On the Structure of Ideal Class Groups of CM-Fields

dedicated to Professor K. Kato on his 50th birthday

Masato Kurihara

Received: November 30, 2002
Revised: June 30, 2003

Abstract. For a CM-field K which is abelian over a totally real number field k and a prime number p, we show that the structure of the χ-component A_K^χ of the p-component of the class group of K is determined by Stickelberger elements (zeta values) (of fields containing K) for an odd character χ of $\mathrm{Gal}(K/k)$ satisfying certain conditions. This is a generalization of a theorem of Kolyvagin and Rubin. We define higher Stickelberger ideals using Stickelberger elements, and show that they are equal to the higher Fitting ideals. We also construct and study an Euler system of Gauss sum type for such fields. In the appendix, we determine the initial Fitting ideal of the non-Teichmüller component of the ideal class group of the cyclotomic $\mathbf{Z}_p$-extension of a general CM-field which is abelian over k.

0 Introduction

It is well-known that the cyclotomic units give a typical example of Euler systems. Euler systems of this type were systematically investigated by Kato [8], Perrin-Riou [14], and in the book by Rubin [18]. In this paper, we propose to study Euler systems of Gauss sum type which are not Euler systems in the sense of [18]. We construct an Euler system in the multiplicative groups of CM-fields, which is a generalization of the Euler system of Gauss sums, and generalize a structure theorem of Kolyvagin and Rubin for the minus class groups of imaginary abelian fields to general CM-fields.

The aim of this paper is to prove the structure theorem (Theorem 0.1 below), and we do not pursue general results on the Euler systems of Gauss sum type in this paper. One of very deep and remarkable works of Kato is his construction of the Euler system (which lies in $H^1(T)$) for a $\mathbf{Z}_p$-representation T associated to a modular form. We remark that we do not have an Euler system of Gauss sum type in $H^1(T)$, but fixing $n > 0$ we can find an Euler system of Gauss sum type in $H^1(T/p^n)$, which will be studied in our forthcoming paper.

We will describe our main result. Let k be a totally real number field, and K be a CM-field containing k such that K/k is finite and abelian. We consider an odd prime number p and the p-primary component $A_K = Cl_K \otimes \mathbf{Z}_p$ of the ideal class group of K. Suppose that p does not divide $[K : k]$. Then, A_K is decomposed into $A_K = \bigoplus_\chi A_K^\chi$ where A_K^χ is the χ-component which is an O_χ-module (where $O_\chi = \mathbf{Z}_p[\operatorname{Image}\chi]$, for the precise definition, see 1.1), and χ ranges over $\mathbf{Q}_p$-conjugacy classes of $\overline{\mathbf{Q}_p}^\times$-valued characters of $\operatorname{Gal}(K/k)$ (see also 1.1).

For $k = \mathbf{Q}$ and $K = \mathbf{Q}(\mu_p)$ (the cyclotomic field of p-th roots of unity), Rubin in [17] described the detail of Kolyvagin's method ([10] Theorem 7), and determined the structure of $A^\chi_{\mathbf{Q}(\mu_p)}$ as a $\mathbf{Z}_p$-module for an odd χ, by using the Euler system of Gauss sums (Rubin [17] Theorem 4.4). We generalize this result to arbitrary CM-fields.

In our previous paper [11], we proposed a new definition of the Stickelberger ideal. In this paper, for certain CM-fields, we define higher Stickelberger ideals which correspond to higher Fitting ideals. In §3, using the Stickelberger elements of fields containing K, we define the higher Stickelberger ideals $\Theta_{i,K} \subset \mathbf{Z}_p[\operatorname{Gal}(K/k)]$ for $i \geq 0$ (cf. 3.2). Our definition is different from Rubin's. (Rubin defined the higher Stickelberger ideal using the argument of Euler systems. We do not use the argument of Euler systems to define our $\Theta_{i,K}$.) We remark that our $\Theta_{i,K}$ is numerically computable, since the Stickelberger elements are numerically computable. We consider the χ-component $\Theta^\chi_{i,K}$.

We study the structure of the χ-component A_K^χ as an O_χ-module. We note that p is a prime element of O_χ because the order of $\operatorname{Image}\chi$ is prime to p.

Theorem 0.1. *We assume that the Iwasawa μ-invariant of K is zero (cf. Proposition 2.1), and χ is an odd character of* $\operatorname{Gal}(K/k)$ *such that $\chi \neq \omega$ (where ω is the Teichmüller character giving the action on μ_p), and that $\chi(\mathfrak{p}) \neq 1$ for every prime $\mathfrak{p}$ of k above p. Suppose that*

$$A_K^\chi \simeq O_\chi/(p^{n_1}) \oplus ... \oplus O_\chi/(p^{n_r})$$

with $0 < n_1 \leq ... \leq n_r$. Then, for any i with $0 \leq i < r$, we have

$$(p^{n_1+...+n_{r-i}}) = \Theta^\chi_{i,K}$$

and $\Theta^\chi_{i,K} = (1)$ for $i \geq r$. Namely,

$$A_K^\chi \simeq \bigoplus_{i \geq 1} \Theta^\chi_{i,K}/\Theta^\chi_{i-1,K}.$$

In the case $K = \mathbf{Q}(\mu_p)$ and $k = \mathbf{Q}$, Theorem 0.1 is equivalent to Theorem 4.4 in Rubin [17].

This theorem says that the structure of A_K^χ as an O_χ-module is determined by the Stickelberger elements. Since the Stickelberger elements are defined from the partial zeta functions, we may view our theorem as a manifestation of a very general phenomena in number theory that zeta functions give us information on various important arithmetic objects.

In general, for a commutative ring R and an R-module M such that

$$R^m \xrightarrow{f} R^r \longrightarrow M \longrightarrow 0$$

is an exact sequence of R-modules, the i-th Fitting ideal of M is defined to be the ideal of R generated by all $(r-i)\times(r-i)$ minors of the matrix corresponding to f for i with $0 \leq i < r$. If $i \geq r$, it is defined to be R. (For more details, see Northcott [13]). Using this terminology, Theorem 0.1 can be simply stated as

$$\mathrm{Fitt}_{i,O_\chi}(A_K^\chi) = \Theta_{i,K}^\chi$$

for all $i \geq 0$.

The proof of Theorem 0.1 is divided into two parts. We first prove the inclusion $\mathrm{Fitt}_{i,O_\chi}(A_K^\chi) \supset \Theta_{i,K}^\chi$. To do this, we need to consider a general CM-field which contains K. Suppose that F is a CM-field containing K such that F/k is abelian, and F/K is a p-extension. Put $R_F = \mathbf{Z}_p[\mathrm{Gal}(F/k)]$. For a character χ satisfying the conditions in Theorem 0.1, we consider $R_F^\chi = O_\chi[\mathrm{Gal}(F/K)]$ and $A_F^\chi = A_F \otimes_{R_F} R_F^\chi$ where $\mathrm{Gal}(K/k)$ acts on O_χ via χ. For the χ-component $\theta_F^\chi \in R_F^\chi$ of the Stickelberger element of F (cf. 1.2), we do not know whether $\theta_F^\chi \in \mathrm{Fitt}_{0,R_F^\chi}(A_F^\chi)$ always holds or not (cf. Popescu [15] for function fields). But we will show in Corollary 2.4 that the dual version of this statement holds, namely

$$\iota(\theta_F^\chi) \in \mathrm{Fitt}_{0,R_F^{\chi^{-1}}}((A_F^\chi)^\vee)$$

where $\iota : R_F \longrightarrow R_F$ is the map induced by $\sigma \mapsto \sigma^{-1}$ for $\sigma \in \mathrm{Gal}(F/k)$, and $(A_F^\chi)^\vee$ is the Pontrjagin dual of A_F^χ. We can also determine the right hand side $\mathrm{Fitt}_{0,R_F^{\chi^{-1}}}((A_F^\chi)^\vee)$. In the Appendix, for the cyclotomic $\mathbf{Z}_p$-extension F_∞/F, we determine the initial Fitting ideal of (the Pontrjagin dual of) the non-ω component of the p-primary component of the ideal class group of F_∞ as a $\Lambda_F = \mathbf{Z}_p[[\mathrm{Gal}(F_\infty/k)]]$-module (we determine $\mathrm{Fitt}_{0,\Lambda_F}((A_{F_\infty})^\vee)$ except ω-component, see Theorem A.5). But for the proof of Theorem 0.1, we only need Corollary 2.4 which can be proved more simply than Theorem A.5, so we postpone Theorem A.5 and its proof until the Appendix. Concerning the Iwasawa module $X_{F_\infty} = \varprojlim A_{F_n}$ where F_n is the n-th layer of F_∞/F, we computed in [11] the initial Fitting ideal under certain hypotheses, for example, if $F/\mathbf{Q}$ is abelian. Greither in his recent paper [4] computed the initial Fitting ideal of X_{F_∞} more generally.
In our previous paper [11] §8, we showed that information on the initial Fitting ideal of the class group of F yields information on the higher Fitting ideals of

the class group of K. Using this method, we will show $\mathrm{Fitt}_{i,O_\chi}(A_K^\chi) \supset \Theta_{i,K}^\chi$ in Proposition 3.2.

In order to prove the other inclusion, we will use the argument of Euler systems. By Corollary 2.4 which was mentioned above, we obtain

$$\theta_F^\chi A_F^\chi = 0.$$

(We remark that this has been obtained recently also in Greither [4] Corollary 2.7.) Using this property, we show that for any finite prime ρ of F there is an element $g_{F,\rho}^\chi \in (F^\times \otimes \mathbf{Z}_p)^\chi$ such that $\mathrm{div}(g_{F,\rho}^\chi) = \theta_F^\chi[\rho]^\chi$ in the divisor group where $[\rho]$ is the divisor corresponding to ρ (for the precise relation, see §4). These $g_{F,\rho}^\chi$'s become an Euler system of Gauss sum type (see §4). For the Euler system of Gauss sums, a crucial property is Theorem 2.4 in Rubin [18] which is a property on the image in finite fields, and which was proved by Kolyvagin, based on the explicit form of Gauss sums. But we do not know the explicit form of our $g_{F,\rho}^\chi$, so we prove, by a completely different method, the corresponding property (Proposition 4.7) which is a key proposition in §4.

It is possible to generalize Theorem 0.1 to characters of order divisible by p satisfying some conditions. We hope to come back to this point in our forthcoming paper.

I would like to express my sincere gratitude to K. Kato for introducing me to the world of arithmetic when I was a student in the 1980's. It is my great pleasure to dedicate this paper to Kato on the occasion of his 50th birthday. I would like to thank C. Popescu heartily for a valuable discussion on Euler systems. I obtained the idea of studying the elements $g_{F,\rho}^\chi$ from him. I would also like to thank the referee for his careful reading of this manuscript, and for his pointing out an error in the first version of this paper. I heartily thank C. Greither for sending me his recent preprint [4].

Notation

Throughout this paper, p denotes a fixed odd prime number. We denote by $\mathrm{ord}_p : \mathbf{Q}^\times \longrightarrow \mathbf{Z}$ the normalized discrete valuation at p. For a positive integer n, μ_n denotes the group of all n-th roots of unity. For a number field F, O_F denotes the ring of integers. For a group G and a G-module M, M^G denotes the G-invariant part of M (the maximal subgroup of M on which G acts trivially), and M_G denotes the G-coinvariant of M (the maximal quotient of M on which G acts trivially). For a commutative ring R, $R^\times$ denotes the unit group.

1 Preliminaries

1.1. Let $\mathcal{G}$ be a profinite abelian group such that $\mathcal{G} = \Delta \times \mathcal{G}'$ where $\#\Delta$ is finite and prime to p, and $\mathcal{G}'$ is a pro-p group. We consider the completed group ring $\mathbf{Z}_p[[\mathcal{G}]]$ which is decomposed into

$$\mathbf{Z}_p[[\mathcal{G}]] = \mathbf{Z}_p[\Delta][[\mathcal{G}']] \simeq \bigoplus_{\chi} O_\chi[[\mathcal{G}']]$$

where χ ranges over all representatives of $\mathbf{Q}_p$-conjugacy classes of characters of Δ (a $\overline{\mathbf{Q}_p}^\times$-valued character χ is said to be $\mathbf{Q}_p$-conjugate to χ' if $\sigma\chi = \chi'$ for some $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}_p}/\mathbf{Q}_p)$), and O_χ is $\mathbf{Z}_p[\mathrm{Image}\,\chi]$ as a $\mathbf{Z}_p$-module, and Δ acts on it via χ ($\sigma x = \chi(\sigma)x$ for $\sigma \in \Delta$ and $x \in O_\chi$). Hence, any $\mathbf{Z}_p[[\mathcal{G}]]$-module M is decomposed into $M \simeq \bigoplus_\chi M^\chi$ where

$$M^\chi \simeq M \otimes_{\mathbf{Z}_p[\Delta]} O_\chi \simeq M \otimes_{\mathbf{Z}_p[[\mathcal{G}]]} O_\chi[[\mathcal{G}']].$$

In particular, M^χ is an $O_\chi[[\mathcal{G}']]$-module. For an element x of M, the χ-component of x is denoted by $x^\chi \in M^\chi$.
Let 1_Δ be the trivial character $\sigma \mapsto 1$ of Δ. We denote by M^1 the trivial character component, and define M^* to be the component obtained from M by removing M^1, namely

$$M = M^1 \oplus M^*.$$

Suppose further that $\mathcal{G}' = G \times \mathcal{G}''$ where G is a finite p-group. Let ψ be a character of G. We regard $\chi\psi$ as a character of $\mathcal{G}_0 = \Delta \times G$, and define $M^{\chi\psi}$ by $M^{\chi\psi} = M \otimes_{\mathbf{Z}_p[\mathcal{G}_0]} O_{\chi\psi}$ where $O_{\chi\psi}$ is $O_{\chi\psi} = \mathbf{Z}_p[\mathrm{Image}\,\chi\psi]$ on which $\mathcal{G}_0$ acts via $\chi\psi$. By definition, if $\chi \neq 1_\Delta$, we have $M^{\chi\psi} \simeq (M^*)^{\chi\psi}$.

Let k be a totally real number field and F be a CM-field such that F/k is finite and abelian, and $\mu_p \subset F$. We denote by F_∞/F the cyclotomic $\mathbf{Z}_p$-extension, and put $\mathcal{G} = \mathrm{Gal}(F_\infty/k)$. We write $\mathcal{G} = \Delta \times \mathcal{G}'$ as above. A $\mathbf{Z}_p[[\mathcal{G}]]$-module M is decomposed into $M = M^+ \oplus M^-$ with respect to the action of the complex conjugation where $M^\pm$ is the $\pm$-eigenspace. By definition, $M^- = \bigoplus_{\chi:\mathrm{odd}} M^\chi$ where χ ranges over all odd characters of Δ. We consider the Teichmüller character ω giving the action of Δ on μ_p, and define $M^\sim$ to be the component obtained from M^- by removing M^ω, namely

$$M^- = M^\sim \oplus M^\omega.$$

For an element x of M, we write $x^\sim$ the component of x in $M^\sim$.

