J. reine angew. Math. **561** (2003), 39—86

Journal für die reine und
angewandte Mathematik
© Walter de Gruyter
Berlin · New York 2003

Iwasawa theory and Fitting ideals

By *Masato Kurihara* at Tokyo

Abstract. By studying the Fitting ideals of the minus parts of the ideal class groups of CM fields, we give a more precise relationship than the usual main conjecture between the analytic side and the algebraic side. In particular, for the cyclotomic $\mathbb{Z}_p$-extension F_∞ of an abelian field F, we determine the initial Fitting ideal of the minus part of the Galois group of the maximal unramified abelian pro-p-extension of F_∞ over F_∞ as a $\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/\mathbb{Q})]]$-module. We also study the Fitting ideals of the Selmer groups of an elliptic curve and certain Galois cohomology groups.

0. Introduction

Iwasawa theory studies a relationship between arithmetic objects and special values of the zeta functions. Their relationship is usually stated as a main conjecture which claims that the p-adic L-function defined p-adic analytically gives a characteristic power series of the arithmetic object. In this paper, we show that we can get more information on the arithmetic object than the characteristic power series by studying p-adic analytic zeta functions, namely p-adic measures on the Galois groups of abelian extensions of the ground field.

Our main tools are Fitting ideals (for the definition, cf. 1.1). In this paper, first of all, we study the initial Fitting ideals of ideal class groups. Let $F/\mathbb{Q}$ be an imaginary abelian extension of finite degree, and Cl_F the ideal class group of F. In this paper, we neglect the 2-primary part and only consider $Cl'_F = Cl_F \otimes \mathbb{Z}'$ where $\mathbb{Z}' = \mathbb{Z}[1/2]$. We regard Cl'_F as a $\mathbb{Z}'[\mathrm{Gal}(F/\mathbb{Q})]$-module. Note that every $\mathbb{Z}'[\mathrm{Gal}(F/\mathbb{Q})]$-module M is decomposed into $M = M^+ \oplus M^-$ where M^+ (resp. M^-) means the part on which the complex conjugation acts as 1 (resp. -1). We will study the minus part of the initial Fitting ideal

$$\mathrm{Fitt}_{0,\mathbb{Z}'[\mathrm{Gal}(F/\mathbb{Q})]}(Cl'_F)^- = \mathrm{Fitt}_{0,\mathbb{Z}'[\mathrm{Gal}(F/\mathbb{Q})]}\big((Cl'_F)^-\big)^- \subset \mathbb{Z}'[\mathrm{Gal}(F/\mathbb{Q})]^-.$$

In general, for an R-module M, the Fitting ideals $\mathrm{Fitt}_{i,R}(M)$ give information on the structure of the R-module M (cf. 1.1). In §2 we will define the Stickelberger ideal $\Theta_{F/\mathbb{Q}} \subset \mathbb{Z}'[\mathrm{Gal}(F/\mathbb{Q})]$, which is essentially generated by the Stickelberger elements of abelian fields. (For a cyclotomic field $F = \mathbb{Q}(\mu_m)$, our $\Theta^-_{F/\mathbb{Q}}$ coincides with Sinnott's Stickelberger ideal [39], but for an abelian field our ideal is slightly different from Sinnott's Stickelberger ideal [40], in general.) We first propose

Conjecture 0.1. $\mathrm{Fitt}_{0,\mathbb{Z}'[\mathrm{Gal}(F/\mathbb{Q})]}(Cl'_F)^- = \Theta^-_{F/\mathbb{Q}}$.

Remark 0.2. (1) The left hand side of Conjecture 0.1 is an algebraic object and the right hand side is an analytic object (in the sense that the Stickelberger elements are related to the zeta functions). So this conjecture gives a relationship between the algebraic side and the analytic side. Conjecture 0.1's for all n-th layers of the cyclotomic $\mathbb{Z}_p$-extension F_∞/F formally imply the usual Iwasawa main conjecture for F_∞ and an odd Dirichlet character (for an odd prime p). We will also see that this conjecture contains more information than the usual Iwasawa main conjecture, so this is a refinement of the usual Iwasawa main conjecture.

