) times the Stick-
elberger element is not in the Fitting ideal of the dualized Iwasawa
module if the \( p \)-component of the bottom Galois group is ele-
tmatory \( p \)-abelian with \( p \)-rank \( \geq 4 \). Our results can be applied to the
case that the base field is \( \mathbb{Q} \).

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 \( k_{\infty}/k, L_{\infty}/L \) the cyclotomic
\( \mathbb{Z}_p \)-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 \( L_{\infty} \). 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
\( L_{\infty}/S/L_{\infty} \) which is the maximal abelian pro-\( p \) extension unrami-
fied 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 \( \chi \) of \( \text{Gal}(L/k) \) the characteristic
ideal of the \( \chi \)-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 \( \mathbb{Z}_p \) times) the \( S \)-truncated \( p \)-adic \( L \)-function \( \Theta_{L_{\infty}/k,S} \) is in
the Fitting ideal of the \( \Lambda_L \)-module \( \mathcal{X}_{L,S} \) where \( \Lambda_L = \mathbb{Z}_p[[\text{Gal}(L_{\infty}/k)]] \)
(concerning general properties of Fitting ideals, see [10]). Using our
previous results, we can show that the answer is always No if the \( p \)-com-
ponent of \( \text{Gal}(L/k) \) 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.
When we take $S$ to be minimal, namely the set of the ramifying primes of $k$ in $L_\infty$, 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 $L_{L_\infty,S_p}/L_\infty$ which is the maximal abelian pro-$p$ extension unramified outside $p$. We write $X_L = \text{Gal}(L_{L_\infty,S_p}/L_\infty)$, and study the Fitting ideal of the $L$-module $X_L$, especially the problem whether $(\gamma - 1)\Theta_{L_\infty/k}$ is in the Fitting ideal of $X_L$ or not, where $\gamma$ is a generator of $\text{Gal}(L_\infty/L)$. 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 $\text{Cl}_F$ the class group and $A_F = \text{Cl}_F \otimes \mathbb{Z}_p$. Let $\mu_p$ 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 $\omega : \text{Gal}(L'/k) \to \mathbb{Z}_p^\times$ be the Teichmüller character, which gives the action on $\mu_p$. We denote by $L'_{\infty}/L'$ the cyclotomic $\mathbb{Z}_p$-extension, and define $A_{L'_{\infty}}$ to be the inductive limit of $A_{L_n}$ where $L_n$ is the $n$-th layer of $L'_{\infty}/L'$. Consider the $\omega$-component $A_{L'_{\infty}}^\omega$. Then the Kummer pairing gives a well-known isomorphism $(A_{L'_{\infty}}^\omega)^\vee(1) \simeq X_L$ of Galois modules (see [13] Proposition 13.32), where $(A_{L'_{\infty}}^\omega)^\vee$ is the Pontrjagin dual and $(1)$ is the Tate twist. Put $\Lambda_{L'} = \mathbb{Z}_p[[\text{Gal}(L'_{\infty}/k)]]$. We consider the cogredient action of the Galois group on the Pontrjagin dual $(A_{L'_{\infty}}^\omega)^\vee$, and regard it as a $\Lambda_{L'}$-module. Let $\gamma$ be a generator of $\text{Gal}(L'/L)$ and $\kappa$ 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 $\text{Gal}(L/k) \simeq (\mathbb{Z}/p\mathbb{Z})^\oplus s$ with $s \geq 4$. Then we always have

$$(\gamma - \kappa(\gamma))\theta_{L'_{\infty}} \not\in \text{Fitt}_{\Lambda_{L'}}((A_{L'_{\infty}}^\omega)^\vee).$$

In previous work, see [3], it was shown: If $L/k$ is unramified outside $p$ and $\text{Gal}(L/k)$ 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 $k = \mathbb{Q}$. In our previous work, if $L/k$ is unramified outside $p$ and $\text{Gal}(L/k)$ is not cyclic, then $k$ cannot be $\mathbb{Q}$. 
A key result in the proof of Theorems 6.1 and 5.1 is Theorem 3.1 which determines the structure of \((X_L)_{\text{Gal}(L/k)}\) for elementary \(p\)-abelian \(\text{Gal}(L/k)\). In particular, we prove that the \(\mathbb{Z}_p\)-torsion part of \((X_L)_{\text{Gal}(L/k)}\) is annihilated by \(p\) in this setting.

1-3. We study finite abelian extensions over \(\mathbb{Q}\) in \S\S 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 \(L = \mathbb{Q}(\mu_m)\) we can show that

\[
(\text{Ann}_{\mathbb{Z}[\text{Gal}(L/\mathbb{Q})]}(\mu_m) \otimes \mathbb{Z}_p) \not\subseteq \text{Fitt}_{\mathbb{Z}_p[\text{Gal}(L/\mathbb{Q})]}(A_L^\vee)
\]

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

\[
(\text{Ann}_{\mathbb{Z}[\text{Gal}(L/\mathbb{Q})]}(\mu_m) \otimes \mathbb{Z}_p) \subset \text{Fitt}_{\mathbb{Z}_p[\text{Gal}(L/\mathbb{Q})]}(A_L)
\]

for any \(m\) and \(p\). Such a negative result is surprising because people sometimes thought that the Pontryagin 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

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

for any finite abelian \(L/\mathbb{Q}\) such that \(\mu_p \not\subseteq L\). But the above negative result shows that this equality does not hold in general if \(\mu_p \subset L\). We discuss this problem in \S 8 in the case \(\mu_p \subset L\) and \(s = 2\) (the latter simply meaning that the \(p\)-component of \(\text{Gal}(L/\mathbb{Q})\) is \((\mathbb{Z}/p\mathbb{Z})^\oplus 2\)). 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

\[\text{Fitt}_{\mathbb{Z}_p[\text{Gal}(L/\mathbb{Q})]}((A_L^-)^\vee) \subset \text{Fitt}_{\mathbb{Z}_p[\text{Gal}(L/\mathbb{Q})]}(A_L^-)\]

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 \( F_\infty/F \) the cyclotomic \( \mathbb{Z}_p \)-extension.