1.2. Let k, F, F_∞ be as in 1.1, and S be a finite set of finite primes of k containing all the primes which ramify in F/k. We define in the usual way the partial zeta function for $\sigma \in \mathrm{Gal}(F/k)$ by

$$\zeta_S(s, \sigma) = \sum_{\substack{(\mathfrak{a}, F/k) = \sigma \\ \mathfrak{a} \text{ is prime to } S}} N(\mathfrak{a})^{-s}$$

for $\mathrm{Re}(s) > 1$ where $N(\mathfrak{a})$ is the norm of $\mathfrak{a}$, and $\mathfrak{a}$ runs over all integral ideals of k, coprime to the primes in S such that the Artin symbol $(\mathfrak{a}, F/k)$ is equal to σ. The partial zeta functions are meromorphically continued to the whole complex plane, and holomorphic everywhere except for $s = 1$. We define

$$\theta_{F,S} = \sum_{\sigma \in \mathrm{Gal}(F/k)} \zeta_S(0, \sigma)\sigma^{-1}$$

which is an element of $\mathbf{Q}[\mathrm{Gal}(F/k)]$ (cf. Siegel [21]). Suppose that S_F is the set of ramifying primes of k in F/k. We simply write θ_F for θ_{F,S_F}. We know by Deligne and Ribet the non ω-component $(\theta_{F,S})^{\sim} \in \mathbf{Q}_p[\mathrm{Gal}(F/k)]^{\sim}$ is in $\mathbf{Z}_p[\mathrm{Gal}(F/k)]^{\sim}$. In particular, for a character χ of Δ with $\chi \neq \omega$, we have $(\theta_{F,S})^{\chi} \in \mathbf{Z}_p[\mathrm{Gal}(F/k)]^{\chi}$.
Suppose that S contains all primes above p. Let F_n denote the n-th layer of the cyclotomic $\mathbf{Z}_p$-extension F_∞/F, and consider $(\theta_{F_n,S})^{\sim} \in \mathbf{Z}_p[\mathrm{Gal}(F_n/k)]^{\sim}$. These $\theta^{\sim}_{F_n,S}$'s become a projective system with respect to the canonical restriction maps, and we define

$$\theta^{\sim}_{F_\infty,S} \in \mathbf{Z}_p[[\mathrm{Gal}(F_\infty/k)]]^{\sim}$$

to be their projective limit. This is essentially (the non ω-part of) the p-adic L-function of Deligne and Ribet [1].

2 Initial Fitting ideals

Let k, F, F_∞ be as in §1. We denote by k_∞/k the cyclotomic $\mathbf{Z}_p$-extension, and assume that $F \cap k_\infty = k$. Our aim in this section is to prove Proposition 2.1 and Corollary 2.4 below.

2.1. Let S be a finite set of finite primes of k containing ramifying primes in F_∞/k. We denote by F^+ the maximal real subfield of F. Put $\Lambda_F = \mathbf{Z}_p[[\mathrm{Gal}(F_\infty/k)]]$ and $\Lambda_{F^+} = \mathbf{Z}_p[[\mathrm{Gal}(F^+_\infty/k)]]$ which is naturally isomorphic to the plus part Λ_F^+ of Λ_F. We denote by $\mathcal{M}_{\infty,S}$ the maximal abelian pro-p extension of F^+_∞ which is unramified outside S, and by $\mathcal{X}_{F^+_\infty,S}$ the Galois group of $\mathcal{M}_{\infty,S}/F^+_\infty$. We study $\mathcal{X}_{F^+_\infty,S}$ which is a torsion Λ_{F^+}-module.
We consider a ring homomorphism $\tau^{-1}\iota : \Lambda_F \longrightarrow \Lambda_F$ which is defined by $\sigma \mapsto \kappa(\sigma)\sigma^{-1}$ for $\sigma \in \mathrm{Gal}(F_\infty/k)$ where $\kappa : \mathrm{Gal}(F_\infty/k) \longrightarrow \mathbf{Z}_p^\times$ is the cyclotomic character giving the action of $\mathrm{Gal}(F_\infty/k)$ on μ_{p^∞}. Let $(\Lambda_F)^{\sim}$ and $(\Lambda_F^+)^* = (\Lambda_{F^+})^*$ be as in §1.1. Then, $\tau^{-1}\iota$ induces

$$\tau^{-1}\iota : (\Lambda_F)^{\sim} \longrightarrow (\Lambda_{F^+})^*.$$

Let $\theta^{\sim}_{F_\infty,S} \in (\Lambda_F)^{\sim}$ be the Stickelberger element defined in 1.2.

Proposition 2.1. *Assume that the the Iwasawa μ-invariant of F is zero, namely $\mathcal{X}_{F^+_\infty,S}$ is a finitely generated $\mathbf{Z}_p$-module. Then,* $\mathrm{Fitt}_{0,\Lambda_{F^+}}((\mathcal{X}_{F^+_\infty,S})^*)$ *is generated by $\tau^{-1}\iota(\theta^{\sim}_{F_\infty,S})$ except the trivial character component, namely*

$$\mathrm{Fitt}_{0,\Lambda_{F^+}}((\mathcal{X}_{F^+_\infty,S})^*)^* = (\tau^{-1}\iota(\theta^{\sim}_{F_\infty,S})).$$

Proof. We use the method in [11]. In fact, the proof of this proposition is much easier than that of Theorem 0.9 in [11].

We decompose $\mathcal{G} = \mathrm{Gal}(F_\infty/k)$ as in 1.1 ($\mathcal{G} = \Delta \times \mathcal{G}'$). Suppose that $\mathbf{c}$ is the complex conjugation in Δ and put $\Delta^+ = \Delta/ < \mathbf{c} >$, and $\mathcal{G}_0 = \mathrm{Gal}(F^+/k)$. Then, we can write $\mathcal{G}_0 = \Delta^+ \times G$ where G is a p-group. For a character χ of Δ^+ with $\chi \neq 1_{\Delta^+}$, and a character ψ of G, we regard $\chi\psi$ as a character of $\mathcal{G}_0$. We consider $(\mathcal{X}_{F^+_\infty,S})^{\chi\psi}$ which is an $O_{\chi\psi}[[\mathrm{Gal}(F_\infty/F)]]$-module (cf. 1.1). Our assumption of the vanishing of the μ-invariant implies that $(\mathcal{X}_{F^+_\infty,S})^{\chi\psi}$ is a finitely generated $O_{\chi\psi}$-module. We will first show that $(\mathcal{X}_{F^+_\infty,S})^{\chi\psi}$ is a free $O_{\chi\psi}$-module.

Let $H \subset G$ be the kernel of ψ, and M be the subfield of F corresponding to H, namely $\mathrm{Gal}(F/M) = H$. We denote by M_∞ the cyclotomic $\mathbf{Z}_p$-extension of M and regard H as the Galois group of F_∞/M_∞. We will see that the H-coinvariant $((\mathcal{X}_{F^+_\infty,S})^\chi)_H$ is naturally isomorphic to $(\mathcal{X}_{M^+_\infty,S})^\chi$. In fact, by taking the dual, it is enough to show that the natural map $H^1_{et}(O_{M^+_\infty}[1/S], \mathbf{Q}_p/\mathbf{Z}_p)^{\chi^{-1}} \longrightarrow (H^1_{et}(O_{F^+_\infty}[1/S], \mathbf{Q}_p/\mathbf{Z}_p)^{\chi^{-1}})^H$ of etale cohomology groups is bijective where $O_{M^+_\infty}[1/S]$ (resp. $O_{F^+_\infty}[1/S]$) is the ring of S-integers in M^+_∞ (resp. F^+_∞). This follows from the Hochschild-Serre spectral sequence and $H^1(H, \mathbf{Q}_p/\mathbf{Z}_p)^{\chi^{-1}} = H^2(H, \mathbf{Q}_p/\mathbf{Z}_p)^{\chi^{-1}} = 0$. Hence, regarding $\chi\psi$ as a character of $\mathrm{Gal}(M^+/k)$, we have

$$(\mathcal{X}_{F^+_\infty,S})^{\chi\psi} = (\mathcal{X}_{M^+_\infty,S})^{\chi\psi}.$$

We note that $(\mathcal{X}_{M^+_\infty,S})^\chi$ does not have a nontrivial finite $O_\chi[[\mathcal{G}']]$-submodule (Theorem 18 in Iwasawa [5]), so is free over O_χ by our assumption of the μ-invariant. We will use the same method as Lemma 5.5 in [11] to prove that $(\mathcal{X}_{M^+_\infty,S})^{\chi\psi}$ is free over $O_{\chi\psi}$. We may assume $\psi \neq 1_G$, so p divides the order of $\mathrm{Gal}(M^+/k)$. Let C be the subgroup of $\mathrm{Gal}(M^+/k)$ of order p, M' the subfield such that $\mathrm{Gal}(M^+/M') = C$, and put $N_C = \Sigma_{\sigma\in C}\sigma$. We have an isomorphism $(\mathcal{X}_{M^+_\infty,S})^{\chi\psi} \simeq (\mathcal{X}_{M^+_\infty,S})^\chi/(N_C)$. Let σ_0 be a generator of C. In order to prove that $(\mathcal{X}_{M^+_\infty,S})^{\chi\psi}$ is free over $O_{\chi\psi}$, it is enough to show that the map

$$\sigma_0 - 1 : (\mathcal{X}_{M^+_\infty,S})^\chi/(N_C) \longrightarrow (\mathcal{X}_{M^+_\infty,S})^\chi$$

is injective. Hence, it suffices to show $((\mathcal{X}_{M^+_\infty,S})^\chi)^C = N_C((\mathcal{X}_{M^+_\infty,S})^\chi)$, hence to show $\hat{H}^0(C, (\mathcal{X}_{M^+_\infty,S})^\chi) = 0$. Taking the dual, it is enough to show $H^1(C, H^1_{et}(O_{M^+_\infty}[1/S], \mathbf{Q}_p/\mathbf{Z}_p)^{\chi^{-1}}) = 0$. This follows from the Hochschild-Serre spectral sequence and $H^2_{et}(O_{M'_\infty}[1/S], \mathbf{Q}_p/\mathbf{Z}_p) = 0$ (which is a famous

property called the weak Leopoldt conjecture and which follows immediately from the vanishing of the p-component of the Brauer group of M'_∞).
Thus, $(\mathcal{X}_{F^+_\infty,S})^{\chi\psi}$ is a free $O_{\chi\psi}$-module of finite rank. This shows that $\mathrm{Fitt}_{0,O_{\chi\psi}[[\mathrm{Gal}(F_\infty/F)]]}((\mathcal{X}_{F^+_\infty,S})^{\chi\psi})$ coincides with its characteristic ideal. By Wiles [25] and our assumption, the μ-invariant of $(\tau^{-1}\iota(\theta^{\sim}_{F_\infty,S}))^{\chi\psi}$ is also zero, and by the main conjecture proved by Wiles [25], we have

$$\mathrm{Fitt}_{0,O_{\chi\psi}[[\mathrm{Gal}(F_\infty/F)]]}((\mathcal{X}_{F^+_\infty,S})^{\chi\psi}) = (\tau^{-1}\iota(\theta^{\sim}_{F_\infty,S})^{\chi\psi}).$$

This holds for any χ and ψ with $\chi \neq 1_\Delta$. Hence, by Corollary 4.2 in [11], we obtain the conclusion of Proposition 2.1.

2.2. For any number field $\mathcal{F}$, we denote by $A_{\mathcal{F}}$ the p-primary component of the ideal class group of $\mathcal{F}$. Let F be as above. We define

$$A_{F_\infty} = \varinjlim A_{F_n}$$

where F_n is the n-th layer of F_∞/F. We denote by $(A_{F_\infty})^\vee$ the Pontrjagin dual of A_{F_∞}. Let S_p be the set of primes of k lying over p. By the orthogonal pairing in P.276 of Iwasawa [5] which is defined by the Kummer pairing, we have an isomorphism

$$(\mathcal{X}_{F^+_{\infty,S_p}})^* \simeq (A^{\sim}_{F_\infty})^\vee(1).$$

Let $\iota : \Lambda_F \longrightarrow \Lambda_F$ be the ring homomorphism induced by $\sigma \mapsto \sigma^{-1}$ for $\sigma \in \mathrm{Gal}(F_\infty/k)$. For a character χ of Δ, ι induces a ring homomorphism $\Lambda_F^\chi \longrightarrow \Lambda_F^{\chi^{-1}}$ which we also denote by ι. Since there is a natural surjective homomorphism $(\mathcal{X}_{F^+_{\infty,S}})^* \longrightarrow (\mathcal{X}_{F^+_{\infty,S_p}})^*$, Proposition 2.1 together with the above isomorphism implies

Corollary 2.2. *Let χ be an odd character of Δ such that $\chi \neq \omega$. Under the assumption of Proposition 2.1, we have*

$$\iota(\theta^\chi_{F_\infty,S}) \in \mathrm{Fitt}_{0,\Lambda_F^{\chi^{-1}}}((A^\chi_{F_\infty})^\vee).$$

Next, we consider a general CM-field F such that F/k is finite and abelian (Here, we do not assume $\mu_p \subset F$). Put $R_F = \mathbf{Z}_p[\mathrm{Gal}(F/k)]$. Let G be the p-primary component of $\mathrm{Gal}(F/k)$, and $\mathrm{Gal}(F/k) = \Delta \times G$. Suppose that χ is an odd character of Δ with $\chi \neq \omega$. We consider $R_F^\chi = O_\chi[G]$, and define $\iota : R_F \longrightarrow R_F$ and $\iota : R_F^\chi \longrightarrow R_F^{\chi^{-1}}$ similarly as above. If we assume that the Iwasawa μ-invariant of F vanishes, $(\mathcal{X}_{F(\mu_p)_\infty,S})^{\chi^{-1}\omega}$ is a finitely generated O_χ-module, so we can apply the proof of Proposition 2.1 to get $\iota(\theta^\chi_{F_\infty,S}) \in \mathrm{Fitt}_{0,\Lambda_F^{\chi^{-1}}}((A^\chi_{F_\infty})^\vee)$. Since $A_F^- \longrightarrow A^-_{F(\mu_p)_\infty}$ is injective ([24] Prop.13.26), $(A^\chi_{F(\mu_p)_\infty})^\vee \longrightarrow (A^\chi_F)^\vee$ is surjective. The image of $\iota(\theta^\chi_{F_\infty,S}) \in \Lambda_F^{\chi^{-1}}$ in $R_F^{\chi^{-1}}$ is $\iota(\theta^\chi_{F,S})$. Hence, we obtain

COROLLARY 2.3. *Assume that the Iwasawa μ-invariant of F is zero. Then, we have*

$$\iota(\theta^{\chi}_{F,S}) \in \mathrm{Fitt}_{0,R_F^{\chi^{-1}}}((A_F^{\chi})^{\vee}).$$

Let $S_{F(\mu_p)_\infty}$ (resp. S_F) be the set of ramifying primes in $F(\mu_p)_\infty/k$ (resp. F/k). Note that $S_{F(\mu_p)_\infty} \setminus S_F \subset S_p$ and

$$\theta_{F,S_{F(\mu_p)_\infty}} = (\Pi_{\mathfrak{p}\in S_{F(\mu_p)_\infty}\setminus S_F}(1-\varphi_{\mathfrak{p}}^{-1}))\theta_{F,S_F}$$

where $\varphi_{\mathfrak{p}}$ is the Frobenius of $\mathfrak{p}$ in $\mathrm{Gal}(F/k)$. If $\chi(\mathfrak{p}) \neq 1$ for all $\mathfrak{p}$ above p, $(1-\varphi_{\mathfrak{p}}^{-1})^{\chi}$ is a unit of $R_F^{\chi^{-1}}$ because the order of χ is prime to p. Therefore, we get

COROLLARY 2.4. *Assume that the Iwasawa μ-invariant of F is zero, and that $\chi(\mathfrak{p}) \neq 1$ for all $\mathfrak{p}$ above p. Then, we have*

$$\iota(\theta^{\chi}_{F}) \in \mathrm{Fitt}_{0,R_F^{\chi^{-1}}}((A_F^{\chi})^{\vee}).$$

3 HIGHER STICKELBERGER IDEALS

In this section, for a finite abelian extension K/k whose degree is prime to p, we will define the ideal $\Theta_{i,K} \subset \mathbf{Z}_p[\mathrm{Gal}(K/k)]$ for $i \geq 0$. We also prove the inclusion $\Theta^{\chi}_{i,K} \subset \mathrm{Fitt}_{i,O_\chi}(A_K^{\chi})$ for K and χ as in Theorem 0.1.