(2) Stickelberger's theorem implies that $\Theta_{F/\mathbb{Q}} \subset \mathrm{Ann}_{\mathbb{Z}'[\mathrm{Gal}(F/\mathbb{Q})]}(Cl'_F)$ where $\mathrm{Ann}_{\mathbb{Z}'[\mathrm{Gal}(F/\mathbb{Q})]}(Cl'_F)$ is the annihilator of $\mathbb{Z}'[\mathrm{Gal}(F/\mathbb{Q})]$-module Cl'_F. In general, the Fitting ideal is contained in the annihilator, so the above conjecture may also be regarded as a refinement of Stickelberger's theorem for the minus part of the ideal class groups.

(3) The minus component Cl_F^- is usually defined to be the cokernel of the natural map $Cl_{F^+} \to Cl_F$ where F^+ is the maximal real subfield of F. Mazur and Wiles in [26] posed the problem to determine the initial Fitting ideal $\mathrm{Fitt}_{0,\mathbb{Z}[\mathrm{Gal}(F/\mathbb{Q})]}(Cl_F^-)$ of Cl_F^- completely. If Conjecture 0.1 is true, it would give an answer to their problem except 2-primary component because $\left(\mathrm{Fitt}_{0,\mathbb{Z}[\mathrm{Gal}(F/\mathbb{Q})]}(Cl_F^-) \otimes \mathbb{Z}'\right)^- = \mathrm{Fitt}_{0,\mathbb{Z}'[\mathrm{Gal}(F/\mathbb{Q})]}(Cl'_F)^-$.

(4) After the first version of this paper was circulated, I was informed of several people's works on the Fitting ideals of ideal class groups and some cohomology groups. I would like to thank heartily D. Burns, C. Greither, T. Nguyen Quang Do, C. Popescu, J. Ritter, V. Snaith, and A. Weiss for giving me some comments. In [13], Greither determined the Fitting ideal of Cl_F^- under the assumption that F is "admissible" in the sense of [13]. This condition "admissibility" was improved in [14] to "niceness". For a CM field F over a totally real field k such that F/k is finite abelian and "nice" in the sense of [14], Greither determined the Fitting ideal of Cl'_F (by using the Stickelberger element of F). For example, $\mathbb{Q}(\mu_{p^n})/\mathbb{Q}$ (with some prime p) is nice, and Greither's result in [14] says that Conjecture 0.1 is true for $F = \mathbb{Q}(\mu_{p^n})$. A key point is that if F/k is nice, the Fitting ideal of $(Cl_F \otimes \mathbb{Z}_p)^-$ over $\mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})]$ is locally principal for all odd p (cf. also Schoof [35]). But in Conjecture 0.1, we are dealing with *general F*, and one of our difficulties lies in treating the Fitting ideal which is not principal. (In §8 we need essentially the general case to investigate the higher Fitting ideals.) For the Fitting ideals of class groups of real abelian fields, see also Cornacchia and Greither [8]. Ritter and Weiss established a refinement of the Iwasawa main conjecture from a different point of view (cf. Remark 0.11 (2)).

Fitting ideals are elementary objects, and our conjecture has the advantage to get information on ideal class groups more directly than other "main conjectures" which are formulated by using some techniques of homological algebra (for example, equivariant Tamagawa Number conjecture cf. [18] and [1]). It would be interesting to find beautiful relations between natural objects rather than modifications of the objects. (We also remark that Burns and Greither [2] recently determined the Fitting ideal of certain cohomology groups, using the equivariant Tamagawa Number conjecture proved in [1].)

Note that the ideal $\mathrm{Fitt}_{0,\mathbb{Z}'[\mathrm{Gal}(F/\mathbb{Q})]}(Cl'_F)^-$ is determined if we determine the ideals $\mathrm{Fitt}_{0,\mathbb{Z}'[\mathrm{Gal}(F/\mathbb{Q})]}(Cl'_F)^- \otimes \mathbb{Z}_p = \mathrm{Fitt}_{0,\mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})]}(Cl_F \otimes \mathbb{Z}_p)^- \subset \mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})]^-$ for all odd prime numbers p. So Conjecture 0.1 is equivalent to the following Conjecture 0.3 for all odd p.