Suppose that \( L/K \) is a finite abelian \( p \)-extension of totally real number fields such that \( L \cap K_\infty = K \) and \( G = \text{Gal}(L/K) \). Consider the maximal abelian pro-\( p \) extension \( L_{\infty,s_p}/L_\infty \) which is unramified outside \( p \), and put \( X_L = \text{Gal}(L_{\infty,s_p}/L_\infty) \). 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 \( G = \text{Gal}(L/K) \). Then we have an exact sequence

\[
0 \rightarrow \bigoplus_{v \in S'_{K_\infty}} I_v \rightarrow \hat{H}^{-1}(G, X_L) \rightarrow \bigoplus_{v \in S'_{K_\infty}} I_v \rightarrow G \rightarrow \hat{H}^0(G, X_L) \rightarrow 0,
\]

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

**Remark 2.2.** Put \( K' = K(\mu_p) \) and \( L' = L(\mu_p) \). We denote by \( L'_n \) the \( n \)-th layer of \( L' \), and by \( A^p_{L_n} \) 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 \( \lim_{\rightarrow} A^p_{L_n} \), which we write \( A^p_{L_\infty} \). Namely we have

\[
X_L \simeq (A^p_{L_\infty})^\vee(1)
\]

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

\[
0 \rightarrow \hat{H}^{-1}(G, X_L) \rightarrow (X_L)_G \rightarrow X_K \rightarrow \mathcal{G} \rightarrow 0
\]

where \( (X_L)_G \) is the module of \( G \)-coinvariants of \( X_L \), and \( (X_L)_G \rightarrow X_K \) 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 \( Cl_{L'_n} \rightarrow Cl_{K'_n} \) 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 \( A^i_{L'_\infty} \rightarrow A^i_{K'_\infty} \) is finite. Using the above duality, we know that the kernel of the canonical map \( X_K \rightarrow X_L \) is finite. On the other hand, by Theorem 18 in Iwasawa [4] we know that \( X_K \) has no nontrivial finite \( \mathbb{Z}/n \mathbb{Z} \). Therefore, the localization sequence of etale cohomology gives a short exact sequence \( \mathbb{Z}/n \mathbb{Z} \) subextension of \( G \), when \( n \) is sufficiently large. Therefore, the cokernel of this map is \( G \). \( \square \)

Now we prove the fundamental exact sequence (Proposition 2.1). Let \( S \) 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 \( S = S' \cup S \). Let \( \mathcal{O}_{K, S} \) be the ring of \( S \)-integers in \( K \). We denote by \( H^i(\mathcal{O}_{K, S}, \mathbb{Q}_p/\mathbb{Z}_p) \) the étale cohomology \( H^i_{et}(Spec \mathcal{O}_{K, S}, \mathbb{Q}_p/\mathbb{Z}_p) \), which is the same as the Galois cohomology \( H^i(M/K, \mathbb{Q}_p/\mathbb{Z}_p) \) where \( M/K \) is the maximal extension unramified outside \( S \). We define \( H^i(\mathcal{O}_{K, S}, \mathbb{Q}_p/\mathbb{Z}_p) \), \( H^i(\mathcal{O}_{L, S}, \mathbb{Q}_p/\mathbb{Z}_p) \), \( H^i(\mathcal{O}_{L, S}, \mathbb{Q}_p/\mathbb{Z}_p) \), 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 \( I_v(M/K) \) be the inertia group of \( v \) in \( Gal(M/K) \). Since \( v \) is prime to \( p \), \( I_v(M/K) \) is isomorphic to \( \mathbb{Z}/p \) where \( (1) \) means the Tate twist, and

\[
H^0(\kappa(v), H^1(I_v(M/K), \mathbb{Q}_p/\mathbb{Z}_p)) = H^0(\kappa(v), \mathbb{Q}_p/\mathbb{Z}_p(-1)) = \mathbb{Q}_p/\mathbb{Z}_p(-1).
\]

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

\[
(1) \quad 0 \rightarrow H^1(\mathcal{O}_{K, S}, \mathbb{Q}_p/\mathbb{Z}_p) \rightarrow H^1(\mathcal{O}_{K, S}, \mathbb{Q}_p/\mathbb{Z}_p) \rightarrow \bigoplus_{v \in S_{K, \infty}} \mathbb{Q}_p/\mathbb{Z}_p(-1) \rightarrow 0.
\]
Using the same exact sequence for $L$ and the spectral sequence, we have a commutative diagram of exact sequences

$$
0 \rightarrow H^1(G, \mathbb{Q}_p/\mathbb{Z}_p) \rightarrow \bigoplus_v \mathbb{Z}/e_v \mathbb{Z}(1) \rightarrow 0
$$

Here, $H^1(\mathcal{O}_{K_s, s_p}, \mathbb{Q}_p/\mathbb{Z}_p)$ and $H^1(\mathcal{O}_{L_s, s_p}, \mathbb{Q}_p/\mathbb{Z}_p)$ 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 $L_{s_p}/K_s$. We also note that $H^1(G, \mathbb{Q}_p/\mathbb{Z}_p)$, $H^2(G, \mathbb{Q}_p/\mathbb{Z}_p)$ are the Pontrjagin duals of $G$ and $\bigwedge^2 G$, respectively. In the third vertical sequence, $v$ runs over $S'_{K_s}$ and $w$ runs over $S'_{L_s}$ which is the set of primes of $L$ above $S'$. We have $(\bigoplus_w \mathbb{Q}_p/\mathbb{Z}_p(-1))^G \simeq \bigoplus_v \mathbb{Q}_p/\mathbb{Z}_p(-1)^G$ 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

$$
0 \rightarrow \bigwedge^2 G \rightarrow \hat{H}^{-1}(G, X_L) \rightarrow \bigoplus_{v \in S'_{K_s}} \mathbb{Z}/e_v \mathbb{Z}(1) \rightarrow G \rightarrow G \rightarrow 0.
$$

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

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

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 $G \simeq \mathbb{Z}/p\mathbb{Z}$. Let $X_{K, S}$ be the Galois group of $L_{K, s_p}/K_s$ which is the maximal abelian pro-$p$ extension unramified outside $S$. Taking the dual of the exact sequence (1), we have an exact sequence

$$
0 \rightarrow \bigoplus_{v \in S'_{K_s}} I_v(\mathcal{M}_S/K_s) \rightarrow X_{K, S} \rightarrow X_K \rightarrow 0
$$

where $\mathcal{M}_S/K_s$ is the maximal abelian pro-$p$ extension unramified outside $S$. We note that $I_v$ is isomorphic to $\mathbb{Z}/e_v \mathbb{Z}(1)$.
where \( I_v(M_S/K_\infty) \simeq \mathbb{Z}_p(1) \) is the inertia group of \( v \) in \( \mathcal{X}_{K,S} \). As we proved in the proof of Proposition 2.3, \( X_K \rightarrow X_L \) is injective. We define \( X_{L,S} \) similarly. Then the above injectivity implies that the canonical map \( \mathcal{X}_{K,S} \rightarrow \mathcal{X}_{L,S} \) is also injective. Taking the dual, we know that the corestriction map \( H^1(\mathcal{O}_{L_{\infty,S}}, \mathbb{Q}_p/\mathbb{Z}_p) \rightarrow H^1(\mathcal{O}_{K_{\infty,S}}, \mathbb{Q}_p/\mathbb{Z}_p) \) is surjective.