3.1. In this subsection, we assume that O is a discrete valuation ring with maximal ideal (p). We denote by ord_p the normalized discrete valuation of O, so $\mathrm{ord}_p(p) = 1$. For n, $r > 0$, we consider a ring

$$A_{n,r} = O[[S_1, ..., S_r]]/((1+S_1)^{p^n}-1, ..., (1+S_r)^{p^n}-1).$$

Suppose that f is an element of $A_{n,r}$ and write $f = \Sigma_{i_1,...i_r\geq 0} a_{i_1...i_r} S_1^{i_1}...S_r^{i_r}$ mod $\mathcal{I}$ where $\mathcal{I} = ((1+S_1)^{p^n}-1, ..., (1+S_r)^{p^n}-1)$. For positive integers i and s, we set $s' = \min\{x \in \mathbf{Z} : s < p^x\}$. Assume $s' \leq n$. If $0 < j < p^{s'}$, we have $\mathrm{ord}_p(\binom{p^n}{j}) = \mathrm{ord}_p(p^n!/(j!(p^n-j)!)) \geq n - s' + 1$. Hence, for $i_1, ..., i_r \leq s < p^{s'}$, $a_{i_1,...,i_r}$ mod $p^{n-s'+1}$ is well-defined from $f \in A_{n,r}$. For positive integers i and s with $s' \leq n$, we define $I_{i,s}(f)$ to be the ideal of O which is generated by $p^{n-s'+1}$ and

$$\{a_{i_1,...,i_r} \ : \ 0 \leq i_1, ..., i_r \leq s \ \text{ and } \ i_1 + ... + i_r \leq i\}.$$

Since $a_{i_1,...,i_r}$ is well-defined mod $p^{n-s'+1}$, $I_{i,s}(f) \subset O$ is well-defined for any i and $s \in \mathbf{Z}_{>0}$ such that $n \geq s'$.

Lemma 3.1. *Let* $\alpha : A_{n,r} \longrightarrow A_{n,r}$ *be the homomorphism of* O*-algebras defined by* $\alpha(S_k) = \Pi_{j=1}^{r}(1+S_j)^{a_{kj}} - 1$ *for* $1 \leq k,\, j \leq r$ *such that* $(a_{kj}) \in GL_n(\mathbf{Z}/p^n\mathbf{Z})$. *Then, we have*

$$I_{i,s}(\alpha(f)) = I_{i,s}(f).$$

Proof. It is enough to show $I_{i,s}(f) \subset I_{i,s}(\alpha(f))$ because if we obtain this inclusion, the other inclusion is also obtained by applying it to α^{-1}. Further, since (a_{kj}) is a product of elementary matrices, it suffices to show the inclusion in the case that α corresponds to an elementary matrix, in which case, the inclusion can be easily checked.

In particular, let $\iota : A_{n,r} \longrightarrow A_{n,r}$ be the ring homomorphism defined by $\iota(S_k) = (1 + S_k)^{-1} - 1$ for $k = 1, ..., r$. Then, we have

$$I_{i,s}(\iota(f)) = I_{i,s}(f)$$

which we will use later.

3.2. Suppose that k is totally real, K is a CM-field, and K/k is abelian such that p does not divide $[K : k]$. Put $\Delta = \mathrm{Gal}(K/k)$. For $i \geq 0$, we will define the higher Stickelberger ideal $\Theta_{i,K} \subset \mathbf{Z}_p[\Delta]$. Since $\mathbf{Z}_p[\Delta] \simeq \bigoplus_\chi O_\chi$, it is enough to define $(\Theta_{i,K})^\chi$. We replace K by the subfield corresponding to the kernel of χ, and suppose the conductor of K/k is equal to that of χ.

For $n,\, r > 0$, let $\mathcal{S}_{K,n,r}$ denote the set of CM fields F such that $K \subset F$, F/k is abelian, and F/K is a p-extension satisfying $\mathrm{Gal}(F/K) \simeq (\mathbf{Z}/p^n)^{\oplus r}$. For $F \in \mathcal{S}_{K,n,r}$, we have an isomorphism

$$\mathbf{Z}_p[\mathrm{Gal}(F/k)]^\chi \simeq \mathbf{Z}_p[\Delta]^\chi[\mathrm{Gal}(F/K)] = O_\chi[\mathrm{Gal}(F/K)].$$

Fixing generators of $\mathrm{Gal}(F/K)$, we have an isomorphism between $O_\chi[\mathrm{Gal}(F/K)]$ and $A_{n,r}$ with $O = O_\chi$ in 3.1 (the fixed generators σ_1,...,σ_r correspond to $1 + S_1$,...,$1 + S_r$).

We first assume χ is odd and $\chi \neq \omega$. Then, θ_F^χ is in $\mathbf{Z}_p[\mathrm{Gal}(F/k)]^\chi = O_\chi[\mathrm{Gal}(F/K)]$ (cf. 1.2). Using the isomorphism between $O_\chi[\mathrm{Gal}(F/K)]$ and $A_{n,r}$, for i and s such that $n \geq s'$, we define the ideal $I_{i,s}(\theta_F^\chi)$ of O_χ (cf. 3.1). By Lemma 3.1, $I_{i,s}(\theta_F^\chi)$ does not depend on the choice of generators of $\mathrm{Gal}(F/K)$.

We define $(\Theta_{0,K})^\chi = (\theta_K^\chi)$. Suppose that $(\Theta_{0,K})^\chi = (p^m)$. If $m = 0$, we define $(\Theta_{i,K})^\chi = (1)$ for all $i \geq 0$. We assume $m > 0$. We define $\mathcal{S}_{K,n} = \bigcup_{r>0} \mathcal{S}_{K,n,r}$. We define $(\Theta_{i,s,K})^\chi$ to be the ideal generated by all $I_{i,s}(\theta_F^\chi)$'s where F ranges over all fields in $\mathcal{S}_{K,n}$ for all $n \geq m + s' - 1$ where $s' = \min\{x \in \mathbf{Z} : s < p^x\}$ as in 3.1, namely

$$(\Theta_{i,s,K})^\chi = \bigcup_{\substack{F \in \mathcal{S}_{K,n} \\ n \geq m+s'-1}} I_{i,s}(\theta_F^\chi).$$

We define $(\Theta_{i,K})^\chi$ by $(\Theta_{i,K})^\chi = \bigcup_{s>0} (\Theta_{i,s,K})^\chi$. For χ satisfying the condition of Theorem 0.1, we will see later in §5 that $(\Theta_{i,K})^\chi = (\Theta_{i,1,K})^\chi$.

For $F \in \mathcal{S}_{K,m}$ with $m > 0$, $I_{i,1}(\theta_F^\chi)$ contains p^m (note that $s' = 1$ when $s = 1$), so $p^m \in (\Theta_{i,K})^\chi$. Since $(\Theta_{0,K})^\chi = (p^m)$, $(\Theta_{0,K})^\chi$ is in $(\Theta_{i,K})^\chi$. It is also clear from definition that $(\Theta_{i,s,K})^\chi \subset (\Theta_{i+1,s,K})^\chi$ for $i > 0$ and $s > 0$. Hence, we have a sequence of ideals

$$(\Theta_{0,K})^\chi \subset (\Theta_{1,K})^\chi \subset (\Theta_{2,K})^\chi \subset ...$$

We do not use the ω-component in this paper, but for $\chi = \omega$, we define $(\Theta_{0,K})^\chi = (\theta_K \operatorname{Ann}_{\mathbf{Z}_p[\mathrm{Gal}(K/k)]}(\mu_{p^\infty}(K)))^\chi$. For $i > 0$, $(\Theta_{i,K})^\chi$ is defined similarly as above by using $x\theta_F^\chi$ instead of θ_F^χ where x ranges over elements of $\operatorname{Ann}_{\mathbf{Z}_p[\mathrm{Gal}(F/k)]}(\mu_{p^\infty}(F))^\chi$. For an even χ, we define $(\Theta_{i,K})^\chi = (0)$ for all $i \geq 0$.

Proposition 3.2. *Suppose that K and χ be as in Theorem 0.1. Then, for any $i \geq 0$, we have*

$$(\Theta_{i,K})^\chi \subset \operatorname{Fitt}_{i,O_\chi}(A_K^\chi).$$

Proof. At first, by Theorem 3 in Wiles [26] we know $\# A_K^\chi = \#(O_\chi/(\theta_K^\chi))$, hence $(\Theta_{0,K})^\chi = \operatorname{Fitt}_{0,O_\chi}(A_K^\chi)$. (In our case, this is a direct consequence of the main conjecture proved by Wiles [25].) We assume $i > 0$. By the definition of $(\Theta_{i,K})^\chi$, we have to show $I_{i,s}(\theta_F^\chi) \subset \operatorname{Fitt}_{i,O_\chi}(A_K^\chi)$ for $F \in \mathcal{S}_{K,n,r}$ where the notation is the same as above. By Lemma 3.1, $I_{i,s}(\theta_F^\chi) = I_{i,s}(\iota(\theta_F^\chi))$. Hence, it is enough to show

$$I_{i,s}(\iota(\theta_F^\chi)) \subset \operatorname{Fitt}_{i,O_\chi}(A_K^\chi).$$

We will prove this inclusion by the same method as Theorem 8.1 in [11]. We write $O = O_\chi = O_{\chi^{-1}}$, and $G = \mathrm{Gal}(F/K)$. As in 3.2, we fix an isomorphism $O[\mathrm{Gal}(F/K)] \simeq A_{n,r}$ by fixing generators of G. We consider $(A_F^\chi)^\vee = (A_F \otimes_{\mathbf{Z}_p[\Delta]} O)^\vee = (A_F \otimes_{\mathbf{Z}_p[\mathrm{Gal}(F/k)]} O[G])^\vee$ which is an $O[G]$-module. Since F/K is a p-extension, it is well-known that the vanishing of the Iwasawa μ-invariant of K implies the vanishing of the Iwasawa μ-invariant of F ([6] Theorem 3). By Corollary 2.4, we have

$$\iota(\theta_F^\chi) \in \operatorname{Fitt}_{0,O[G]}((A_F^\chi)^\vee).$$

Since $\chi \neq \omega$ and χ is odd, for a unit group $O_F^\times$, we have $(O_F^\times \otimes \mathbf{Z}_p)^\chi = \mu_{p^\infty}(F)^\chi = 0$, so $H^1(\mathrm{Gal}(F/K), O_F^\times)^\chi = H^1(\mathrm{Gal}(F/K), (O_F^\times \otimes \mathbf{Z}_p)^\chi) = 0$. This shows that the natural map $A_K^\chi \longrightarrow A_F^\chi$ is injective. Hence, regarding A_K^χ as an $O[G]$-module (G acting trivially on it), we have

$$\operatorname{Fitt}_{0,O[G]}((A_F^\chi)^\vee) \subset \operatorname{Fitt}_{0,O[G]}((A_K^\chi)^\vee),$$

and

$$\iota(\theta_F^\chi) \in \operatorname{Fitt}_{0,O[G]}((A_K^\chi)^\vee).$$

Hence, by the lemma below, we obtain

$$I_{i,s}(\iota(\theta_F^\chi)) \subset \mathrm{Fitt}_{i,O}(A_K^\chi).$$

This completes the proof of Proposition 3.2.

Lemma 3.3. *Put* $I_G = (S_1, ..., S_r)$. *Then,* $\mathrm{Fitt}_{0,O[G]}((A_K^\chi)^\vee)$ *is generated by* $\mathrm{Fitt}_{j,O}(A_K^\chi)(I_G)^j$ *for all* $j \geq 0$.

Proof. Put $M = (A_K^\chi)^\vee$. Since O is a discrete valuation ring, $M^\vee$ is isomorphic to M as an O-module. Hence, $\mathrm{Fitt}_{j,O}(M) = \mathrm{Fitt}_{j,O}(M^\vee) = \mathrm{Fitt}_{j,O}(A_K^\chi)$.
We take generators $e_1,...,e_m$ and relations $\Sigma_{k=1}^m a_{kl}e_k = 0$ ($a_{kl} \in O$, $l = 1, 2, ..., m$) of M as an O-module. Put $A = (a_{kl})$. We also consider a relation matrix of M as an $O[G]$-module. By definition, I_G annihilates M. Hence, the relation matrix of M as an $O[G]$-module is of the form

$$\left(\begin{array}{cccccccccc} S_1 & ... & S_r & ... & ... & 0 & ... & 0 & & \\ 0 & ... & 0 & ... & ... & 0 & ... & 0 & & \\ . & ... & . & ... & ... & . & ... & . & & A \\ . & ... & . & ... & ... & . & ... & . & & \\ 0 & ... & 0 & ... & ... & S_1 & ... & S_r & & \end{array}\right).$$

Therefore, $\mathrm{Fitt}_{0,O[G]}(M)$ is generated by $\mathrm{Fitt}_{j,O}(M)(I_G)^j$ for all $j \geq 0$.