Conjecture 0.3. *Let p be an odd prime. Then we have*

$$\mathrm{Fitt}_{0,\mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})]}(Cl_F \otimes \mathbb{Z}_p)^- = (\Theta_{F/\mathbb{Q}} \otimes \mathbb{Z}_p)^-.$$

In several cases we can verify this conjecture easily. For example, suppose that p does not divide the class number of F. Then, Conjecture 0.3 is trivial because both sides of the formula are equal to $\mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})]$. (For the right hand side, this follows from the analytic class number formula, cf. [39], [40].)

Next, consider the case that the degree $[F:\mathbb{Q}]$ is prime to p. Then, $\mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})]$ is a product of discrete valuation rings, and the conjecture just claims that every component of the ideal class group has the right order. This was proved by Mazur and Wiles [26], §10, Theorem 2 in Chap. 1 as a corollary of the Iwasawa main conjecture, so Conjecture 0.3 holds in this case.

Let us call the case $p \mid [F:\mathbb{Q}]$ "non-trivial" case. We proceed to the non-trivial cases.

Theorem 0.4. *Assume that no prime of F^+ above p splits in F/F^+. Then Conjecture* 0.3 *holds.*

Theorem 0.5. *Suppose that K is an abelian field such that the degree $[K:\mathbb{Q}]$ is prime to p, and K_n is the n-th layer of the cyclotomic $\mathbb{Z}_p$-extension K_∞/K for some $n > 0$. Then Conjecture* 0.3 *holds for $F = K_n$.*

Theorem 0.6. *Suppose that p is tamely ramified in $F/\mathbb{Q}$, and F does not contain a primitive p-th root of unity. Then Conjecture* 0.3 *holds.*

Combining Theorems 0.5 and 0.6, we obtain

Corollary 0.7. *Suppose that $K/\mathbb{Q}$ is a finite abelian extension such that every odd prime dividing $[K:\mathbb{Q}]$ is unramified in $K/\mathbb{Q}$. We take an odd prime p which does not divide $[K:\mathbb{Q}]$. Then, for $n \geqq 0$, Conjecture* 0.1 *is true for $F = K(\mu_{p^n})$.*

This corollary is a generalization of a result of Greither that Conjecture 0.1 is true for $F = \mathbb{Q}(\mu_{p^n})$.

These theorems are obtained by consideration of cyclotomic $\mathbb{Z}_p$-extensions. We fix an odd prime number p, and for a general number field F we denote by F_∞/F the cyclotomic $\mathbb{Z}_p$-extension. We consider the p-primary component A_{F_n} of Cl_{F_n} for the n-th layer F_n, and define

$$X_{F_\infty} = \varprojlim A_{F_n}$$

where the projective limit is taken with respect to the norm maps.

Let k be a totally real number field, and F be a CM field such that F/k is a finite abelian extension. We regard X_{F_∞} as a $\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/k)]]$-module and study its Fitting ideal. We assume F satisfies the conditions in the subsection 3.2 in §3, namely the existence of the auxiliary field F' as in 3.2 for F and the Leopoldt conjecture for k. In §3, we will define the Stickelberger ideal $\Theta_{F_\infty/k}$ of $\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/k)]]$.

Conjecture 0.8. *For F satisfying the conditions in* 3.2, *we have*

$$\mathrm{Fitt}_{0,\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/k)]]}(X_{F_\infty})^- = (\Theta_{F_\infty/k})^-.$$

Theorem 0.9. *For F satisfying the conditions in* 3.2, *we assume that the Iwasawa μ invariant of F_∞ vanishes, namely X_{F_∞} is a finitely generated $\mathbb{Z}_p$-module. Then, Conjecture* 0.8 *is true.*

If $k = \mathbb{Q}$, the conditions in 3.2 are satisfied (F' always exists for F), hence, from Theorem 0.9 we obtain (we give the proof in §6)