By the Serre-Hochschild spectral sequence, we have an isomorphism
\[
H^1(G, H^1(\mathcal{O}_{L_{\infty,S}}, \mathbb{Q}_p/\mathbb{Z}_p)) \simeq H^3(G, \mathbb{Q}_p/\mathbb{Z}_p).
\]
The latter group is isomorphic to \( H^1(G, \mathbb{Q}_p/\mathbb{Z}_p) \) because \( G \) is cyclic. Therefore, we have
\[
H^1(G, H^1(\mathcal{O}_{L_{\infty,S}}, \mathbb{Q}_p/\mathbb{Z}_p)) \simeq \mathbb{Z}/p\mathbb{Z}.
\]
This shows that the kernel of
\[
H^1(\mathcal{O}_{L_{\infty,S}}, \mathbb{Q}_p/\mathbb{Z}_p)_G \rightarrow H^1(\mathcal{O}_{K_{\infty,S}}, \mathbb{Q}_p/\mathbb{Z}_p) \rightarrow H^1(\mathcal{O}_{L_{\infty,S}}, \mathbb{Q}_p/\mathbb{Z}_p)
\]
is of order \( p \) where \( M_G \) means the module of \( G \)-coinvariants of \( M \). Since the kernel of the restriction map \( H^1(\mathcal{O}_{K_{\infty,S}}, \mathbb{Q}_p/\mathbb{Z}_p) \rightarrow H^1(\mathcal{O}_{L_{\infty,S}}, \mathbb{Q}_p/\mathbb{Z}_p) \) is \( H^1(G, \mathbb{Q}_p/\mathbb{Z}_p) \) which is of order \( p \), we know that the corestriction map gives an isomorphism
\[
H^1(\mathcal{O}_{L_{\infty,S}}, \mathbb{Q}_p/\mathbb{Z}_p)_G \simeq H^1(\mathcal{O}_{K_{\infty,S}}, \mathbb{Q}_p/\mathbb{Z}_p).
\]
Consider the commutative diagram
\[
\begin{array}{c}
H^1(\mathcal{O}_{L_{\infty,S}}, \mathbb{Q}_p/\mathbb{Z}_p)_G \\
\downarrow \\
H^1(\mathcal{O}_{K_{\infty,S}}, \mathbb{Q}_p/\mathbb{Z}_p)_G
\end{array} \quad \begin{array}{c}
\longrightarrow \\
\downarrow \\
\longrightarrow
\end{array} \quad \begin{array}{c}
H^1(\mathcal{O}_{L_{\infty,S}}, \mathbb{Q}_p/\mathbb{Z}_p)_G \\
\downarrow \\
H^1(\mathcal{O}_{K_{\infty,S}}, \mathbb{Q}_p/\mathbb{Z}_p)_G
\end{array}
\]
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 \( X_K \rightarrow X_L^G \) is surjective.

As we have mentioned, we proved the injectivity of \( X_K \rightarrow X_L \) in the proof of Proposition 2.3. Therefore, we get the bijectivity of \( X_K \rightarrow X_L^G \).

We go back to the proof of (2). By Lemma 2.4, we have
\[
\hat{H}^0(G, X_L) \simeq \text{Coker}(X_L \rightarrow X_K).
\]
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 \( \mu \)-invariant of \( L \) to prove the fundamental exact sequence in Proposition 2.1. The argument becomes much simpler if one is willing to assume \( \mu = 0 \).
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 \(K_\infty, L_\infty\), respectively. We also use the notation \(G = \text{Gal}(L''_\infty/K_\infty)\) in the previous section where \(L''_\infty/K_\infty\) is the maximal subextension of \(L_\infty/K_\infty\), which is unramified outside \(p\).

**Theorem 3.1.** Let \(L/K\) be as above and \(G = \text{Gal}(L/K)\). We assume that \(G\) is elementary abelian and \(G \simeq (\mathbb{Z}/p\mathbb{Z})^{s}\) for some \(s \in \mathbb{Z}_{>0}\). We assume that the \(\mu\)-invariant of \(X_K\) is zero, and denote the \(\lambda\)-invariant by \(\lambda_K\). Let \(S'_{K_\infty}\) be the set of primes of non-\(p\)-adic primes of \(K_\infty\) that are ramified in \(L_\infty\), \(n(L/K) = \#S'_{K_\infty}\), and \(\epsilon(L/K) = \dim_{\mathbb{F}_p} G\). Then the structure of the module \((X_L)_G\) of Galois coinvariants as a \(\mathbb{Z}_p\)-module is as follows:

\[
(X_L)_G \simeq (\mathbb{Z}/p\mathbb{Z})^{t} \oplus \mathbb{Z}_p^{\oplus \lambda_K},
\]

where

\[
t = \frac{s(s - 3)}{2} + n(L/K) + \epsilon(L/K).
\]

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

**Proof.** Since we assumed the vanishing of the \(\mu\)-invariant of \(X_K\), it is a free \(\mathbb{Z}_p\)-module by Theorem 18 in [4], and \(X_K \simeq \mathbb{Z}_p^{\oplus \lambda_K}\) as \(\mathbb{Z}_p\)-modules. By Proposition 2.3, \((X_L)_G\) is a finitely generated \(\mathbb{Z}_p\)-module with rank \(\lambda_K\), and the \(\mathbb{Z}_p\)-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

\[
t = \frac{s(s - 1)}{2} + n(L/K) + \epsilon(L/K) - s = \frac{s(s - 3)}{2} + n(L/K) + \epsilon(L/K).
\]

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 \(\mathbb{Z}_p\)-module.

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

By the fundamental exact sequence, we have $H^{-1}(G_1, X_L) = 0$. 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 $\mathbb{Z}_p$-module, so we can write

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

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

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

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 $\hat{H}^{-1}(G, X_L) = (\mathbb{Z}/p\mathbb{Z})^{\oplus n\epsilon(L/K)}$, which implies $c = n(L/K)$. By the fundamental exact sequence for $M/K$, we get $\hat{H}^{-1}(G_2, X_M) = (\mathbb{Z}/p\mathbb{Z})^{\oplus n(M/K)-1} = (\mathbb{Z}/p\mathbb{Z})^{\oplus n(L/K)-1}$ and $\hat{H}^0(G_2, X_M) = 0$, which imply

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

(This procedure is the same as the proof of Kida’s formula in Iwasawa [5].) Comparing the $\mathbb{Z}_p$-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 $\epsilon(L/K) = 0$. 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 $K_\infty$ in $M_\infty$, and $S'(L_\infty/M_\infty)$ is the set of non $p$-adic ramifying primes of $M_\infty$ in $L_\infty$. 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 $M_\infty$ 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 $K_\infty$ below $w$, then $v$ is not in $S'(M_\infty/K_\infty)$ and it splits completely in $M_\infty$. 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 $G_1 = \text{Gal}(L/M)$. By the fundamental exact sequence for $L/M$, we have an exact sequence

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

Therefore, we have an isomorphism

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

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

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

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

We take a generator \(\sigma\) of \(G_2\) and put \(S = \sigma - 1\). We identify \(\mathbb{F}_p[G_2]\) with \(\mathbb{F}_p[[S]]/(S^p)\). The above exact sequence is a sequence of \(\mathbb{F}_p[[S]]/(S^p)\)-modules. We put \(R = \mathbb{F}_p[[\pi]]\) in the following Lemma 3.2, where \(\pi\) is an indeterminate. Then \(\mathbb{F}_p[G_2] \cong R/(\pi^p)\) and \(\mathbb{F}_p[G_2]/(N_{G_2}) \cong R/(\pi^{p-1})\). From the lemma we obtain that the minimal number of generators of the \(\mathbb{F}_p[G_2]\)-module \(((X_L)_{G_1}) \otimes \mathbb{F}_p\) 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 \(((X_L)_{G_1}) \otimes \mathbb{F}_p\), which of course gives \(((X_L)_G) \otimes \mathbb{F}_p\). On the other hand, taking \(G_2\)-coinvariants simply means factoring out by \(\pi\). Therefore, we obtain

\[
((X_L)_G) \otimes \mathbb{F}_p = ((X_L)_{G_1} \otimes \mathbb{F}_p)_{G_2} \\
\cong (\mathbb{Z}/p\mathbb{Z})^{\oplus n(L/K)+\lambda_K-1}. 
\]