4 Euler systems

Let K/k be a finite and abelian extension of degree prime to p. We also assume that K is a CM-field, and the Iwasawa μ-invariant of K is zero. We consider a CM field F such that F/k is finite and abelian, $F \supset K$, and F/K is a p-extension. Since the Iwasawa μ-invariant of F is also zero, by Corollary 2.4, we have $\iota(\theta_F^\sim)(A_F^\sim)^\vee = 0$. Hence, we have

$$\theta_F^\sim A_F^\sim = 0.$$

We denote by $O_F^\times$, Div_F, and A_F the unit group of F, the divisor group of F, and the p-primary component of the ideal class group of F. We write $[\rho]$ for the divisor corresponding to a finite prime ρ, and write an element of Div_F of the form $\Sigma a_i[\rho_i]$ with $a_i \in \mathbf{Z}$. If $(x) = \Pi \rho_i^{a_i}$ is the prime decomposition of $x \in F^\times$, we write $\mathrm{div}(x) = \Sigma a_i[\rho_i] \in \mathrm{Div}_F$. Consider an exact sequence $0 \longrightarrow O_F^\times \otimes \mathbf{Z}_p \longrightarrow F^\times \otimes \mathbf{Z}_p \xrightarrow{\mathrm{div}} \mathrm{Div}_F \otimes \mathbf{Z}_p \longrightarrow A_F \longrightarrow 0$. Since the functor $M \mapsto M^\sim$ is exact and $(O_F^\times \otimes \mathbf{Z}_p)^\sim = 0$,

$$0 \longrightarrow (F^\times \otimes \mathbf{Z}_p)^\sim \xrightarrow{\mathrm{div}} (\mathrm{Div}_F \otimes \mathbf{Z}_p)^\sim \longrightarrow A_F^\sim \longrightarrow 0$$

is exact. For any finite prime ρ_F of F, since the class of $\theta_F^\sim[\rho_F]^\sim$ in $A_F^\sim$ vanishes, there is a unique element g_{F,ρ_F} in $(F^\times \otimes \mathbf{Z}_p)^\sim$ such that

$$\mathrm{div}(g_{F,\rho_F}) = \theta_F^\sim[\rho_F]^\sim.$$

By this property, we have

Lemma 4.1. *Suppose that M is an intermediate field of F/K, and S_F (resp. S_M) denotes the set of ramifying primes of k in F/k (resp. M/k). Let ρ_M be a prime of M, ρ_F be a prime of F above ρ_M, and $f = [O_F/\rho_F : O_F/\rho_M]$. Then, we have*

$$N_{F/M}(g_{F,\rho_F}) = (\prod_{\lambda \in S_F \setminus S_M} (1 - \varphi_\lambda^{-1}))^{\sim}(g_{M,\rho_M})^f$$

where $N_{F/M} : F^\times \longrightarrow M^\times$ is the norm map, and φ_λ is the Frobenius of λ in $\mathrm{Gal}(M/k)$.

Proof. In fact, we have

$$\mathrm{div}(N_{L/M}(g_{F,\rho_F})) = c_{F/M}(\theta_F)^{\sim}[N_{F/M}(\rho_F)]^{\sim}$$

where $c_{F/M} : \mathbf{Z}_p[\mathrm{Gal}(F/k)] \longrightarrow \mathbf{Z}_p[\mathrm{Gal}(M/k)]$ is the map induced by the restriction $\sigma \mapsto \sigma_{|M}$ and $N_{F/M}(\rho_F)$ is the norm of ρ_F. By a famous property of the Stickelberger elements (see Tate [23] p.86), we have

$$c_{F/M}(\theta_F^{\sim}) = ((\prod_{\lambda \in S_F \setminus S_M} (1 - \varphi_\lambda^{-1}))\theta_M)^{\sim},$$

hence the right hand side of the first equation is equal to $((\prod_{\lambda \in S_F \setminus S_M}(1 - \varphi_\lambda^{-1}))\theta_M)^{\sim} f[\rho_M]^{\sim}$. This is also equal to $\mathrm{div}((\prod_{\lambda \in S_F \setminus S_M}(1-\varphi_\lambda^{-1}))^{\sim}(g_{M,\rho_M})^f)$. Since div is injective, we get this lemma.

Remark 4.2. By the property $\theta_F^{\sim} A_F^{\sim} = 0$, we can also obtain an Euler system in some cohomology groups by the method of Rubin in [18] Chapter 3, section 3.4. But here, we consider the Euler system of these g_{F,ρ_F}'s, which is an analogue of the Euler system of Gauss sums. I obtained the idea of studying the elements g_{F,ρ_F} from C. Popescu through a discussion with him.

Let H_k be the Hilbert p-class field of k, namely the maximal abelian p-extension of k which is unramified everywhere. Suppose that the p-primary component A_k of the ideal class group of k is decomposed into $A_k = \mathbf{Z}/p^{a_1}\mathbf{Z} \oplus ... \oplus \mathbf{Z}/p^{a_s}\mathbf{Z}$. We take and fix a prime ideal $\mathfrak{q}_j$ which generates the j-th direct summand for each $j = 1, ..., s$. We take $\xi_j \in k^\times$ such that $\mathfrak{q}_j^{p^{a_j}} = (\xi_j)$ for each j. Let $\mathcal{U}$ denote the subgroup of $k^\times$ generated by the unit group $O_k^\times$ and ξ_1,...,ξ_s. For a positive integer $n > 0$, we define $\mathcal{P}_n$ to be the set of primes of k with degree 1 which are prime to $p\mathfrak{q}_1 \cdot ... \cdot \mathfrak{q}_s$, and which split completely in $KH_k(\mu_{p^n}, \mathcal{U}^{1/p^n})$.

Lemma 4.3. *Suppose $\lambda \in \mathcal{P}_n$. Then, there exists a cyclic extension $k_n(\lambda)/k$ of degree p^n, which is unramified outside λ, and in which λ is totally ramified.*

Proof. We prove this lemma by class field theory. Let $\mathcal{C}_k$ (resp. Cl_k) be the idele class group (resp. the ideal class group) of k. For a prime v, we denote by k_v the completion of k at v, and define U_{k_v} to be the unit group of the ring of integers of k_v for a finite prime v, and $U_{k_v} = k_v$ for an infinite prime v. We denote by $U^1_{k_v}$ the group of principal units for a finite prime v. We define $\mathcal{C}_{k,\lambda,n}$ which is a quotient of $\mathcal{C}_k \otimes \mathbf{Z}_p$ by

$$\mathcal{C}_{k,\lambda,n} = ((k_\lambda^\times/U^1_{k_\lambda}) \otimes \mathbf{Z}/p^n\mathbf{Z} \oplus \bigoplus_{v\neq\lambda}(k_v^\times/U_{k_v}) \otimes \mathbf{Z}_p)/(\text{the image of } k^\times)$$

where v ranges over all primes except λ. Since λ splits in H_k, the class of λ in $Cl_k \otimes \mathbf{Z}_p = A_k$ is trivial. Hence, the natural map

$$\bigoplus_v k_v^\times \otimes \mathbf{Z}_p \longrightarrow \bigoplus_v (k_v^\times/U_{k_v}) \otimes \mathbf{Z}_p \longrightarrow (\bigoplus_v \mathbf{Z}_p)/(\text{the image of } k^\times) = A_k$$

(v ranges over all primes) induces $\mathcal{C}_{k,\lambda,n} \longrightarrow A_k$, and we have an exact sequence

$$(U_{k_\lambda}/U^1_{k_\lambda}) \otimes \mathbf{Z}/p^n\mathbf{Z} \stackrel{a}{\longrightarrow} \mathcal{C}_{k,\lambda,n} \stackrel{b}{\longrightarrow} A_k \longrightarrow 0.$$

Let $\kappa(\lambda)$ denote the residue field of λ. Since λ splits in $k(\mu_{p^n})$, $(U_{k_\lambda}/U^1_{k_\lambda}) \otimes \mathbf{Z}/p^n\mathbf{Z} = \kappa(\lambda)^\times \otimes \mathbf{Z}/p^n\mathbf{Z}$ is cyclic of order p^n. Since λ splits in $k(\mu_{p^n}, (O_k^\times)^{1/p^n})$, $O_k^\times$ is in $(U_{k_\lambda})^{p^n}$ and a is injective (Rubin [18] Lemma 4.1.2 (i)). Next, we will show that the exact sequence

$$0 \longrightarrow (U_{k_\lambda}/U^1_{k_\lambda}) \otimes \mathbf{Z}/p^n\mathbf{Z} \stackrel{a}{\longrightarrow} \mathcal{C}_{k,\lambda,n} \stackrel{b}{\longrightarrow} A_k \longrightarrow 0$$

splits. Let $\mathfrak{q}_j$, a_j, ξ_j be as above. Suppose that $\pi_{\mathfrak{q}_j}$ is a uniformizer of $k_{\mathfrak{q}_j}$. We denote by $\Pi_{\mathfrak{q}_j}$ the idele whose $\mathfrak{q}_j$-component is $\pi_{\mathfrak{q}_j}$ and whose v-component is 1 for every prime v except for $\mathfrak{q}_j$ (the λ-component is also 1). Since λ splits in $k(\xi_j^{1/p^n})$, we have $\xi_j \in (U_{k_\lambda})^{p^n}$. Hence, the class of $\xi_j \in k^\times$ in $(k_\lambda^\times/U^1_{k_\lambda}) \otimes \mathbf{Z}/p^n\mathbf{Z} \oplus \bigoplus_{v\neq\lambda}(k_v^\times/U_{k_v}) \otimes \mathbf{Z}_p$ coincides with $(\Pi_{\mathfrak{q}_j})^{p^{a_j}}$. This shows that the class $[\Pi_{\mathfrak{q}_j}]_{\mathcal{C}_{k,\lambda,n}}$ of $\Pi_{\mathfrak{q}_j}$ in $\mathcal{C}_{k,\lambda,n}$ has order p^{a_j} because $b([\Pi_{\mathfrak{q}_j}]_{\mathcal{C}_{k,\lambda,n}}) = [\mathfrak{q}_j]_{A_k}$ where $[\mathfrak{q}_j]_{A_k}$ is the class of $\mathfrak{q}_j$ in A_k. We define a homomorphism $b' : A_k \longrightarrow \mathcal{C}_{k,\lambda,n}$ by $[\mathfrak{q}_j]_{A_k} \mapsto [\Pi_{\mathfrak{q}_j}]_{\mathcal{C}_{k,\lambda,n}}$ for all $j = 1, ..., s$. Clearly, b' is a section of b, hence the above exact sequence splits. By class field theory, this implies that there is a cyclic extension $k_n(\lambda)/k$ of degree p^n, which is linearly disjoint with k_H/k. From the construction, we know that λ is totally ramified in $k_n(\lambda)$, and $k_n(\lambda)/k$ is unramified outside λ.

As usual, we consider Kolyvagin's derivative operator. Put $G_\lambda = \mathrm{Gal}(k_n(\lambda)/k)$, and fix a generator σ_λ of G_λ for $\lambda \in \mathcal{P}_n$. We define $N_\lambda = \Sigma_{i=0}^{p^n-1}\sigma_\lambda^i \in \mathbf{Z}[G_\lambda]$ and $D_\lambda = \Sigma_{i=0}^{p^n-1} i\sigma_\lambda^i \in \mathbf{Z}[G_\lambda]$. For a squarefree product $\mathfrak{a} = \lambda_1 \cdot ... \cdot \lambda_r$ with $\lambda_i \in \mathcal{P}_n$, we define $k_n(\mathfrak{a})$ to be the compositum $k_n(\lambda_1)...k_n(\lambda_r)$, and $K_{n,(\mathfrak{a})} = Kk_n(\mathfrak{a})$. We simply write $K_{(\mathfrak{a})}$ for $K_{n,(\mathfrak{a})}$ if no confusion arises. For $\mathfrak{a} = \lambda_1 \cdot ... \cdot \lambda_r$, we also define $N_\mathfrak{a} = \prod_{i=1}^r N_{\lambda_i}$ and $D_\mathfrak{a} = \prod_{i=1}^r D_{\lambda_i} \in \mathbf{Z}[\mathrm{Gal}(k_n(\mathfrak{a})/k)] = \mathbf{Z}[\mathrm{Gal}(K_{(\mathfrak{a})}/K)]$. For a finite prime ρ of k which splits completely in $K_{(\mathfrak{a})}$, we take a prime $\rho_{K_{(\mathfrak{a})}}$ of $K_{(\mathfrak{a})}$. By the standard method of Euler systems (cf. Lemmas 2.1 and 2.2 in Rubin [17], or Lemma 4.4.2 (i) in Rubin [18]),

we know that there is a unique $\kappa_{\mathfrak{a},\rho_{K_{(\mathfrak{a})}}} \in (K^\times \otimes \mathbf{Z}/p^n)^\sim$ whose image in $(K_{(\mathfrak{a})}^\times \otimes \mathbf{Z}/p^n)^\sim$ coincides with $D_\mathfrak{a}(g_{K_{(\mathfrak{a})},\rho_{K_{(\mathfrak{a})}}})$. We also have an element $\delta_\mathfrak{a} \in \mathbf{Z}/p^n[\mathrm{Gal}(K/k)]^\sim$ such that $D_\mathfrak{a}\theta^\sim_{K_{(\mathfrak{a})}} \equiv \nu_{K_{(\mathfrak{a})}/K}(\delta_\mathfrak{a}) \pmod{p^n}$ where $\nu_{K_{(\mathfrak{a})}/K} : \mathbf{Z}_p[\mathrm{Gal}(K/k)]^\sim \longrightarrow \mathbf{Z}_p[\mathrm{Gal}(K_{(\mathfrak{a})}/k)]^\sim$ is the map induced by $\sigma \mapsto \sum_{\tau_{|K}=\sigma} \tau$ for $\sigma \in \mathrm{Gal}(K/k)$. This $\delta_\mathfrak{a}$ is also determined uniquely by this property. We sometimes write $\kappa_\mathfrak{a}$ for $\kappa_{\mathfrak{a},\rho_{K_{(\mathfrak{a})}}}$ if no confusion arises.
We take an odd character χ of $\mathrm{Gal}(K/k)$ such that $\chi \neq \omega$, and consider the χ-component $\kappa_\mathfrak{a}^\chi \in (K^\times \otimes \mathbf{Z}/p^n)^\chi$, $\delta_\mathfrak{a}^\chi \in \mathbf{Z}/p^n[\mathrm{Gal}(K/k)]^\chi = O_\chi$, ...etc.