Corollary 0.10. *For any finite abelian extension $F/\mathbb{Q}$ and any odd p, we have*

$$\mathrm{Fitt}_{0,\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/\mathbb{Q})]]}(X_{F_\infty})^- = \Theta^-_{F_\infty/\mathbb{Q}}.$$

Remark 0.11. (1) The Leopoldt conjecture is needed only for studying the Teichmüller character component of X_{F_∞} in the proof of Theorem 0.9 (more precisely, see Remark 6.1 in §6). In this paper, our interest is mainly in the abelian fields over $\mathbb{Q}$, and we assumed in Conjecture 0.8 and Theorem 0.9 the strong conditions in 3.2. In our forthcoming paper [24], we study general CM fields without assuming the existence of F' (but study the dual of the ideal class groups). In a very recent preprint [15], Greither studied the Fitting ideals of the Iwasawa modules of CM fields satisfying a weak assumption without assuming the existence of F'.

(2) Theorem 0.9 may also be regarded as a refinement of the usual Iwasawa main conjecture (cf. Remark 3.6). We remark that Ritter and Weiss also obtained a different refinement of the usual Iwasawa main conjecture, which they call "equivariant Iwasawa theory" [30], [31]. An essential difference is that they consider the plus part $\mathscr{X}_S^+$ of the Galois group of the maximal abelian pro-p-extension of F_∞ which is unramified outside S over F_∞ where S is a set of primes which contains *ramifying primes* in F_∞/k. On the other hand, our interest is in X_{F_∞} which is the Galois group of the maximal *unramified* abelian pro-p-extension of F_∞. Nguyen Quang Do informed me that he recently succeeded to compute the Fitting ideal of a certain module related to $\mathscr{X}_S^+$ by using the result of Ritter and Weiss [27].

(3) C. Popescu found an example of a finite abelian extension of function fields such that the Stickelberger element (times an annihilator of the group of roots of unity) *does not* belong to the Fitting ideal of the class group [29]. For cyclotomic $\mathbb{Z}_p$-extensions of number fields, we can also construct a finite abelian field F/k such that the Stickelberger element of F_∞ (times an annihilator of the group of roots of unity) does not belong to the Fitting ideal of X_{F_∞} if we remove the assumption in Conjecture 0.8 (if F_∞/k_∞ is wildly ramified at a prime above p). We hope to come back to this point in our forthcoming paper.

These results on the initial Fitting ideals yield information on the higher Fitting ideals. In §8 we study the higher Fitting ideals of ideal class groups. From the Stickelberger elements we can define some elements $\delta_{i_1,\dots,i_r}(x)$ which we will show belong to the higher Fitting ideal (Theorem 8.1). We propose Conjecture 8.2 which claims that under certain hypotheses, the higher Fitting ideals of $X^-_{F_\infty}$ would be generated by the Stickelberger ideal and these elements $\delta_{i_1,\dots,i_r}(x)$. These elements have relation with the argument of the Euler system for number fields of finite degree. For example, for $F = \mathbb{Q}(\mu_p)$ Rubin and Kolyvagin determined the structure of $A^{-}_{\mathbb{Q}(\mu_p)}$ by using the Euler system of Gauss sums [32], and if we state their theorem by using Fitting ideals, it says that the higher Fitting ideals of $A^{-}_{\mathbb{Q}(\mu_p)}$ are generated by the Stickelberger ideal and the elements $\delta_{1,\dots,1}(x)$. In Theorem 8.4, we prove Conjecture 8.2 for the 1-st Fitting ideal $\mathrm{Fitt}_{1,\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/\mathbb{Q})]]}(X_{F_\infty})$. The argument of this section will be used in [24] to determine the structure of the ideal class groups of certain CM fields.

In §9 we study the case $\lambda = 2$. More precisely, for an odd Dirichlet character χ of $\mathrm{Gal}(F/\mathbb{Q})$, we consider the χ-quotient $X^{\chi}_{F_\infty}$ (cf. 1.3) which we assume to be a free $\mathbb{Z}_p[\mathrm{Image}\,\chi]$-module of rank 2. Then, we show that the isomorphism class of $X^{\chi}_{F_\infty}$ as a $\mathbb{Z}_p[\chi][[\mathrm{Gal}(F_\infty/F)]]$-module is determined completely by the Stickelberger elements, by using the initial Fitting ideal and the 1-st Fitting ideal (see the explanation after Corollary 9.3). This also means that the isomorphism class can be determined easily by numerical computation.