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 \(\mathbb{Z}/\pi\)-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 \(\pi\) 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

\[
M \cong (R/(\pi^n))^{\oplus(a+b+\delta)} \oplus (R/(\pi^{n-1}))^{\oplus(c+1-2\delta)} \oplus (R/(\pi^{n-2}))^{\oplus\delta}, 
\]

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 \(\pi^n\) 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 $G = (\mathbb{Z}/p\mathbb{Z})^{\oplus s}$ 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 $X_L \rightarrow X_{M(H)}$ on the Galois groups induces the canonical homomorphism $\hat{H}^{-1}(G, X_L) \rightarrow \hat{H}^{-1}(G/H, X_{M(H)})$ on the cohomology groups by the commutative diagram

$$
\begin{array}{c}
0 \rightarrow \hat{H}^{-1}(G, X_L) \rightarrow (X_L)_G \rightarrow X_K \\
\downarrow \text{can} \quad \downarrow \text{Res} \quad \downarrow \text{id}
\end{array}
$$

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

$$
\begin{array}{c}
0 \rightarrow \bigwedge^2 G \rightarrow \hat{H}^{-1}(G, X_L) \rightarrow \bigoplus_v I_v(L/K) \\
\downarrow \text{can} \quad \downarrow \text{can} \quad \downarrow \text{id}
\end{array}
$$

where the left vertical arrow is induced by the natural map $G \rightarrow G/H$, and the right vertical arrow 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:

$$
\begin{array}{c}
0 \rightarrow \bigwedge^2 G \rightarrow \hat{H}^{-1}(G, X_L) \rightarrow \bigoplus_{H \in \mathcal{H}} I_v(L/K) \\
0 \rightarrow \bigwedge^2 G/H \rightarrow \hat{H}^{-1}(G/H, X_{M(H)}) \rightarrow \bigoplus_{H \in \mathcal{H}} I_v(M(H)/K)
\end{array}
$$

Since $G$ is elementary abelian, $\alpha$ is injective. It is also easy to see that $\gamma$ is injective. Therefore, $\beta$ is also injective. Since $G/H \simeq (\mathbb{Z}/p\mathbb{Z})^{\oplus 2}$, we have shown in Step 2 that the range of $\beta$ 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 $\hat{H}^{-1}(G, X_L) \simeq (\mathbb{Z}/p\mathbb{Z})^{\oplus t}$ 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 $\Lambda_L = \mathbb{Z}_p[[\text{Gal}(L_{\infty}/k)]]$. We fix a generator $\gamma$ of $\text{Gal}(L_{\infty}/L) \simeq \mathbb{Z}_p$ and put $T = \gamma - 1$. Then we have $\Lambda_L = \mathbb{Z}_p[[\text{Gal}(L/k)][[T]]]$. 
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 $\kappa : \text{Gal}(L(\mu_p)_\infty/k) \rightarrow \mathbb{Z}_p^\times$. For a character $\chi$ of $\text{Gal}(L/k)$ and $n \in \mathbb{Z}_{>0}$ we regard $\chi^n$ as a $p$-adic character of $\text{Gal}(L(\mu_p)_\infty/k)$. The group homomorphism $\chi^n$ extends to a ring homomorphism $\Lambda_{L(\mu_p)} \rightarrow \mathbb{Q}_p$. Furthermore, we can extend it to the total quotient ring of $\Lambda_{L(\mu_p)}$ and denote it also by $\chi^n$. 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

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

for all positive integers $n \in \mathbb{Z}_{>0}$ and all characters $\chi$ of $\text{Gal}(L/k)$ 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 $\chi$ 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 $X_{L,S}$ be the Galois group of $L_{L_\infty,S}/L_\infty$, the maximal abelian pro-$p$ extension which are unramified outside $S$. Therefore, $X_{L,S}$ is the Pontrjagin dual of the étale cohomology $H^1(\mathcal{O}_{L_\infty,S}, \mathbb{Q}_p/\mathbb{Z}_p)$ (see the proof of Proposition 2.1). Let $\chi$ be a character of $\text{Gal}(L/k)$, and $\mathcal{O}_\chi = \mathbb{Z}_p[\text{Image}(\chi)]$ on which $\text{Gal}(L/k)$ acts via $\chi$. For a $\mathbb{Z}_p[\text{Gal}(L/k)]$-module $M$, we define the $\chi$-quotient by $M_\chi = M \otimes_{\mathbb{Z}_p[\text{Gal}(L/k)]} \mathcal{O}_\chi$. Then $(X_{L,S})_\chi$ is a finitely generated torsion $(\Lambda_L)_\chi$-module. Let $\tilde{\chi} : \Lambda_L \rightarrow (\Lambda_L)_\chi$ be the ring homomorphism induced by $\chi$. The main conjecture which was proved by Wiles in [14] Theorem 1.3 (at least assuming the vanishing of the $\mu$-invariant) is

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

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 $\text{char}((\Lambda_L)_\chi)(M) = \text{Fitt}((\Lambda_L)_\chi)(M)$ 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 $\text{Fitt}_{\Lambda_L}(X_{L,S})$ or not. The answer is No if $\text{Gal}(L/k) \otimes \mathbb{Z}_p$ 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 $\mu$-invariant of $X_L$. Suppose that the $p$-Sylow subgroup of $\text{Gal}(L/k)$ is generated by exactly $s$ elements. Then we have

$$\text{Fitt}_{\Lambda_L}(X_{L,S}) = T^{1-s} \mathfrak{A}_{\text{Gal}(L/k)} \Theta_{L_\infty/k,S}$$
where \( \mathfrak{A}_{\text{Gal}(L/k)} \) is the ideal of \( \Lambda_L \) 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 \( \text{Gal}(L/k) \).

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 \( T^{1-s}\mathfrak{A}_{\text{Gal}(L/k)} \). The precise definition is to be found in §1 of loc. cit. Let \( \Delta \) be the non-\( p \)-part of \( \text{Gal}(L/k) \) and \( G \) be the \( p \)-part, in particular, \( \text{Gal}(L/k) \approx \Delta \times G \). The ideal \( \mathfrak{A}_{\text{Gal}(L/k)} \) is a purely algebraic invariant that depends only on \( G \). For every character \( \xi \) of \( \Delta \) except for the trivial character, the \( \xi \)-component of \( T^{1-s}\mathfrak{A}_{\text{Gal}(L/k)} \) is the unit ideal. We regard the trivial character component \( (T^{1-s}\mathfrak{A}_{\text{Gal}(L/k)})^1 = T^{1-s}(\mathfrak{A}_{\text{Gal}(L/k)})^1 \) as an ideal of \( \Lambda[G] \). The ideal \( (\mathfrak{A}_{\text{Gal}(L/k)})^1 \) is defined by \( (\mathfrak{A}_{\text{Gal}(L/k)})^1 = \text{Fitt}_{\Lambda[G]}(\Omega^2) \) with a certain explicit second syzygy \( \Omega^2 \) of the module \( Z \) over \( G \) with trivial \( \text{Gal}(k_\infty/k) \)-action.