Lemma 4.4. *Put* $S_i = \sigma_{\lambda_i} - 1 \in O_\chi[\mathrm{Gal}(K_{(\mathfrak{a})}/K)]$. *Then, we have*

$$\theta^\chi_{K_{(\mathfrak{a})}} \equiv (-1)^r \delta^\chi_\mathfrak{a} S_1 \cdot ... \cdot S_r \pmod{(p^n, S_1^2, ..., S_r^2)}.$$

Proof. We first prove $\theta^\chi_{K_{(\mathfrak{a})}} \equiv aS_1 \cdot ... \cdot S_r \mod (S_1^2, ..., S_r^2)$ for some $a \in O_\chi$ by induction on r. For any subfields M_1 and M_2 such that $K \subset M_1 \subset M_2 \subset K_{(\mathfrak{a})}$, we denote by $c_{M_2/M_1} : O_\chi[\mathrm{Gal}(M_2/K)] \longrightarrow O_\chi[\mathrm{Gal}(M_1/K)]$ the map induced by the restriction $\sigma \mapsto \sigma_{|M_1}$. Since $c_{K_{(\lambda_1)}/K}(\theta^\chi_{K_{(\lambda_1)}}) = ((1-\varphi^{-1}_{\lambda_1})\theta_K)^\chi$ (cf. Tate [23] p.86) and λ_1 splits completely in K, we have $c_{K_{(\lambda_1)}/K}(\theta^\chi_{K_{(\lambda_1)}}) = 0$. Hence, $S_1 = \sigma_{\lambda_1} - 1$ divides $\theta^\chi_{K_{(\lambda_1)}}$. So the first assertion was verified for $r = 1$.
Let $\mathfrak{a}_i = \mathfrak{a}/\lambda_i$ for i with $1 \le i \le r$. Then, we have $c_{K_{(\mathfrak{a})}/K_{(\mathfrak{a}_i)}}(\theta^\chi_{K_{(\mathfrak{a})}}) = ((1-\varphi^{-1}_{\lambda_i})\theta_{K_{(\mathfrak{a}_i)}})^\chi$. Since λ_i splits completely in K, φ_{λ_i} is in $\mathrm{Gal}(K_{(\mathfrak{a}_i)}/K)$. Hence, $1 - \varphi^{-1}_{\lambda_i}$ is in the ideal $I_{\mathrm{Gal}(K_{(\mathfrak{a}_i)}/K)} = (S_1, ..., S_{i-1}, S_{i+1}, ..., S_r)$. This implies that $c_{K_{(\mathfrak{a})}/K_{(\mathfrak{a}_i)}}(\theta^\chi_{K_{(\mathfrak{a})}})$ is in the ideal $(S_1^2, ..., S_{i-1}^2, S_{i+1}^2, ..., S_r^2)$ by the hypothesis of the induction. This holds for all i, so $\theta^\chi_{K_{(\mathfrak{a})}}$ can be written as $\theta^\chi_{K_{(\mathfrak{a})}} = \alpha + \beta$ where α is divisible by all S_i for $i = 1, ..., r$, and β is in $(S_1^2, ..., S_r^2)$. Therefore, $\theta^\chi_{K_{(\mathfrak{a})}} \equiv aS_1 \cdot ... \cdot S_r \mod (S_1^2, ..., S_r^2)$ for some $a \in O_\chi$.
Next, we determine a mod p^n. Note that $S_i D_{\lambda_i} \equiv -N_{\lambda_i} \pmod{p^n}$. Hence, $S_i^2 D_{\lambda_i} \equiv 0 \pmod{p^n}$. Thus, we have

$$D_\mathfrak{a}(\theta^\chi_{K_{(\mathfrak{a})}}) \equiv D_\mathfrak{a}(aS_1 \cdot ... \cdot S_r) \equiv (-1)^r N_\mathfrak{a}(a) \pmod{p^n}.$$

Hence, $N_\mathfrak{a}((-1)^r a) = \nu_{K_{(\mathfrak{a})}/K}((-1)^r a) \equiv \nu_{K_{(\mathfrak{a})}/K}(\delta^\chi_\mathfrak{a}) \pmod{p^n}$, which implies $\delta^\chi_\mathfrak{a} \equiv (-1)^r a \pmod{p^n}$ because $\nu_{K_{(\mathfrak{a})}/K}$ mod p^n is injective. This completes the proof of Lemma 4.4.

We put $G = \mathrm{Gal}(K_{(\mathfrak{a})}/K)$. As in §3, we have an isomorphism $O_\chi[G] \simeq A_{n,r}$ by the correspondence $\sigma_{\lambda_j} \leftrightarrow 1 + S_j$ where $A_{n,r}$ is the ring in 3.1 with $O = O_\chi$. For i, $s > 0$ and $\theta^\chi_{K_{(\mathfrak{a})}} \in O_\chi[G]$, we have an ideal $I_{i,s}(\theta^\chi_{K_{(\mathfrak{a})}})$ of O_χ as in 3.2. By the definition of $I_{i,s}(\theta^\chi_{K_{(\mathfrak{a})}})$ and Lemma 4.4, we know that $I_{r,1}(\theta^\chi_{K_{(\mathfrak{a})}})$ is generated by $\delta^\chi_\mathfrak{a}$ and p^n. Thus, we get

Corollary 4.5.

$$I_{r,1}(\theta^\chi_{K_{(\mathfrak{a})}}) = (\delta^\chi_\mathfrak{a}, p^n).$$

For a prime λ of k, we define the subgroup Div_K^λ of $\mathrm{Div}_K \otimes \mathbf{Z}_p$ by $\mathrm{Div}_K^\lambda = \bigoplus_{\lambda_K|\lambda} \mathbf{Z}_p[\lambda_K]$ where λ_K ranges over all primes of K above λ. We fix a prime λ_K, then $\mathrm{Div}_K^\lambda = \mathbf{Z}_p[\mathrm{Gal}(K/k)/D_{\lambda_K}][\lambda_K]$ where D_{λ_K} is the decomposition group of λ_K in $\mathrm{Gal}(K/k)$. Let $\mathrm{div}_\lambda : (K^\times \otimes \mathbf{Z}_p)^\chi \longrightarrow (\mathrm{Div}_K^\lambda)^\chi$ be the map induced by the composite of $\mathrm{div} : K^\times \otimes \mathbf{Z}_p \longrightarrow \mathrm{Div}_K \otimes \mathbf{Z}_p$ and the projection $\mathrm{Div}_K \otimes \mathbf{Z}_p \longrightarrow \mathrm{Div}_K^\lambda$. The following lemma is immediate from the defining properties of $\kappa_{\mathfrak{a},\rho_{K_{(\mathfrak{a})}}}$ and $\delta_\mathfrak{a}$, which we stated above.

Lemma 4.6. *Assume that ρ is a finite prime of k which splits completely in $K_{(\mathfrak{a})}$. We take a prime $\rho_{K_{(\mathfrak{a})}}$ of $K_{(\mathfrak{a})}$ and a prime ρ_K of K such that $\rho_{K_{(\mathfrak{a})}} \mid \rho_K \mid \rho$.*
(i) $\mathrm{div}_\rho(\kappa^\chi_{\mathfrak{a},\rho_{K_{(\mathfrak{a})}}}) \equiv (\delta_\mathfrak{a}[\rho_K])^\chi \pmod{p^n}$.
(ii) *If λ is prime to $\mathfrak{a}\rho$, we have* $\mathrm{div}_\lambda(\kappa^\chi_{\mathfrak{a},\rho_{K_{(\mathfrak{a})}}}) \equiv 0 \pmod{p^n}$.

We next proceed to an important property of $\kappa^\chi_{\mathfrak{a},\rho_{K_{(\mathfrak{a})}}}$. Suppose that λ is a prime in $\mathcal{P}_n$ with $(\lambda, \mathfrak{a}) = 1$ and ρ is a prime with $(\rho, \mathfrak{a}\lambda) = 1$. We assume both ρ and λ split completely in $K_{(\mathfrak{a})}$. Put $W = \mathrm{Ker}(\mathrm{div}_\lambda : (K^\times \otimes \mathbf{Z}_p)^\chi \longrightarrow (\mathrm{Div}_K^\lambda)^\chi)$, and $R_K^\lambda = \bigoplus_{\lambda_K|\lambda} \kappa(\lambda_K)^\times$ where $\kappa(\lambda_K)$ is the residue field of λ_K ($\kappa(\lambda_K)$ coincides with the residue field $\kappa(\lambda) = O_k/\lambda$ of λ because λ splits in K) and λ_K ranges over all primes of K above λ. We consider a natural map

$$\ell_\lambda : W/W^{p^n} \longrightarrow (R_K^\lambda/(R_K^\lambda)^{p^n})^\chi$$

induced by $x \mapsto (x \bmod \lambda_K)$. Note that $N(\lambda) \equiv 1 \pmod{p^n}$ because $\lambda \in \mathcal{P}_n$. So, $R_K^\lambda/(R_K^\lambda)^{p^n}$ is a free $\mathbf{Z}/p^n\mathbf{Z}[\mathrm{Gal}(K/k)]$-module of rank 1. We take a basis $u \in (R_K^\lambda/(R_K^\lambda)^{p^n})^\chi$, and define $\ell_{\lambda,u} : W/W^{p^n} \longrightarrow (\mathbf{Z}/p^n\mathbf{Z}[\mathrm{Gal}(K/k)])^\chi \simeq O_\chi/(p^n)$ to be the composite of ℓ_λ and $u \mapsto 1$. By Lemma 4.6 (ii), $\kappa^\chi_{\mathfrak{a},\rho_{K_{(\mathfrak{a})}}}$ is in W/W^{p^n} (note that $W/W^{p^n} \subset (K^\times \otimes \mathbf{Z}/p^n\mathbf{Z})^\chi$). We are interested in $\ell_{\lambda,u}(\kappa^\chi_{\mathfrak{a},\rho_{K_{(\mathfrak{a})}}})$. We take a prime $\rho_{K_{(\mathfrak{a})}}$ (resp. $\lambda_{K_{(\mathfrak{a})}}$) of $K_{(\mathfrak{a})}$ and a prime ρ_K (resp. λ_K) of K such that $\rho_{K_{(\mathfrak{a})}} \mid \rho_K \mid \rho$ (resp. $\lambda_{K_{(\mathfrak{a})}} \mid \lambda_K \mid \lambda$).

Proposition 4.7. *We assume that $\chi(\mathfrak{p}) \neq 1$ for any prime $\mathfrak{p}$ of k above p, and that $[\rho_K]$ and $[\lambda_K]$ yield the same class in A_K^χ. Then, there is an element $x \in W/W^{p^n}$ satisfying the following properties.*
(i) *For any prime λ' of k such that $(\lambda', \mathfrak{a}) = 1$, we have*

$$\mathrm{div}_{\lambda'}(\kappa^\chi_{\mathfrak{a},\rho_{K_{(\mathfrak{a})}}}/x) \equiv 0 \pmod{p^n}.$$

(ii) *Choosing u suitably, we have*

$$\frac{1 - N(\lambda)^{-1}}{p^n}\ell_{\lambda,u}(x) \equiv \delta^\chi_{\mathfrak{a}\lambda} \pmod{(\delta^\chi_\mathfrak{a}, p^n)}$$

where $N(\lambda) = \#\kappa(\lambda) = \#(O_k/\lambda)$.
In particular, in the case $\mathfrak{a} = (1)$ we can take $x = g^\chi_{K,\rho_K} \bmod W^{p^n}$.

This proposition corresponds to Theorem 2.4 in Rubin [17], which was proved by using some extra property of the Gauss sums. For our g_{F,ρ_F} we do not have the property corresponding to Lemma 2.5 in [17], so we have to give here a proof in which we use only the definition of g_{F,ρ_F}, namely $\mathrm{div}(g^{\chi}_{F,\rho_F}) = (\theta_F[\rho_F])^{\chi}$.

Proof of Proposition 4.7. We denote by $\lambda_{K_{(\mathfrak{a}\lambda)}}$ the unique prime of $K_{(\mathfrak{a}\lambda)}$ above $\lambda_{K_{(\mathfrak{a})}}$. Put $N = \mathrm{ord}_p(N(\lambda)-1)+2n$. We take by Chebotarev density theorem a prime ρ' of k which splits completely in $K_{(\mathfrak{a}\lambda)}(\mu_{p^N})$ such that the class of $[\rho'_{K_{(\mathfrak{a}\lambda)}}]$ in $A^{\chi}_{K_{(\mathfrak{a}\lambda)}}$ for a prime $\rho'_{K_{(\mathfrak{a}\lambda)}}$ of $K_{(\mathfrak{a}\lambda)}$ over ρ' coincides with the class of $[\lambda_{K_{(\mathfrak{a}\lambda)}}]$. Let ρ'_K be the prime below $\rho'_{K_{(\mathfrak{a}\lambda)}}$. Then, the class of $[\lambda_K]$, the class of $[\rho'_K]$, and the class of $[\rho_K]$ in A^{χ}_K all coincide. Hence, there is an element $a \in W$ such that $\mathrm{div}(a) = [\rho_K]-[\rho'_K]$. Define $x \in W/W^{p^n}$ by $x = \kappa^{\chi}_{\mathfrak{a},\rho'_{K_{(\mathfrak{a})}}} \cdot a^{\delta^{\chi}_{\mathfrak{a}}}$. By Lemma 4.6 (ii), $\mathrm{div}_{\lambda'}(\kappa^{\chi}_{\mathfrak{a},\rho_{K_{(\mathfrak{a})}}}/x) \equiv 0 \pmod{p^n}$ for a prime λ' such that $(\lambda', \mathfrak{a}\rho\rho') = 1$. By Lemma 4.6 (i), the same is true for $\lambda' = \rho$ and ρ'. Thus, we get the first assertion. In the case $\mathfrak{a} = (1)$, we take $y = g^{\chi}_{K,\rho'_K} a^{\theta^{\chi}_K}$. Then, $\mathrm{div}(y) = \mathrm{div}(g^{\chi}_{K,\rho_K})$, so $y = g^{\chi}_{K,\rho_K}$, and we have $g^{\chi}_{K,\rho_K} \bmod W^{p^n} = y \bmod W^{p^n} = x$.