Our method can be applied for more general arithmetic objects. In §10 we study the Selmer group of an elliptic curve. For an elliptic curve E defined over $\mathbb{Q}$, Mazur and Tate [25] defined the modular element θ^{E}_{F} for an abelian field F. They conjectured the modular element is in the Fitting ideal of the Pontrjagin dual of the Selmer group ([25], Conjecture 3). We take a prime p at which E has good ordinary reduction, and consider the Pontrjagin dual $\mathrm{Sel}(E/F_\infty)^{\vee}$ of the p-primary part of the Selmer group over the cyclotomic $\mathbb{Z}_p$-extension F_∞. We define an ideal $\Theta_{F_\infty,E}$ of $\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/\mathbb{Q})]]$ which is essentially generated by the modular elements. We conjecture that it is equal to the Fitting ideal of $\mathrm{Sel}(E/F_\infty)^{\vee}$ under certain hypotheses (Conjecture 10.1). Using Kato's theorem [19], we will show $\Theta_{F_\infty,E}$ is in the Fitting ideal of $\mathrm{Sel}(E/F_\infty)^{\vee}$ (see Theorem 10.2 and Corollary 10.3). Theorem 10.2 implies some results on the higher Fitting ideals (cf. Corollary 10.4 and Remark 10.5) which are similar to Theorem 8.1.

Even if E has supersingular reduction at p, we conjecture that the Fitting ideal of $\mathrm{Sel}(E/F)^{\vee}$ is essentially generated by the modular elements (cf. [23], Conjecture 0.3). This is related to the asymptotic behaviour of the order of the p-primary torsion part of $\mathrm{Sel}(E/F_n)^{\vee}$ as $n \to \infty$.

In §12, for a totally real number field F and a positive even integer r, we consider the etale cohomology group $H^2(O_F[1/p], \mathbb{Z}_p(r))$ (which is isomorphic to $H^2(G_{F,p}, \mathbb{Z}_p(r))$ where $G_{F,p}$ is the Galois group of the maximal extension of F unramified outside p over F). We will show under a certain assumption that the twisted Stickelberger elements are not only in the annihilator of the cohomology group, but also in its Fitting ideal. (By a well-known and easily proved fact, the Fitting ideal is in the annihilator, in general.) If $F/\mathbb{Q}$ is a finite abelian extension and F is real, we will determine $\mathrm{Fitt}_{\mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})]}(H^2(O_F[1/p], \mathbb{Z}_p(r))$ completely. We will show that it is essentially generated by twisted Stickelberger elements (Corollary 12.4). In particular, we will show an element $S_r(b) \in \mathbb{Z}[\mathrm{Gal}(F/\mathbb{Q})]$ defined by Coates and Sinnott [5] is in the Fitting ideal of $H^2(O_F[1/p], \mathbb{Z}_p(r))$ (Corollary 12.5). This is a refinement of Conjecture 1 of Coates and Sinnott [5]. More generally, for a totally real number field F and a subfield k such that F/k is abelian and satisfies the conditions in the subsection 3.2, we will define the twisted Stickelberger ideal $(\Theta_{F_\infty/k}(1-r))^{(p)} \subset \mathbb{Z}_p[[\mathrm{Gal}(F_\infty/k)]]$ for the cyclotomic $\mathbb{Z}_p$-extension F_∞, and will show that it is equal to the Fitting ideal of $\mathbb{H}^2(O_{F_\infty}[1/p], \mathbb{Z}_p(r)) = \varprojlim H^2(O_{F_n}[1/p], \mathbb{Z}_p(r))$ under certain hypotheses (see Theorem 12.2 and Corollary 12.3).