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

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

(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 \( \mathbb{Z}_p[G] \) and \( J_G \) the ideal of \( \mathbb{Z}_p[G] \) generated by \( I_G \) and \( p^{n_1} \). Then \( \mathfrak{n}_d \) in [3] §1 satisfies \( \mathfrak{n}_d \subset J_{\Lambda[G]}^d \), which implies \( \mathfrak{m}_d \subset J_G^d \) by Proposition 1.5 in [3] where \( \mathfrak{m}_d \) is the ideal of \( \mathbb{Z}_p[G] \) appearing in Proposition 1.6 in [3]. We also note \( \mathfrak{m}_{s+1} \subset I_G J_G^t \) for \( t = (s-1)/2 \), since any monomial appearing in a \( (t+1) \)-minor of \( \tilde{M}_s \) can only have \( t \) factors of type \( \nu \) and therefore must have at least one factor of type \( \tau \). 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 \( L = L(p) \). We put \( \Lambda_L = \mathbb{Z}_p[[\text{Gal}(L_\infty/k)]] \). As in §2 let \( X_L \) be the Galois group of the maximal abelian pro-\( p \) extension \( L_{L_\infty,S_p}/L_\infty \), which is unramified outside \( p \). We call \( X_L \) the \( p \)-ramified Iwasawa module of \( L_\infty \); it is a module over \( \Lambda_L \).

For \( L(p)^+ \), consider \( \Theta_{L(p)^+}^{S_p/k_S} \) defined in the previous section. When we take \( S \) to be minimal, namely the set of ramifying primes
of $k$ in $L(\mu_p)^+$, we simply write $\Theta_{L(\mu_p)^+_{/k}}$ for $\Theta_{L(\mu_p)^+_{/k,S}}$. We note that $[L(\mu_p)^+:L]$ is prime to $p$, which implies that $\Lambda_L$ can be regarded as a direct summand of $\Lambda_{L(\mu_p)^+}$. We denote by $\Theta_{L_{/k}} \in \Lambda_L$ the $\Lambda_L$-component of $\Theta_{L(\mu_p)^+_{/k}}$. We are interested in whether $T\Theta_{L_{/k}}$ is in the Fitting ideal $\text{Fitt}_{\Lambda_L}(X_L)$ 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 $\text{Gal}(L/K)$ is elementary $p$-abelian. We write $\text{Gal}(L/K) = (\mathbb{Z}/p\mathbb{Z})^s$ for some $s \geq 0$. We also assume the vanishing of the $\mu$-invariant of $X_L$ and one of the following conditions.

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

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

(iii) $s \geq 4$.

Then we have

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

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

**Proof of Thm. 5.1.** We may assume that $K = k$. In fact, put $\Delta = \text{Gal}(K/k)$, and regard it as a subgroup of $\text{Gal}(L/k)$. Let $L(\Delta)$ be the intermediate field of $L/k$ such that $\text{Gal}(L/L(\Delta)) = \Delta$, so $L(\Delta)/k$ is a $p$-extension. Then, since $\#\Delta$ is prime to $p$, $\Lambda_{L(\Delta)}$ is a direct summand of $\Lambda_L$. The $\Lambda_{L(\Delta)}$-component of $\Theta_{L_{/k}}$ is $\Theta_{L(\Delta)_{/k}}$ because the set of primes of $k$ ramifying in $L_\infty$ coincides with the set of primes of $k$ ramifying in $L(\Delta)_\infty$. Since $H^1(O_{L(\Delta)_\infty,S_p}, Q_p/Z_p) \rightarrow H^1(O_{L_\infty,S_p}, Q_p/Z_p)^\Delta$ 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 $\Lambda = \Lambda_k = \mathbb{Z}_p[[\text{Gal}(k_\infty/k)]] \simeq \mathbb{Z}_p[[T]]$. We first consider the restriction homomorphism $c_{L_\infty/k_\infty} : \Lambda_L \rightarrow \Lambda$. Let $S'$ be the set of non $p$-adic ramifying primes of $k$ in $L_\infty$. Since only $p$-adic primes are ramified in $k_\infty$, we have

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

where $\varphi_v$ is the Frobenius of $v$ in $\text{Gal}(k_\infty/k)$. 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 $p \in \Lambda/p = \mathbb{F}_p[[T]]$ satisfies

$$\text{ord}_T(T\Theta_{k_\infty/k} \mod p) = \lambda_k,$$
where $\lambda_k$ is the $\lambda$-invariant of $X_L$ and $\text{ord}_T$ is the normalized additive valuation of $\mathbb{F}_p[[T]]$, because we are assuming the vanishing of the $\mu$-invariant.

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

$$\text{ord}_T(\prod_{v \in S'} (1 - N(v)^{-1}\varphi_v) \mod p) = \text{ord}_T(\prod_{v \in S'} (1 - \varphi_v) \mod p)$$

$$= \sum_{v \in S'} \text{ord}_T((1 - \varphi_v) \mod p)$$

$$= \#S'_{k_\infty}$$

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

$$(3) \quad \text{ord}_T(c_{L_{\infty}/k_\infty}(T\Theta_{L_{\infty}/k}) \mod p) = \lambda_k + \#S'_{k_\infty}.$$

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

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

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

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

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

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

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

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 $A_F = \text{Cl}_F \otimes \mathbb{Z}_p$. For a CM-field $L$ and the cyclotomic $\mathbb{Z}_p$-extension $L_{\infty}/L$ and the $n$-th layer $L_n$, we define $A_{L_{\infty}} = \lim_{\rightarrow} A_{L_n}$, which is a discrete $\Lambda_L = \mathbb{Z}_p[[\text{Gal}(L_{\infty}/k)]]$-module. We consider the Pontrjagin dual $(A_{L_{\infty}})^{\vee}$ with the cogredient action of $\text{Gal}(L_{\infty}/k)$. So it is a compact $\Lambda_L$-module.
For a finite abelian extension $L/k$ where $k$ is totally real and $L$ is a CM-field, the Stickelberger element $\theta_{L/k} \in \mathbb{Q}[\text{Gal}(L/k)]$ is the unique element which satisfies
\[
\chi(\theta_{L/k}) = LS_L(0, \chi^{-1})
\]
for all characters $\chi$ of $\text{Gal}(L/k)$ where we extended $\chi$ to the ring homomorphism $\chi : \mathbb{Q}[\text{Gal}(L/k)] \rightarrow \mathbb{Q}(\text{Image}(\chi))$ 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 $\gamma$ be the generator we fixed and $\kappa$ the cyclotomic character. We know $(\gamma - \kappa(\gamma))\theta_{L_n/k} \in \mathbb{Z}_p[\text{Gal}(L_n/k)]$ and denote the projective limit by $(\gamma - \kappa(\gamma))\theta_{L_\infty/k} \in A_L$.