In order to show the second assertion, it is enough to prove

$$\frac{1-N(\lambda)^{-1}}{p^n}\ell_{\lambda,u}(\kappa^{\chi}_{\mathfrak{a},\rho'_{K_{(\mathfrak{a})}}}) \equiv \delta^{\chi}_{\mathfrak{a}\lambda} \pmod{p^n} \tag{1}$$

for some u. Set $\mathrm{Div}^{\lambda}_{K_{(\mathfrak{a}\lambda)}} = \bigoplus_{v|\lambda} \mathbf{Z}_p[v]$ and $R^{\lambda}_{K_{(\mathfrak{a}\lambda)}} = \bigoplus_{v|\lambda} \kappa(v)^{\times} = \bigoplus_{v|\lambda} (O_{K_{(\mathfrak{a}\lambda)}}/v)^{\times}$ where v ranges over all primes of $K_{(\mathfrak{a}\lambda)}$ above λ. Since the primes of $K_{(\mathfrak{a})}$ above λ are totally ramified in $K_{(\mathfrak{a}\lambda)}$, $(\mathrm{Div}^{\lambda}_{K_{(\mathfrak{a}\lambda)}})^{\chi}$ is isomorphic to $O_{\chi}[\mathrm{Gal}(K_{(\mathfrak{a})}/K)]$ and $(R^{\lambda}_{K_{(\mathfrak{a}\lambda)}}/(R^{\lambda}_{K_{(\mathfrak{a}\lambda)}})^{p^n})^{\chi}$ is isomorphic to $O_{\chi}/(p^n)[\mathrm{Gal}(K_{(\mathfrak{a})}/K)]$. We consider $W_{K_{(\mathfrak{a}\lambda)}} = \mathrm{Ker}(\mathrm{div}_{\lambda} : (K^{\times}_{(\mathfrak{a}\lambda)} \otimes \mathbf{Z}_p)^{\chi} \longrightarrow (\mathrm{Div}^{\lambda}_{K_{(\mathfrak{a}\lambda)}})^{\chi})$ and a natural map

$$\ell_{\lambda,K_{(\mathfrak{a}\lambda)}} : W_{K_{(\mathfrak{a}\lambda)}}/W^{p^n}_{K_{(\mathfrak{a}\lambda)}} \longrightarrow (R^{\lambda}_{K_{(\mathfrak{a}\lambda)}}/(R^{\lambda}_{K_{(\mathfrak{a}\lambda)}})^{p^n})^{\chi}.$$

We take $b \in (K^{\times}_{(\mathfrak{a}\lambda)} \otimes \mathbf{Z}_p)^{\chi}$ such that $\mathrm{div}(b) = [\lambda_{K_{(\mathfrak{a}\lambda)}}] - [\rho'_{K_{(\mathfrak{a}\lambda)}}]$. Then, $b' = \ell_{\lambda,K_{(\mathfrak{a}\lambda)}}(b^{\sigma_{\lambda}-1})$ is a generator of $(R^{\lambda}_{K_{(\mathfrak{a}\lambda)}}/(R^{\lambda}_{K_{(\mathfrak{a}\lambda)}})^{p^n})^{\chi}$ as an $O_{\chi}/(p^n)[\mathrm{Gal}(K_{(\mathfrak{a})}/K)]$-module ([19] Chap.4 Prop.7 Cor.1). Using this b', we identify $(R^{\lambda}_{K_{(\mathfrak{a}\lambda)}}/(R^{\lambda}_{K_{(\mathfrak{a}\lambda)}})^{p^n})^{\chi}$ with $O_{\chi}/(p^n)[\mathrm{Gal}(K_{(\mathfrak{a})}/K)]$, and define

$$\ell_{\lambda,K_{(\mathfrak{a}\lambda)},b'} : W_{K_{(\mathfrak{a}\lambda)}}/W^{p^n}_{K_{(\mathfrak{a}\lambda)}} \longrightarrow O_{\chi}/p^n[\mathrm{Gal}(K_{(\mathfrak{a})}/K)].$$

Since λ splits completely in $K_{(\mathfrak{a})}$, $c_{K_{(\mathfrak{a}\lambda)}/K_{(\mathfrak{a})}}(\theta^{\chi}_{K_{(\mathfrak{a}\lambda)}}) = 0$ by the formula in the proof of Lemma 4.1. Hence, $\sigma_{\lambda}-1$ divides $\theta^{\chi}_{K_{(\mathfrak{a}\lambda)}}$. Since $(\sigma_{\lambda}-1)[\lambda_{K_{(\mathfrak{a}\lambda)}}] = 0$, we have $\theta^{\chi}_{K_{(\mathfrak{a}\lambda)}}[\lambda_{K_{(\mathfrak{a}\lambda)}}]^{\chi} = 0$. So, $\mathrm{div}(g^{\chi}_{K_{(\mathfrak{a}\lambda)},\rho'_{K_{(\mathfrak{a}\lambda)}}}) = \mathrm{div}((b^{-\theta_{K_{(\mathfrak{a}\lambda)}}})^{\chi}) =$

$\theta^{\chi}_{K_{(\mathfrak{a}\lambda)}}[\rho'_{K_{(\mathfrak{a}\lambda)}}]^{\chi}$. The injectivity of div implies that $g^{\chi}_{K_{(\mathfrak{a}\lambda)},\rho'_{K_{(\mathfrak{a}\lambda)}}} = (b^{-\theta_{K_{(\mathfrak{a}\lambda)}}})^{\chi}$. Further, by Lemma 4.4, we can write

$$\theta^{\chi}_{K_{(\mathfrak{a}\lambda)}} \equiv (-1)^{r+1}\delta^{\chi}_{\mathfrak{a}\lambda}S_1\cdot\ldots\cdot S_r(\sigma_\lambda-1)+\beta \pmod{p^n}$$

where $\beta\in(S_1^2,\ldots,S_r^2,(\sigma_\lambda-1)^2)$. Since $\sigma_\lambda-1$ divides $\theta^{\chi}_{K_{(\mathfrak{a}\lambda)}}$, $\sigma_\lambda-1$ also divides β. We write $\beta=(\sigma_\lambda-1)\beta'$. So $\theta^{\chi}_{K_{(\mathfrak{a}\lambda)}}\equiv(\sigma_\lambda-1)((-1)^{r+1}\delta^{\chi}_{\mathfrak{a}\lambda}S_1\cdot\ldots\cdot S_r+\beta')$ (mod p^n). Then,

$$\begin{aligned}\ell_{\lambda,K_{(\mathfrak{a}\lambda)},b'}(g^{\chi}_{K_{(\mathfrak{a}\lambda)},\rho'_{K_{(\mathfrak{a}\lambda)}}}) &= \ell_{\lambda,K_{(\mathfrak{a}\lambda)},b'}((b^{-\theta_{K_{(\mathfrak{a}\lambda)}}})^{\chi})\\ &= -c_{K_{(\mathfrak{a}\lambda)}/K_{(\mathfrak{a})}}((-1)^{r+1}\delta^{\chi}_{\mathfrak{a}\lambda}S_1\cdot\ldots\cdot S_r+\beta')\\ &= (-1)^r\delta^{\chi}_{\mathfrak{a}\lambda}S_1\cdot\ldots\cdot S_r-c_{K_{(\mathfrak{a}\lambda)}/K_{(\mathfrak{a})}}(\beta').\end{aligned}$$

Since $c_{K_{(\mathfrak{a}\lambda)}/K_{(\mathfrak{a})}}(\beta')\in(S_1^2,\ldots,S_r^2)$, using $S_iD_{\lambda_i}\equiv -N_{\lambda_i}\pmod{p^n}$ and $S_i^2D_{\lambda_i}\equiv 0\pmod{p^n}$, we have

$$\begin{aligned}\ell_{\lambda,K_{(\mathfrak{a}\lambda)},b'}((g^{\chi}_{K_{(\mathfrak{a}\lambda)},\rho'_{K_{(\mathfrak{a}\lambda)}}})^{D_{\mathfrak{a}}}) &= D_{\mathfrak{a}}((-1)^r\delta^{\chi}_{\mathfrak{a}\lambda}S_1\cdot\ldots\cdot S_r-c_{K_{(\mathfrak{a}\lambda)}/K_{(\mathfrak{a})}}(\beta'))\\ &= N_{\mathfrak{a}}\delta^{\chi}_{\mathfrak{a}\lambda}\\ &= \nu_{K_{(\mathfrak{a})}/K}(\delta^{\chi}_{\mathfrak{a}\lambda}).\end{aligned}$$

We similarly define $W_{K_{(\mathfrak{a})}}=\mathrm{Ker}(\mathrm{div}_\lambda$ for $K_{(\mathfrak{a})})\subset(K_{(\mathfrak{a})}^{\times}\otimes\mathbf{Z}_p)^{\chi}$. Recall that $W=\mathrm{Ker}(\mathrm{div}_\lambda$ for $K)\subset(K^{\times}\otimes\mathbf{Z}_p)^{\chi}$. Let ℓ_λ (resp. $\ell_{\lambda,K_{(\mathfrak{a})}}$, $\ell_{\lambda,K_{(\mathfrak{a}\lambda)}}$) be the natural map $W_K/W_K^{p^n}\longrightarrow(R_K^\lambda/(R_K^\lambda)^{p^n})^{\chi}$ (resp. $W_{K_{(\mathfrak{a})}}/W_{K_{(\mathfrak{a})}}^{p^n}\longrightarrow(R^\lambda_{K_{(\mathfrak{a})}}/(R^\lambda_{K_{(\mathfrak{a})}})^{p^n})^{\chi}$, $W_{K_{(\mathfrak{a}\lambda)}}/W_{K_{(\mathfrak{a}\lambda)}}^{p^n}\longrightarrow(R^\lambda_{K_{(\mathfrak{a}\lambda)}}/(R^\lambda_{K_{(\mathfrak{a}\lambda)}})^{p^n})^{\chi}$). We have a commutative diagram

$$\begin{array}{ccccc} W_K/W_K^{p^n} & \longrightarrow & W_{K_{(\mathfrak{a})}}/W_{K_{(\mathfrak{a})}}^{p^n} & \longrightarrow & W_{K_{(\mathfrak{a}\lambda)}}/W_{K_{(\mathfrak{a}\lambda)}}^{p^n}\\ \downarrow{\scriptstyle \ell_\lambda} & & \downarrow{\scriptstyle \ell_{\lambda,K_{(\mathfrak{a})}}} & & \downarrow{\scriptstyle \ell_{\lambda,K_{(\mathfrak{a}\lambda)}}}\\ (R_K^\lambda/(R_K^\lambda)^{p^n})^{\chi} & \longrightarrow & (R^\lambda_{K_{(\mathfrak{a})}}/(R^\lambda_{K_{(\mathfrak{a})}})^{p^n})^{\chi} & \longrightarrow & (R^\lambda_{K_{(\mathfrak{a}\lambda)}}/(R^\lambda_{K_{(\mathfrak{a}\lambda)}})^{p^n})^{\chi}\end{array}$$

where the horizontal arrows are the natural maps. We take a generator u' of $(R^\lambda_{K_{(\mathfrak{a})}}/(R^\lambda_{K_{(\mathfrak{a})}})^{p^n})^{\chi}$ as an $O_\chi/(p^n)[\mathrm{Gal}(K_{(\mathfrak{a})}/K)]$-module, and a generator u'' of $(R_K^\lambda/(R_K^\lambda)^{p^n})^{\chi}$ as an $O_\chi/(p^n)$-module such that the diagram

$$\begin{array}{ccccc} W_K/W_K^{p^n} & \longrightarrow & W_{K_{(\mathfrak{a})}}/W_{K_{(\mathfrak{a})}}^{p^n} & \longrightarrow & W_{K_{(\mathfrak{a}\lambda)}}/W_{K_{(\mathfrak{a}\lambda)}}^{p^n}\\ \downarrow{\scriptstyle \ell_{\lambda,u''}} & & \downarrow{\scriptstyle \ell_{\lambda,K_{(\mathfrak{a})},u'}} & & \downarrow{\scriptstyle \ell_{\lambda,K_{(\mathfrak{a}\lambda)},b'}}\\ O_\chi/(p^n) & \overset{\nu_{K_{(\mathfrak{a})}/K}}{\longrightarrow} & O_\chi/(p^n)[\mathrm{Gal}(K_{(\mathfrak{a})}/K)] & \overset{id}{\longrightarrow} & O_\chi/(p^n)[\mathrm{Gal}(K_{(\mathfrak{a})}/K)]\end{array}$$

commutes where $\nu_{K_{(\mathfrak{a})}/K}$ is the norm map defined before Lemma 4.4, and id is the identity map.

Using the above computation of $\ell_{\lambda,K_{(\mathfrak{a}\lambda)},b'}((g^{\chi}_{K_{(\mathfrak{a}\lambda)},\rho'_{K_{(\mathfrak{a}\lambda)}}})^{D_{\mathfrak{a}}})$, if we get

$$\frac{1-N(\lambda)^{-1}}{p^n}\ell_{\lambda,K_{(\mathfrak{a})}}(g^{\chi}_{K_{(\mathfrak{a})},\rho'_{K_{(\mathfrak{a})}}}) = \ell_{\lambda,K_{(\mathfrak{a}\lambda)}}(g^{\chi}_{K_{(\mathfrak{a}\lambda)},\rho'_{K_{(\mathfrak{a}\lambda)}}}), \tag{2}$$

we obtain (1) from the above commutative diagram.