For the Fitting ideals of cohomology groups, many results have been obtained by various authors. Cornacchia and Østvær determined in [7] the Fitting ideal of $H^2(O_F[1/p], \mathbb{Z}_p(r))$ for F with prime power conductor, and proved a refinement of Coates and Sinnott conjecture for such a special F. V. Snaith [41] recently proved an interesting relation between the Fitting ideal of $H^2(O_F[1/S], \mathbb{Z}_p(r))$ and the twisted Stickelberger elements where S is a set of primes which contains ramifying primes in F and primes above p, and $O_F[1/S]$ denotes the ring of S-integers. Snaith's approach is completely different from ours, and interesting. After that, Burns and Greither proved in [2] a very beautiful result, using the equivariant Tamagawa number conjecture (cf. [1]). Their result is more precise than the above relation by Snaith. Especially, they determined the Fitting ideal of $H^2(O_F[1/S], \mathbb{Z}_p(r))$ completely. Their result also implies Corollary 12.5 in the case $F/\mathbb{Q}$ in cyclic by a different method from that in this paper. An essential difference is that we are dealing with the Fitting ideal of $H^2(O_F[1/p], \mathbb{Z}_p(r))$ directly, which is generated by several (twisted) Stickelberger elements not only of F but also of some abelian fields (cf. Theorem 12.2 and Corollary 12.4), while Burns and Greither studied the Fitting ideal of $H^2(O_F[1/S], \mathbb{Z}_p(r))$ which they showed is generated by the (twisted) Stickelberger element of F (times the annihilators of H^1). Nguyen Quang Do also announced to compute the Fitting ideal of $H^2(O_F[1/S], \mathbb{Z}_p(r))$ recently [27], using the result of Ritter and Weiss.

I would like to express my sincere gratitude to late Professor Iwasawa for his interest in this work. A part of this work was done during my stay in Harvard University in 1992. I would like to thank B. Mazur heartily for valuable discussion. I would also like to thank J. Coates heartily for giving me a comment on the Stickelberger ideal of Iwasawa and Sinnott. I also thank very much D. Burns, C. Greither, T. Nguyen Quang Do, C. Popescu, J. Ritter, V. Snaith, and A. Weiss who gave me some information and helpful comments after the first version of this paper was circulated. I especially thank C. Greither for sending me his recent preprint [2] with Burns, and also for his paper [14] from which I learned the argument avoiding the trivial zeros.

Notation. For an abelian group A and an integer n, $A[n]$ (resp. A/n) denotes the kernel (resp. cokernel) of the multiplication by n. For a positive integer n, μ_n denotes the group of all n-th roots of unity. For a number field or a local field F, O_F denotes the ring of integers. For a group G and a G-module M, we denote by M^G the G-invariant part of M (the maximal subgroup of M on which G acts trivially), and by M_G the G-coinvariant of M (the maximal quotient of M on which G acts trivially).

1. Preliminaries

1.1. For a commutative ring R and an R-module M such that

$$R^m \xrightarrow{f} R^n \to M \to 0$$

is an exact sequence of R-modules (where m and n are positive integers), Fitting ideals are defined as follows. For an integer $i \geqq 0$ the i-th Fitting ideal of M is defined to be the ideal of R generated by all $(n-i) \times (n-i)$ minors of the matrix corresponding to f. (If $i \geqq n$, it is defined to be R.) This definition depends only on M and does not depend on the choice of the above exact sequence. We denote the i-th Fitting ideal of M over R by $\mathrm{Fitt}_{i,R}(M)$. So we have a sequence of ideals

$$\mathrm{Fitt}_{0,R}(M) \subset \mathrm{Fitt}_{1,R}(M) \subset \cdots \subset \mathrm{Fitt}_{n,R}(M) = \mathrm{Fitt}_{n+1,R}(M) = \cdots = R.$$

These ideals reflect the structure of M as an R-module. For example, assume that R is a principal ideal domain and M is a finitely generated torsion R-module. Suppose

$$M \simeq R/(a_1) \oplus \cdots \oplus R/(a_r)$$

with $(a_1) \supset (a_2) \supset \cdots \supset (a_r)$. Then we have $\mathrm{Fitt}_{i,R}(M) = (a_1 \cdot \ldots \cdot a_{r-i})$. So determining the Fitting ideals of M is equivalent to determining the structure of M in this case. Another example is $\Lambda = R[[T]]$ where R is a complete discrete valuation ring. Let M be a finitely generated torsion Λ-module such that M does not contain a nonzero Λ-submodule with finite length as an R-module. (For example, suppose M is free of finite rank as an R-module.) Then, $\mathrm{Fitt}_{0,\Lambda}(M)$ is equal to the characteristic ideal of M, namely the ideal generated by a characteristic power series (cf. [26], Appendix).