**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
\[
(\gamma - \kappa(\gamma))\theta_{L_\infty/k} \not\in \text{Fitt}_{\Lambda_L}((A_{L_\infty})^\vee).
\]

**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 $k = \mathbb{Q}$ and suitable abelian fields $L$. Indeed, the paper [7] determines the Fitting ideal of the non-dualised class group over $L_\infty$, 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 Thm. 6.1.** Suppose that $\kappa : \text{Gal}(L_\infty/k) \rightarrow \mathbb{Z}_p^\times$ is the cyclotomic character. Let $\tau$, $\iota$ be the automorphisms of the total quotient ring of $\Lambda_L$ induced by $\sigma \mapsto \kappa(\sigma)\sigma$, $\sigma \mapsto \sigma^{-1}$, respectively, for any $\sigma \in \text{Gal}(L_\infty/k)$. 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 $A_{L_\infty}$ (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
\[
(\kappa(\gamma)\gamma^{-1} - 1)\theta_{L_\infty/k} \not\in \text{Fitt}_{\Lambda_L}((A_{L_\infty}^-)^\vee),
\]
which completes the proof. \(\square\)
Remark 6.3. Put $\Delta = \text{Gal}(K/k)$ and let $\omega : \Delta \rightarrow \mathbb{Z}_p^\times$ be the Teichmüller character. Since the order of $\Delta$ is prime to $p$, $\mathbb{Z}_p[\Delta]$ is decomposed into character components, so any $\mathbb{Z}_p[\Delta]$-module $M$ is decomposed into character components, $M = \bigoplus_\chi M^\chi$ where $\chi$ runs over $\mathbb{Q}_p$-conjugacy classes of characters of $\Delta$. By the same method as the proof of Theorem 6.1, we see that

$$(\gamma - \kappa(\gamma))\theta_{L_\infty/k} \not\in \text{Fitt}_\Lambda((A_{L_\infty}^\infty)^\vee)$$

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

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

where $L(\Delta)$ is the intermediate field of $L/k$ such that $\text{Gal}(L/L(\Delta)) = \Delta$. Since $T\Theta_{L(\Delta)/k} \not\in \text{Fitt}_{\Lambda_t(\Delta)}(X_{L(\Delta)})$ by Theorem 5.1, we get the above statement on the $\omega$-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 $k = \mathbb{Q}$. We note that the vanishing of the $\mu$-invariant is proved by Ferrero and Washington. We repeat that the cases (i) and (ii) in Theorem 6.1 never happen over $k = \mathbb{Q}$, and so we may concentrate on the case (iii).

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

$$p^n > \sum_{\ell \in S'} p^{\text{ord}_\ell(t-1)-1}.$$ 

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

$$\text{Ann}_{R_n}(\mu_p^{n+1})\theta_{L_n/\mathbb{Q}} \not\subset \text{Fitt}_{R_n}((A_{L_n}^\infty)^\vee),$$

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

$$\text{Ann}_{R_n}(\mu_p^{n+1})\theta_{L_n/\mathbb{Q}}^\omega \not\subset \text{Fitt}_{R_n^\omega}((A_{L_n}^\infty)^\vee)$$

holds.

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

$$(\gamma - \kappa(\gamma))\theta_{L_n/\mathbb{Q}}^\omega \not\subset \text{Fitt}_{R_n^\omega}((A_{L_n}^\infty)^\vee).$$
Put $K = \mathbb{Q} (\mu_p)$, $\Delta = \text{Gal}(K/\mathbb{Q})$, and $G = \text{Gal}(L/K)$. As in Remark 6.3, we denote by $L(\Delta)$ the intermediate field of $L/\mathbb{Q}$ such that $\text{Gal}(L/L(\Delta)) = \Delta$. Put $G = \text{Gal}(L(\Delta)/\mathbb{Q}) = \text{Gal}(L/\mathbb{Q}(\mu_p)) \simeq (\mathbb{Z}/p\mathbb{Z})^{\oplus s}$. It is well-known that $X_Q = 0$. Therefore, applying Theorem 3.1 for $L(\Delta)/\mathbb{Q}$, we have

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

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

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

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

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

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

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

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

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

Since the $p$-adic primes of $L_n^+$ are ramified in $L_n$, the natural map $A_{L_n}^+ \rightarrow (A^\infty_{L(\Delta)})^\Gamma_n$ is bijective. Therefore, we get

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

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

$$T^{\# S'_{Q_{\infty}} + 1}\theta_{K_n}^\infty \in \text{Fitt}_{\mathbb{F}_p[[T]]/(T^n)} (\hat{H}^{-1} (G, X_{L(\Delta)})) = (T^t)$$

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

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

$$(\text{Ann}_{\mathbb{Z}[\text{Gal}(L/\mathbb{Q})]}(\mu_m)\theta_{L/\mathbb{Q}}) \otimes \mathbb{Z}_p \not\subset \text{Fitt}_{\mathbb{Z}[\text{Gal}(L/\mathbb{Q})]}(A_L^\omega).$$

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

**Proof.** Clearly, $L$ has a unique subfield $L'$ such that the conductor of $L'$ is $m/p^{n-1}$, and $L'$ contains $\mathbb{Q}(\mu_p)$, and $\text{Gal}(L'/\mathbb{Q}(\mu_p)) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$. Put $F = L'(\mu_p)$. By Corollary 7.1, we have

$$(\text{Ann}_{\mathbb{Z}[\text{Gal}(F/\mathbb{Q})]}(\mu_p)\theta_{F/\mathbb{Q}})^\omega \not\subset \text{Fitt}_{\mathbb{Z}[\text{Gal}(F/\mathbb{Q})]}(A_F^\omega)^\omega.$$ 

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

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

where $c_{L/F} : \mathbb{Z}_p[\text{Gal}(L/\mathbb{Q})]^\omega \rightarrow \mathbb{Z}_p[\text{Gal}(F/\mathbb{Q})]^\omega$ is the restriction map.

This implies that

$$(\text{Ann}_{\mathbb{Z}_p[\text{Gal}(L/\mathbb{Q})]}(\mu_p)\theta_{L/\mathbb{Q}})^\omega \not\subset \text{Fitt}_{\mathbb{Z}_p[\text{Gal}(L/\mathbb{Q})]}^\omega((A_L^\omega)^\omega),$$

which implies the conclusion. \qed

**Remark 7.3.** For example, $m = 27\cdot7\cdot13\cdot19\cdot31$ 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 $\mathbb{Q}$ has $p$-rank $\geq 4$ (namely, $s = \dim_{\mathbb{F}_p} \text{Gal}(L/\mathbb{Q}) \otimes \mathbb{F}_p \geq 4$). In this section, let us examine several examples in the case $s = 2$ for $k = \mathbb{Q}$.