The relation (2) is sometimes called the "congruence condition", and can be proved by the method of Rubin [18] Corollary 4.8.1 and Kato [8] Prop.1.1. Put $L = K_{(\mathfrak{a})}(\mu_{p^N})$ and $L_{(\lambda)} = K_{(\mathfrak{a}\lambda)}(\mu_{p^N})$ (Recall that N was chosen in the beginning of the proof). We take a prime $\rho'_{L_{(\lambda)}}$ of $L_{(\lambda)}$ above $\rho'_{K_{(\mathfrak{a}\lambda)}}$, and denote by ρ'_L the prime of L below $\rho'_{L_{(\lambda)}}$. We define $\ell_{\lambda,L} : W_L/W_L^{p^N} \longrightarrow (R^{\lambda}_L/(R^{\lambda}_L)^{p^N})^{\chi}$, and $\ell_{\lambda,L_{(\lambda)}} : W_{L_{(\lambda)}}/W^{p^N}_{L_{(\lambda)}} \longrightarrow (R^{\lambda}_{L_{(\lambda)}}/(R^{\lambda}_{L_{(\lambda)}})^{p^N})^{\chi}$ similarly. We identify $(R^{\lambda}_L/(R^{\lambda}_L)^{p^N})^{\chi}$ with $(R^{\lambda}_{L_{(\lambda)}}/(R^{\lambda}_{L_{(\lambda)}})^{p^N})^{\chi}$ by the map induced by the inclusion. Then, the norm map induces the multiplication by p^n. Since $N_{L_{(\lambda)}/L}(g^{\chi}_{L_{(\lambda)},\rho'_{L_{(\lambda)}}}) = (1-\varphi_{\lambda}^{-1})g^{\chi}_{L,\rho'_L}$, we have $p^n\ell_{\lambda,L_{(\lambda)}}(g^{\chi}_{L_{(\lambda)},\rho'_{L_{(\lambda)}}}) = (1-N(\lambda)^{-1})\ell_{\lambda,L}(g^{\chi}_{L,\rho'_L})$. Hence,

$$\ell_{\lambda,L_{(\lambda)}}(g^{\chi}_{L_{(\lambda)},\rho'_{L_{(\lambda)}}}) \equiv p^{-n}(1-N(\lambda)^{-1})\ell_{\lambda,L}(g^{\chi}_{L,\rho'_L}) \pmod{p^{N-n}}.$$

Let $\mathcal{S}$ be the set of primes of k ramifying in $L_{(\lambda)}$ and not ramifying in $K_{(\mathfrak{a}\lambda)}$. Note that if $\mathfrak{p} \in \mathcal{S}$, $\mathfrak{p}$ is a prime above p. By Lemma 4.1 we have $N_{L_{(\lambda)}/K_{(\mathfrak{a}\lambda)}}(g^{\chi}_{L_{(\lambda)},\rho'_{L_{(\lambda)}}}) = \epsilon_{K_{(\mathfrak{a}\lambda)}}g^{\chi}_{K_{(\mathfrak{a}\lambda)},\rho'_{K_{(\mathfrak{a}\lambda)}}}$ and $N_{L/K_{(\mathfrak{a})}}(g^{\chi}_{L,\rho'_L}) = \epsilon_{K_{(\mathfrak{a})}}g^{\chi}_{K_{(\mathfrak{a})},\rho'_{K_{(\mathfrak{a})}}}$ where $\epsilon_{K_{(\mathfrak{a}\lambda)}} = (\Pi_{\mathfrak{p}\in\mathcal{S}}(1-\varphi_{\mathfrak{p}}^{-1}))^{\chi} \in O_{\chi}[\mathrm{Gal}(K_{(\mathfrak{a}\lambda)}/K)]$ and $\epsilon_{K_{(\mathfrak{a})}} = c_{K_{(\mathfrak{a}\lambda)}/K_{(\mathfrak{a})}}(\epsilon_{K_{(\mathfrak{a}\lambda)}})$ ($c_{K_{(\mathfrak{a}\lambda)}/K_{(\mathfrak{a})}}$ is the restriction map). Since we assumed $\chi(\mathfrak{p}) \neq 1$ for all $\mathfrak{p}$ above p, $\epsilon_{K_{(\mathfrak{a}\lambda)}}$ is a unit of $O_{\chi}[\mathrm{Gal}(K_{(\mathfrak{a}\lambda)}/K)]$. Hence, we obtain (2) by taking the norms $N_{L_{(\lambda)}/K_{(\mathfrak{a}\lambda)}}$ of both sides of the above formula. This completes the proof of Proposition 4.7.

5 The other inclusion

In this section, for K and χ in Theorem 0.1 and $i \geq 0$, we will prove $\mathrm{Fitt}_{i,O_{\chi}}(A^{\chi}_K) \subset (\Theta_{i,K})^{\chi}$ to complete the proof of Theorem 0.1. More precisely, we will show $\mathrm{Fitt}_{i,O_{\chi}}(A^{\chi}_K) \subset (\Theta_{i,1,K})^{\chi}$.

As in Theorem 0.1, suppose that

$$A^{\chi}_K \simeq O_{\chi}/(p^{n_1}) \oplus ... \oplus O_{\chi}/(p^{n_r})$$

with $0 < n_1 \leq ... \leq n_r$. We take generators $\mathbf{c}_1$,...,$\mathbf{c}_r$ corresponding to the above isomorphism ($\mathbf{c}_j$ generates the j-th direct summand). Let $\mathcal{P}_n$ be as in §4. We define

$$\mathcal{Q}_j = \{\lambda \in \mathcal{P}_n : \text{ there is a prime } \lambda_K \text{ of } K \text{ above } \lambda \text{ such that the class of } \lambda_K \text{ in } A^{\chi}_K \text{ is } \mathbf{c}_j\},$$

and $\mathcal{Q} = \bigcup_{1 \leq j \leq r} \mathcal{Q}_j$. We consider an exact sequence

$$0 \longrightarrow (K^\times \otimes \mathbf{Z}_p)^\chi \xrightarrow{\text{div}} (\text{Div}_K \otimes \mathbf{Z}_p)^\chi \longrightarrow A_K^\chi \longrightarrow 0.$$

For $\lambda \in \mathcal{Q}$, we have $(\mathbf{Z}_p[\text{Gal}(K/k)][\lambda_K])^\chi = O_\chi[\lambda_K]^\chi$. We define $M_\mathcal{Q}$ to be the inverse image of $\bigoplus_{\lambda \in \mathcal{Q}} O_\chi[\lambda_K]^\chi$ by div : $(K^\times \otimes \mathbf{Z}_p)^\chi \longrightarrow (\text{Div}_K \otimes \mathbf{Z}_p)^\chi$. On the other hand, as an abstract O_χ-module, A_K^χ fits into an exact sequence

$$0 \longrightarrow \bigoplus_{j=1}^r O_\chi e_j \xrightarrow{f} \bigoplus_{j=1}^r O_\chi e'_j \xrightarrow{g} A_K^\chi \longrightarrow 0$$

where (e_j) and (e'_j) are bases of free O_χ-modules of rank r, f is the map $e_j \mapsto p^{n_j} e'_j$, and g is induced by $e'_j \mapsto \mathbf{c}_j$. We define $\beta : \bigoplus_{\lambda \in \mathcal{Q}} O_\chi[\lambda_K]^\chi \longrightarrow \bigoplus_{j=1}^r O_\chi e'_j$ by $[\lambda_K]^\chi \mapsto e'_j$ for all $\lambda \in \mathcal{Q}_j$ and $j = 1, ..., r$. Then, β induces $\alpha : M_\mathcal{Q} \longrightarrow \bigoplus_{j=1}^r O_\chi e_j$, and we have a commutative diagram of O_χ-modules

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M_\mathcal{Q} & \xrightarrow{\text{div}} & \bigoplus_{\lambda \in \mathcal{Q}} O_\chi[\lambda_K]^\chi & \longrightarrow & A_K^\chi & \longrightarrow & 0 \\
 & & \downarrow \alpha & & \downarrow \beta & & \| & & \\
0 & \longrightarrow & \bigoplus_{j=1}^r O_\chi e_j & \xrightarrow{f} & \bigoplus_{j=1}^r O_\chi e'_j & \xrightarrow{g} & A_K^\chi & \longrightarrow & 0.
\end{array}$$

Put $m = \text{length}_{O_\chi}(A_K^\chi)$. We take $n > 0$ such that $n \geq 2m$ and $\mu_{p^{n+1}} \not\subset K$. We use the same notation as in Proposition 4.7. Especially, we consider

$$\ell_\lambda : W/W^{p^n} \longrightarrow (R_K^\lambda/(R_K^\lambda)^{p^n})^\chi \simeq O_\chi/(p^n)$$

for $\lambda \in \mathcal{Q}$.

Lemma 5.1. *Suppose that $\mathfrak{a}$, λ, ρ,...etc satisfy the hypotheses of Proposition 4.7. We further assume that the primes dividing $\mathfrak{a}\lambda\rho$ are all in $\mathcal{Q}$. Then, there exists $\tilde{\kappa}^\chi_{\mathfrak{a},\rho_{K(\mathfrak{a})}} \in M_\mathcal{Q}$ satisfying the following properties.*
(i) *For any prime λ' such that $(\lambda', \mathfrak{a}\rho) = 1$, we have*

$$\text{div}_{\lambda'}(\tilde{\kappa}^\chi_{\mathfrak{a},\rho_{K(\mathfrak{a})}}) = 0.$$

(ii)

$$\text{div}_\rho(\tilde{\kappa}^\chi_{\mathfrak{a},\rho_{K(\mathfrak{a})}}) \equiv (\delta_\mathfrak{a}[\rho_K])^\chi \pmod{p^n}.$$

(iii)

$$\frac{1 - N(\lambda)^{-1}}{p^n} \ell_\lambda(\tilde{\kappa}^\chi_{\mathfrak{a},\rho_{K(\mathfrak{a})}}) \equiv u\delta^\chi_{\mathfrak{a}\lambda} \pmod{(\delta^\chi_\mathfrak{a}, p^m)}$$

for some $u \in O_\chi^\times$.

Proof. Let x be an element in W/W^{p^n}, which satisfies the conditions in Proposition 4.7, and take a lifting $y \in W$ of x. By Proposition 4.7 (i) and Lemma 4.6, we can write $\text{div}(y) = \mathcal{A} + p^n\mathcal{B}$ where $\mathcal{A}$ is a divisor whose support is contained in the primes dividing $\mathfrak{a}\rho$. Since the class of $p^m\mathcal{B}$ in A_K^χ is zero, we can take $z \in (K^\times \otimes \mathbf{Z}_p)^\chi$ such that $\mathrm{div}(z) = p^m\mathcal{B}$. Put $\tilde{\kappa}^\chi_{\mathfrak{a},\rho_{K_{(\mathfrak{a})}}} = y/z^{p^{n-m}}$. Then, $\tilde{\kappa}^\chi_{\mathfrak{a},\rho_{K_{(\mathfrak{a})}}}$ is in $M_\mathcal{Q}$, and satisfies the above properties (i), (ii), and (iii) by Proposition 4.7 and Lemma 4.6.

We will prove Theorem 0.1. First of all, as we saw in Proposition 3.2, $\mathrm{Fitt}_{0,O_\chi}(A_K^\chi) = \Theta^\chi_{0,K}$. Recall that we put $m = \mathrm{length}_{O_\chi}(A_K^\chi)$, so $\mathrm{Fitt}_{0,O_\chi}(A_K^\chi) = (p^m)$. Next, we consider the commutative diagram before Lemma 5.1. We denote by $\alpha_j : M_\mathcal{Q} \longrightarrow O_\chi e_j \simeq O_\chi$ the composite of α and the j-th projection. We take $\rho_r \in \mathcal{Q}_r$ and a prime $\rho_{r,K}$ of K above ρ_r. We consider $g^\chi_{K,\rho_{r,K}} \in M_\mathcal{Q}$. We choose $\lambda_r \in \mathcal{Q}_r$ such that $\lambda_r \neq \rho_r$, $\mathrm{ord}_p(N(\lambda_r)-1) = n$, the class of $\lambda_{r,K}$ in A_K^χ coincides with the class of $\rho_{r,K}$, and $\alpha_r(g^\chi_{K,\rho_{r,K}}) \bmod p^n = u'\ell_{\lambda_r}(g^\chi_{K,\rho_{r,K}})$ for some $u' \in O_\chi^\times$. This is possible by Chebotarev density theorem (Theorem 3.1 in Rubin [17], cf. also [16]). By the commutative diagram before Lemma 5.1 and $\mathrm{div}(g^\chi_{K,\rho_{r,K}}) = \theta_K^\chi[\rho_{r,K}]^\chi$, we have

$$\mathrm{ord}_p(\alpha_r(g^\chi_{K,\rho_{r,K}})) + n_r = \mathrm{ord}_p(\theta_K^\chi) = m. \tag{3}$$

On the other hand, by Proposition 4.7, we have $\ell_{\lambda_r}(g^\chi_{K,\rho_{r,K}}) = u\delta^\chi_{\lambda_r} \bmod (p^m)$ for some $u \in O_\chi^\times$. Hence, $\alpha_r(g^\chi_{K,\rho_{r,K}}) \equiv u'\ell_{\lambda_r}(g^\chi_{K,\rho_{r,K}}) \equiv uu'\delta^\chi_{\lambda_r} \bmod (p^m)$. From (3), $\delta^\chi_{\lambda_r} \bmod p^m \neq 0$, hence, $\mathrm{ord}_p(\alpha_r(g^\chi_{K,\rho_{r,K}})) = \mathrm{ord}_p(\delta^\chi_{\lambda_r})$ (for a nonzero element x in O_χ/p^m, $\mathrm{ord}_p(x)$ is defined to be $\mathrm{ord}_p(\tilde{x})$ where $\tilde{x}$ is a lifting of x to O_χ). Therefore, we have

$$\mathrm{ord}_p(\delta^\chi_{\lambda_r}) = m - n_r.$$

Hence, $\mathrm{Fitt}_{1,O_\chi}(A_K^\chi) = (p^{m-n_r})$ is generated by $I_{1,1}(\theta^\chi_{K_{(\lambda_r)}})$ by Corollary 4.5. Thus, $\mathrm{Fitt}_{1,O_\chi}(A_K^\chi) \subset (\Theta_{1,1,K})^\chi \subset (\Theta_{1,K})^\chi$.

For any $i > 1$, we prove $\mathrm{Fitt}_{i,O_\chi}(A_K^\chi) \subset \Theta^\chi_{i,K}$ by the same method. We will show that we can take $\lambda_r \in \mathcal{Q}_r$, $\lambda_{r-1} \in \mathcal{Q}_{r-1}$,...inductively such that $\delta^\chi_{\mathfrak{a}_i}$ generates $\mathrm{Fitt}_{i,O_\chi}(A_K^\chi)$ where $\mathfrak{a}_i = \lambda_r \cdot ... \cdot \lambda_{r-i+1}$. For i such that $1 < i \leq r$, suppose that λ_r,...,λ_{r-i+2} were defined. We first take $\rho_{r-i+1} \in \mathcal{Q}_{r-i+1}$, which splits completely in $K_{(\mathfrak{a}_{i-1})}$. We consider $\kappa = \tilde{\kappa}^\chi_{\mathfrak{a}_{i-1},\rho_{r-i+1,K_{(\mathfrak{a}_{i-1})}}} \in M_\mathcal{Q}$ where we used the notation in Lemma 5.1. We choose $\lambda_{r-i+1} \in \mathcal{Q}_{r-i+1}$ such that $\lambda_{r-i+1} \neq \rho_{r-i+1}$, $\mathrm{ord}_p(N(\lambda_{r-i+1})-1) = n$, λ_{r-i+1} splits completely in $K_{(\mathfrak{a}_{i-1})}$, the class of $\lambda_{r-i+1,K}$ in A_K^χ coincides with the class of $\rho_{r-i+1,K}$ in A_K^χ, and $\alpha_{r-i+1}(\kappa) \bmod p^n = u'\ell_{\lambda_{r-i+1}}(\kappa)$ for some $u' \in O_\chi^\times$. This is also possible by Chebotarev density theorem (Theorem 3.1 in Rubin [17], cf. also [16]). By Lemma 5.1 (ii), $\mathrm{div}_{\rho_{r-i+1}}(\kappa) \equiv \delta^\chi_{\mathfrak{a}_{i-1}}[\rho_{r-i+1}]^\chi \pmod{p^n}$. Hence, from the commutative diagram before Lemma 5.1, we obtain

$$\mathrm{ord}_p(\alpha_{r-i+1}(\kappa)) + n_{r-i+1} = \mathrm{ord}_p(\delta^\chi_{\mathfrak{a}_{i-1}}).$$

By the hypothesis of the induction, we have $\mathrm{ord}_p(\delta^{\chi}_{\mathfrak{a}_{i-1}}) = n_1 + ... + n_{r-i+1}$. It follows that

$$\mathrm{ord}_p(\alpha_{r-i+1}(\kappa)) = n_1 + ... + n_{r-i}.$$

On the other hand, by Lemma 5.1 (iii), we have

$$\begin{aligned}\mathrm{ord}_p(\alpha_{r-i+1}(\kappa)) &= \mathrm{ord}_p(\ell_{\lambda_{r-i+1}}(\kappa)) = \mathrm{ord}_p(\delta^{\chi}_{\mathfrak{a}_{i-1}\lambda_{r-i+1}}) \\ &= \mathrm{ord}_p(\delta^{\chi}_{\mathfrak{a}_i}).\end{aligned}$$

Therefore,

$$\mathrm{ord}_p(\delta^{\chi}_{\mathfrak{a}_i}) = n_1 + ... + n_{r-i}.$$

This shows that $\delta^{\chi}_{\mathfrak{a}_i}$ generates $\mathrm{Fitt}_{i,O_\chi}(A^{\chi}_K) = (p^{n_1+\cdots+n_{r-i}})$. Hence, by Corollary 4.5 we obtain

$$I_{i,1}(\theta^{\chi}_{K_{(\mathfrak{a}_i)}}) = (\delta^{\chi}_{\mathfrak{a}_i}) = \mathrm{Fitt}_{i,O_\chi}(A^{\chi}_K).$$

Thus, we have $\mathrm{Fitt}_{i,O_\chi}(A^{\chi}_K) \subset (\Theta_{i,1,K})^{\chi} \subset (\Theta_{i,K})^{\chi}$.
Note that for $i = r$, we have got $\Theta^{\chi}_{r,K} = (1)$. Hence, $\Theta^{\chi}_{i,K} = (1)$ for all $i \geq r$, and we have $\mathrm{Fitt}_{i,O_\chi}(A^{\chi}_K) = \Theta^{\chi}_{i,K}$ for all $i \geq 0$. This completes the proof of Theorem 0.1.