Consider the subset $P = \{\ell \mid \ell \equiv 1 \pmod{p}\}$ of the set of prime numbers. For $\ell \in P$, we denote by $F(\ell)$ the subfield of $\mathbb{Q}(\mu_\ell)$ of degree $p$. For two primes $\ell_1, \ell_2 \in P$, 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 $\ell_1$, $\ell_2$ be two primes in $P$, and assume $\ell_1 \not\equiv 1 \pmod{p^2}$. Put $L = L(\ell_1, \ell_2)$, and $G = \text{Gal}(L/\mathbb{Q}) = \text{Gal}(F(\ell_1, \ell_2)/\mathbb{Q})$.

(1) We have $A^\omega_L(\ell_1) = 0$.

(2) For any $\ell_2 \in P$, $A^\omega_L$ is generated by one element as a $\mathbb{Z}_p[G]$-module.

(3) Suppose that $\ell_2$ satisfies at least one of the following conditions:
   (i) $\ell_2 \not\equiv 1 \pmod{p^2}$;
   (ii) $\ell_2$ does not split completely in $F(\ell_1)$.

Then we have
$$\text{Fitt}_{\mathbb{Z}_p[G]}((A^\omega_L)^\vee) = \text{Fitt}_{\mathbb{Z}_p[G]}(A^\omega_L).$$

(4) Suppose that $\ell_2$ satisfies neither (i) nor (ii) above. Then $N_{G_2}$ is in $\text{Fitt}_{\mathbb{Z}_p[G]}(A^\omega_L)$, but not in $\text{Fitt}_{\mathbb{Z}_p[G]}((A^\omega_L)^\vee)$ where $G_2 = \text{Gal}(L/L(\ell_1))$ and $N_{G_2}$ is the norm element of $G_2$ in $\mathbb{Z}_p[G]$.

In particular, we have
$$\text{Fitt}_{\mathbb{Z}_p[G]}((A^\omega_L)^\vee) \neq \text{Fitt}_{\mathbb{Z}_p[G]}(A^\omega_L).$$

Proof. We first note that the natural maps $A^\omega_{L(\ell_1)} \rightarrow A^\omega_L$, $A^\omega_{L(\ell_1)} \rightarrow A^\omega_{L(\ell_1)\infty}$, $A^\omega_L \rightarrow A^\omega_{L(\ell_1)\infty}$ are all injective.

(1) Put $G_1 = \text{Gal}(F(\ell_1)/\mathbb{Q})$. By our assumption $\ell_1 \not\equiv 1 \pmod{p^2}$, there is only one prime of $F(\ell_1)\infty$ above $\ell_1$. It follows from the fundamental exact sequence for $F(\ell_1)/\mathbb{Q}$ that $\hat{H}^{-1}(G_1, X_{F(\ell_1)}) = 0$. Since $X_{\mathbb{Q}} = 0$, 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 $\ell_i$. We denote by $\kappa(w_i)$ the residue field of $w_i$, and by $D_{\ell_i}$ the decomposition group of $w_i$ in $G$. We need the following lemma.

Lemma 8.2. We have an exact sequence
$$\hat{H}^0(G, \mu_p) \rightarrow \hat{H}^0(D_{\ell_1}, \kappa(w_1)^\times) \oplus \hat{H}^0(D_{\ell_2}, \kappa(w_2)^\times) \rightarrow \hat{H}^{-1}(G, A^\omega_L)$$

$$\rightarrow H^1(G, \mu_p) \xrightarrow{\delta_1} H^1(D_{\ell_1}, \kappa(w_1)^\times) \oplus H^1(D_{\ell_2}, \kappa(w_2)^\times) \rightarrow \hat{H}^0(G, A^\omega_L)$$

$$\rightarrow H^2(G, \mu_p) \xrightarrow{\delta_2} H^2(D_{\ell_1}, \kappa(w_1)^\times) \oplus H^2(D_{\ell_2}, \kappa(w_2)^\times).$$

where $G$ acts on $\mu_p$ trivially. The map $\delta_1$ 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 $H^1(D_{\ell_i}, \kappa(w_i)^\times) = H^1(D_{\ell_i}, U_{L_{w_i}}) \simeq \mathbb{Z}/e_{w_i} \mathbb{Z} = \mathbb{Z}/p\mathbb{Z}$, 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 $L/\mathbb{Q}(\mu_p)$. It is well-known that the kernel of $\delta_1$ is isomorphic to the kernel of $A^\omega_{\mathbb{Q}(\mu_p)} \rightarrow A^\omega_{L(\ell_1, \ell_2)}$. But $A^\omega_{\mathbb{Q}(\mu_p)} = 0$, so the kernel of $\delta_1$ 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, \( \hat{H}^0(D_{\ell_1}, \kappa(w_1)^x) \) is isomorphic to the inertia group of \( \ell_1 \) 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 \( \hat{H}^0(D_{\ell_1}, \kappa(w_1)^x) = F_{\ell_1}^x \otimes \mathbb{Z}/p\mathbb{Z} \cong \mu_p \), and the natural map \( \hat{H}^0(G, \mu_p) = \mu_p \to \hat{H}^0(D_{\ell_1}, \kappa(w_1)^x) = \mu_p \) is bijective. Therefore, it follows from Lemma 8.2 that \( \hat{H}^{-1}(G, A_L^\mu) \) is isomorphic to \( \mathbb{Z}/p\mathbb{Z} \). Since \( A_{Q(\mu_p)}^\mu = 0 \), we know that \( A_L^\mu \) is generated by one element as a \( G \)-module.

(3) We prove that \( (A_L^\mu)^\vee \) 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 \( F(\ell_1, \ell_2)/Q \),

\[
0 \to \bigwedge^2 G \to \hat{H}^{-1}(G, X_{F(\ell_1, \ell_2)}) \to \bigoplus_{v|\ell_1 \ell_2} \mathbb{Z}/p\mathbb{Z} \to G \to 0
\]

is exact. Since neither \( \ell_1 \) nor \( \ell_2 \) splits in \( Q_\infty \) by our assumption (i), we know \( \bigoplus_{v|\ell_1 \ell_2} \mathbb{Z}/p\mathbb{Z} \cong (\mathbb{Z}/p\mathbb{Z})^{\oplus 2} \), which implies \( \hat{H}^{-1}(G, X_{F(\ell_1, \ell_2)}) \cong \mathbb{Z}/p\mathbb{Z} \) by the above exact sequence. Since \( X_Q = 0 \), \( X_{F(\ell_1, \ell_2)} \) 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 \( (A_L^\mu)^\vee \).

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

\[
0 \to \hat{H}^{-1}(G_2, X_{F(\ell_1, \ell_2)}) \to \bigoplus_{v|\ell_2} \mathbb{Z}/p\mathbb{Z} \to G_2 \to 0
\]

is exact where \( v \) runs over primes of \( F(\ell_1)_\infty \) above \( \ell_2 \). By our assumption (ii), \( \bigoplus_{v|\ell_2} \mathbb{Z}/p\mathbb{Z} \) is a quotient of \( \mathbb{F}_p[[\text{Gal}(F(\ell_1)_\infty/F(\ell_1))]] = \mathbb{F}_p[[\text{Gal}(Q_\infty/Q)]] \) and the third map in the exact sequence is induced by the augmentation map \( \mathbb{F}_p[[\text{Gal}(Q_\infty/Q)]] \to \mathbb{F}_p \). It follows that \( \hat{H}^{-1}(G_2, X_{F(\ell_1, \ell_2)}) \) is cyclic as a \( \Lambda_Q \)-module. Since \( X_{F(\ell_1)} = 0 \) by (1), we have \( (X_{F(\ell_1, \ell_2)})_2 = \hat{H}^{-1}(G_2, X_{F(\ell_1, \ell_2)}) \) 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 \( (A_L^\mu)^\vee \).

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

\[
\text{Fitt}_{\mathbb{Z}_p[G]}(A_L^\mu) = \text{Fitt}_{\mathbb{Z}_p[G]}((A_L^\mu)^\vee) = \text{Ann}_{\mathbb{Z}_p[G]}(A_L^\mu).
\]

This completes the proof of (3).
(4) Since $A_{\ell_i}^p = 0$ by (1), $N_{G_2}$ is in $\text{Ann}_{\mathbb{Z}[G]}(A_{\ell_i}^p)$. Therefore, it is also in $\text{Fitt}_{\mathbb{Z}[G]}(A_{\ell_i}^p)$ because $A_{\ell_i}^p$ is cyclic by (2).
Consider the homomorphism $H^2(G, \mu_p) \rightarrow H^2(D_{\ell_2}, \kappa(w_2)^\times)$, which is obtained by the composition of $f_2$ in Lemma 8.2 and the second projection. Since $\ell_2$ splits completely in $L(\ell_1)$ and ramifies in $L/L(\ell_1)$, $\kappa(w_2) = \mathbb{F}_{\ell_2}$. Put $r_2 = \text{ord}_p(\ell_2 - 1)$. 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

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

is induced by the natural homomorphisms $D_{\ell_2} \rightarrow G$, $\mu_p \rightarrow \mu_{p^{r_2}}$. In particular, it factors through $H^2(D_{\ell_2}, \mu_p)$. Recall that $D_{\ell_2}$ is cyclic of order $p$. Therefore, $H^2(D_{\ell_2}, \mu_p) \rightarrow H^2(D_{\ell_2}, \mu_{p^{r_2}})$ is the zero map. It follows that the $\mathbb{F}_p$-dimension of the image of $f_2$ in Lemma 8.2 is equal to or smaller than 1. By Lemma 8.2, we have

$$\dim_{\mathbb{F}_p}(A_{\ell_i}^p)^G \geq \dim_{\mathbb{F}_p} H^2(G, \mu_p) - 1 = 3 - 1 = 2.$$ 
Suppose that $a \in \mathbb{Z}_p[G]$ is in $\text{Fitt}_{\mathbb{Z}_p[G]}((A_{\ell_i}^p)^G)$. Let $c : \mathbb{Z}_p[G] \rightarrow \mathbb{Z}_p$ be the augmentation map. We have $c(a) \in \text{Fitt}_{\mathbb{Z}_p}(((A_{\ell_i}^p)^G)^G)$, so $p^2$ divides $c(a)$ because $\dim_{\mathbb{F}_p}((A_{\ell_i}^p)^G) \geq 2$. Namely, we get

$$a \in \text{Fitt}_{\mathbb{Z}_p[G]}((A_{\ell_i}^p)^G) \implies p^2|c(a).$$

This shows that $N_{G_2}$ is not in $\text{Fitt}_{\mathbb{Z}_p[G]}((A_{\ell_i}^p)^G)$ because $c(N_{G_2}) = p$. This completes the proof of Proposition 8.1.

\[\square\]

**Remark 8.3.** Suppose that $n$ is a product of primes in $P$. We define $\eta_{Q(\mu_n p)}$ by

$$\eta_{Q(\mu_n p)} = \theta_{Q(\mu_n p)/Q} - \nu \theta_{Q(\mu_n p)/Q},$$

where $\nu$ is the corestriction map. It is easy to see that $\eta_{Q(\mu_n p)} \in \mathbb{Z}_p[\text{Gal}(Q(\mu_n p)/Q)]$. For any field $F$ with conductor $n p$, we define $\eta_F$ by the image of $\eta_{Q(\mu_n p)}$. Let $\Theta(L) \subset \mathbb{Z}_p[\text{Gal}(L/Q)]$ 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 $\mathbb{Z}_p[\text{Gal}(L/Q)]^-$. We can check that $\Theta(L)$ of $L = L(\ell_1, \ell_2)$ is generated by four elements, to wit, $\eta_L, \nu \eta_{L(\ell_i)}$ with $i = 1, 2$, and $\nu \eta_{Q(\mu_n p)/Q}$ with suitable corestriction maps $\nu$. By the main theorem in [9] (or Theorem 0.6 in [7]) we have

$$\text{Fitt}_{\mathbb{Z}_p[\text{Gal}(L/Q)]^-}(A_L^p) = \Theta(L).$$

We have seen in Proposition 8.1 that

$$\text{Fitt}_{\mathbb{Z}_p[\text{Gal}(L/Q)]^-}((A_L^p)^-) \neq \Theta(L)$$

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 $\sigma$ of $\text{Gal}(F(7)/\mathbb{Q})$ and $\tau \in \text{Gal}(F(127)/\mathbb{Q})$ 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

$$Z_p[G] = Z_p[S, T]/((1 + S)^3 - 1, (1 + T)^3 - 1)$$

where $G$ is as in Proposition 8.1. (Note: the above $T$ has no relation with $T$ in the previous sections.) Let $\eta_L$ be as in Remark 8.3. We regard $\eta_L$ as an element of $Z_p[\text{Gal}(L/\mathbb{Q})]^{-} = Z_p[G]$. 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 $A_{\mathbb{Q}(\mu_7)} = 0$. Then we can compute numerically the Stickelberger ideal $\Theta(L)$ of $L$. The result is

$$\Theta(L) = (3, S^2T, T^2) \subset Z_p[G].$$

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

$$A_L \simeq Z_p[G]/\Theta(L) = Z_p[G]/(3, S^2T, T^2) = F_p[S, T]/(S^3, S^2T, T^2).$$

(6)

In particular, as an abelian group, we have $A_L \simeq (\mathbb{Z}/p\mathbb{Z})^{\oplus 5}$. 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 $\ell_1, \ell_2$ 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

$$\text{Fitt}_{Z_p[G]}(A_L^\vee) = (9, 3T, 3S, S^2T, T^2).$$

(7)

It follows from (6) and (7) that

$$\text{Fitt}_{Z_p[G]}(A_L^\vee) \subset \text{Fitt}_{Z_p[G]}(A_L) = (3, S^2T, T^2).$$

By (7) we also see

$$\eta_L \in \text{Fitt}_{Z_p[G]}(A_L^\vee),$$

but

$$\nu\eta_{L(7)} \notin \text{Fitt}_{Z_p[G]}(A_L^\vee)$$

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


Institut für Theoretische Informatik und Mathematik, Universität der Bundeswehr, München, 85577 Neubiberg, Germany

E-mail address: cornelius.greither@unibw.de

Department of Mathematics, Faculty of Science and Technology, Keio University, 3-14-1 Hiyoshi, Kohoku-ku, Yokohama, 223-8522, Japan

E-mail address: kurihara@math.keio.ac.jp