A appendix

In this appendix, we determine the initial Fitting ideal of the Pontrjagin dual $(A^{\sim}_{F_\infty})^{\vee}$ (cf. §2) of the non-ω component of the p-primary component of the ideal class group as a $\mathbf{Z}_p[[\mathrm{Gal}(F_\infty/k)]]$-module for the cyclotomic $\mathbf{Z}_p$-extension F_∞ of a CM-field F such that F/k is finite and abelian, under the assumption that the Leopoldt conjecture holds for k and the μ-invariant of F vanishes. Our aim is to prove Theorem A.5. For the initial Fitting ideal of the Iwasawa module $X_{F_\infty} = \varprojlim A_{F_n}$ of F_∞, see [11] and Greither's results [3], [4].
Suppose that λ_1,...,λ_r are all finite primes of k, which are prime to p and ramifying in F_∞/k. We denote by P_{λ_i} the p-Sylow subgroup of the inertia subgroup of λ_i in $\mathrm{Gal}(F_\infty/k)$. We first assume that

$$(*) \qquad P_{\lambda_1} \times ... \times P_{\lambda_r} \subset \mathrm{Gal}(F_\infty/k).$$

(Compare this condition with the condition (A_p) in [11] §3.)
We define a set $\mathcal{H}$ of certain subgroups of $\mathrm{Gal}(F_\infty/k)$ by

$$\mathcal{H} = \{H_0 \times H_1 \times ... \times H_r \mid \begin{array}{l} H_0 \text{ is a finite subgroup of } \mathrm{Gal}(F_\infty/k) \\ \text{with order prime to } p \text{ and } H_i \text{ is} \\ \text{a subgroup of } P_{\lambda_i} \text{ for all } i\ (1 \leq i \leq r)\}.\end{array}$$

We also define

$$\mathcal{M} = \{M_\infty \mid k \subset M_\infty \subset F_\infty,\ \ M \text{ is the fixed field of some } H \in \mathcal{H}\}.$$

For an intermediate field M_∞ of F_∞/k, we denote by

$$\nu_{F_\infty/M_\infty} : \mathbf{Z}_p[[\mathrm{Gal}(M_\infty/k)]]^\sim \longrightarrow \mathbf{Z}_p[[\mathrm{Gal}(F_\infty/k)]]^\sim$$

the map induced by $\sigma \mapsto \Sigma_{\tau_{|M_\infty}=\sigma}\tau$ for $\sigma \in \mathrm{Gal}(M_\infty/k)$. We define $\Theta^\sim_{F_\infty/k}$ to be the $\mathbf{Z}_p[[\mathrm{Gal}(F_\infty/k)]]^\sim$-module generated by $\nu_{F_\infty/M_\infty}(\theta^\sim_{M_\infty})$ for all $M_\infty \in \mathcal{M}_{F_\infty/k}$.
Put $\Lambda_F = \mathbf{Z}_p[[\mathrm{Gal}(F_\infty/k)]]$. Let $\iota : \Lambda_F \longrightarrow \Lambda_F$ be the map defined by $\sigma \mapsto \sigma^{-1}$ for all $\sigma \in \mathrm{Gal}(F_\infty/k)$. For a Λ_F-module M, we denote by $M^\approx$ to be the component obtained from M^- by removing $M^{\omega^{-1}}$, namely $M^- = M^\approx \oplus M^{\omega^{-1}}$ if $\mu_p \subset F$, and $M^- = M^\approx$ otherwise (cf. 1.1). The map ι induces $M^\sim \xrightarrow{\iota} M^\approx$ which is bijective.

PROPOSITION A.1. *We assume that the μ-invariant of F vanishes. Under the assumption of* $(*)$, *we have*

$$\mathrm{Fitt}_{0,\Lambda_F}((A^\sim_{F_\infty})^\vee)^\approx = \iota(\Theta^\sim_{F_\infty/k}).$$

Proof. This can be proved by the same method as the proof of Theorem 0.9 in [11] by using a slight modification of Lemma 4.1 in [11]. In fact, instead of Corollary 5.3 in [11], we can use

LEMMA A.2. *Let L/K be a finite abelian p-extension of CM-fields. Suppose that P is a set of primes of K_∞ which are ramified in L_∞ and prime to p. For $v \in P$, e_v denotes the ramification index of v in L_∞/K_∞. Then, we have an exact sequence*

$$0 \longrightarrow A^\sim_{K_\infty} \longrightarrow (A^\sim_{L_\infty})^{\mathrm{Gal}(L_\infty/K_\infty)} \longrightarrow (\bigoplus_{v\in P} \mathbf{Z}/e_v\mathbf{Z})^\sim \longrightarrow 0$$

Proof of Lemma A.2. It is enough to prove $\hat{H}^0(L_\infty/K_\infty, A^\sim_{L_\infty}) = (\bigoplus_{v\in P}\mathbf{Z}/e_v\mathbf{Z})^\sim$. Let P'_n be the set of primes of K_n ramifying in L_n. Then, by Lemma 5.1 (ii) in [11], we have $\hat{H}^0(L_n/K_n, A^\sim_{L_n}) = (\bigoplus_{v\in P'_n} H^1(L_{n,w}/K_{n,v}, O^\times_{L_{n,w}}))^\sim = (\bigoplus_{v\in P'_n}\mathbf{Z}/e_v\mathbf{Z})^\sim$ where w is a prime of L_n above v. If v is a prime above p, it is totally ramified in K_∞ for sufficiently large n, hence we have $\varinjlim(\bigoplus_{v\in P'_n, v|p}\mathbf{Z}/e_v\mathbf{Z})^\sim = 0$. On the other hand, $\varinjlim(\bigoplus_{v\in P'_n, v\nmid p}\mathbf{Z}/e_v\mathbf{Z})^\sim = (\bigoplus_{v\in P}\mathbf{Z}/e_v\mathbf{Z})^\sim$. Thus, we get $\hat{H}^0(L_\infty/K_\infty, A^\sim_{L_\infty}) = (\bigoplus_{v\in P}\mathbf{Z}/e_v\mathbf{Z})^\sim$.

Next, we consider a general CM-field F with F/k finite and abelian. We assume that the Leopodt conjecture holds for k.

Lemma A.3. (Iwasawa) *Let λ be a prime of k not lying above p. Suppose that $k(\lambda p^{\infty})$ is the maximal abelian pro-p extension of k, unramified outside $p\lambda$. Then the ramification index of λ in $k(\lambda p^{\infty})$ is p^{n_λ} where $n_\lambda = \mathrm{ord}_p(N(\lambda)-1)$.*

In fact, Iwasawa proved that the Leopoldt conjecture implies the existence of "λ-field" ($\mathfrak{q}$-field) in his terminology ([5] Theorem 1). This means that the ramification index of λ is p^{n_λ}.

Lemma A.4. *Let F/k be a finite abelian extension such that F is a CM-field. Then, there is an abelian extension F'/k satisfying the following properties.*
(i) *$F'_\infty \supset F_\infty$, and the extension F'_∞/F_∞ is a finite abelian p-extension which is unramified outside p.*
(ii) *F'_∞ satisfies the condition $(*)$.*

Proof. This follows from Lemme 2.2 (ii) in Gras [2], but we will give here a proof. Suppose that λ_1,...,λ_r are all finite primes ramifying in F_∞/k, and prime to p. We denote by $e^{(p)}_{\lambda_i}$ the p-component of the ramification index of λ_i in F_∞. By class field theory, $e^{(p)}_{\lambda_i} \leq p^{n_{\lambda_i}}$. We take a subfield k_i of $k(\lambda_i p^{\infty})$ such that k_i/k is a p-extension, and the ramification index of k_i/k is $e^{(p)}_{\lambda_i}$. This is possible by Lemma A.3. Take F' such that $F'_\infty = F_\infty k_1 ... k_r$. It is clear that F' satisfies the condition (i). Since $k_1...k_r \subset F'_\infty$, F' satisfies the condition $(*)$.

We define $\iota(\Theta^{\sim}_{F_\infty/k})$ by $\iota(\Theta^{\sim}_{F_\infty/k}) = c_{F'_\infty/F_\infty}(\iota(\Theta^{\sim}_{F'_\infty/k}))$ where $c_{F'_\infty/F_\infty} : \Lambda_{F'} \longrightarrow \Lambda_F$ is the restriction map. This $\iota(\Theta^{\sim}_{F_\infty/k})$ does not depend on the choice of F'. In fact, we have

Theorem A.5. *We assume the Leopoldt conjecture for k and the vanishing of the μ-invariant of F. Then, we have*

$$\mathrm{Fitt}_{0,\Lambda_F}((A^{\sim}_{F_\infty})^{\vee})^{\approx} = \iota(\Theta^{\sim}_{F_\infty/k}).$$

Proof. We take F' as in Lemma A.4. By Proposition A.1, Theorem A.5 holds for F'_∞. Since F'_∞/F_∞ is unramified outside p, by Lemma A.2 the natural map $A^{\sim}_{F_\infty} \longrightarrow (A^{\sim}_{F'_\infty})^{\mathrm{Gal}(F'_\infty/F_\infty)}$ is an isomorphism. Hence, we get

$$\begin{aligned}\mathrm{Fitt}_{0,\Lambda_F}((A^{\sim}_{F_\infty})^{\vee})^{\approx} &= c_{F'_\infty/F_\infty}(\mathrm{Fitt}_{0,\Lambda_{F'}}((A^{\sim}_{F'_\infty})^{\vee})^{\approx}) = c_{F'_\infty/F_\infty}(\iota(\Theta^{\sim}_{F'_\infty/k})) \\ &= \iota(\Theta^{\sim}_{F_\infty/k}).\end{aligned}$$

This completes the proof of Theorem A.5.

References

[1] Deligne, P. and Ribet, K., Values of abelian L-functions at negative integers over totally real fields, Invent. math. 59 (1980), 227-286.

[2] Gras, G., Théorie des genres analytique des fonctions L p-adiques des corps totalement réels, Invent. math. 86 (1986), 1-17.

[3] Greither C., Some cases of Brumer's conjecture for abelian CM extensions of totally real fields, Math. Zeitschrift 233 (2000), 515-534.

[4] Greither, C., Computing Fitting ideals of Iwasawa modules, preprint.

[5] Iwasawa, K., On $\mathbf{Z}_l$-extensions of algebraic number fields, Ann. of Math. 98 (1973), 246-326.

[6] Iwasawa, K., On the μ-invariants of $\mathbf{Z}_l$-extensions, *Number Theory, Algebraic Geometry and Commutative Algebra, in honor of Yasuo Akizuki*, Kinokuniya, Tokyo 1973, 1-11.

[7] Iwasawa, K., A simple remark on Leopoldt's conjecture, Kenkichi Iwasawa Collected Papers, Vol II, Springer-Verlag Tokyo 2001, 862-870.

[8] Kato, K., Euler systems, Iwasawa theory, and Selmer groups, Kodai Math. J. 22 (1999), 313-372.

[9] Kato, K., p-adic Hodge theory and values of zeta functions of modular forms, preprint

[10] Kolyvagin, V.A., Euler systems, The Grothendieck Festschrift Vol II (1990), 435-483.

[11] Kurihara, M., Iwasawa theory and Fitting ideals, J. reine angew. Math. 561 (2003), 39-86.

[12] Mazur, B. and Wiles, A., Class fields of abelian extensions of Q, Invent. math. 76 (1984), 179-330.

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

[14] Perrin-Riou, B., Systèmes d'Euler p-adiques et théorie d'Iwasawa, Ann. Inst. Fourier 48 (1998) 1231-1307.

[15] Popescu, C.D., Stark's question and a strong form of Brumer's conjecture, preprint.

[16] Rubin, K., The main conjecture, Appendix to *Cyclotomic Fields I and II* by S. Lang, Graduate Texts in Math. 121, Springer-Verlag 1990, 397-419.

[17] Rubin, K., Kolyvagin's system of Gauss sums, *Arithmetic Algebraic Geometry*, G. van der Geer et al eds, Progress in Math 89, Birkhäuser 1991, 309-324.

[18] Rubin, K., *Euler systems*, Annals of Math. Studies 147, Princeton Univ. Press 2000.

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

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

[21] Siegel, C. R., Über die Fourierschen Koeffizienten von Modulformen, Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II 1970, 15-56.

[22] Solomon, D., On the classgroups of imaginary abelian fields, Ann. Inst. Fourier, Grenoble 40-3 (1990), 467-492.

[23] Tate J., *Les conjectures de Stark sur les Fonctions L d'Artin en* $s = 0$, Progress in Math. 47, Birkhäuser 1984.

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

[25] Wiles, A., The Iwasawa conjecture for totally real fields, Ann. of Math. 131 (1990), 493-540.

[26] Wiles, A., On a conjecture of Brumer, Ann. of Math. 131 (1990), 555-565.

Masato Kurihara
Department of Mathematics
Tokyo Metropolitan University
Hachioji, Tokyo, 192-0397
Japan
kurihara@math.metro-u.ac.jp