1.2. Let k be a base field. For a finite abelian extension F/k and an intermediate field M such that $k \subset M \subset F$, we consider the canonical homomorphism $\mathrm{Gal}(F/k) \to \mathrm{Gal}(M/k)$ defined by $\sigma \mapsto \sigma_{|M}$. For a ring R, we denote by

$$c_{F/M} : R[\mathrm{Gal}(F/k)] \to R[\mathrm{Gal}(M/k)]$$

the induced homomorphism on the group rings. In this situation,

$$v_{F/M} : R[\mathrm{Gal}(M/k)] \to R[\mathrm{Gal}(F/k)]$$

denotes the homomorphism defined by

$$\sigma \mapsto \sum_{c_{F/M}(\tau)=\sigma} \tau$$

for $\sigma \in \mathrm{Gal}(M/k)$ where τ ranges over elements of $\mathrm{Gal}(F/k)$ such that $c_{F/M}(\tau) = \sigma$. ($c_{F/M}$ (resp. $v_{F/M}$) is sometimes called the restriction (resp. corestriction) map.)

1.3. Let G be a finite abelian group, and p be a prime number. We consider a (p-adic) character (homomorphism)

$$\chi : G \to \overline{\mathbb{Q}_p}^{\times}.$$

We define $\mathbb{Z}_p[\chi] = \mathbb{Z}_p[\mathrm{Image}(\chi)]$, and define $\mathbb{Z}_p[\chi]_{(G)}$ to be the $\mathbb{Z}_p[G]$-module which is $\mathbb{Z}_p[\chi]$ as a $\mathbb{Z}_p$-module, and on which G acts via χ, namely $\sigma \cdot x = \chi(\sigma)x$ for $\sigma \in G$ and $x \in \mathbb{Z}_p[\chi]_{(G)}$. For any $\mathbb{Z}_p[G]$-module M, we define the χ-quotient of M by

$$M^{\chi}_{(G)} = M \otimes_{\mathbb{Z}_p[G]} \mathbb{Z}_p[\chi]_{(G)}.$$

We simply write M^{χ} for $M^{\chi}_{(G)}$ in the case no confusion arises. For an element x of M, the image of $x \otimes 1$ in M^{χ} is denoted by x^{χ}.

Suppose that G is an abelian group such that $G = H \times H'$, and M is a $\mathbb{Z}_p[G]$-module. For a character χ of H, we often regard $M^{\chi}_{(H)}$ as a $\mathbb{Z}_p[\chi][H']$-module. If we regard χ as a character of G, $M^{\chi}_{(G)}$ is also defined, but it is not equal to $M^{\chi}_{(H)}$.

1.4. Suppose that Δ is a finite abelian group whose order is prime to p. Then, the group ring $\mathbb{Z}_p[\Delta]$ is semi-local, and isomorphic to a product of discrete valuation rings. More explicitly, it is described as follows. Let $\hat{\Delta}$ be the group of $\overline{\mathbb{Q}_p}^{\times}$-valued characters of Δ. We say two characters χ_1 and χ_2 are $\mathbb{Q}_p$-conjugate if $\sigma\chi_1 = \chi_2$ for some $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$. We consider this equivalence relation on $\hat{\Delta}$. Then,

$$\mathbb{Z}_p[\Delta] \simeq \bigoplus_{\chi} \mathbb{Z}_p[\chi]_{(\Delta)}$$

where the sum is taken over the equivalence classes of $\hat{\Delta}$, and we choose a character χ from each equivalence class.

Let G be a finite abelian group. We write $G = \Delta \times P$ where P is a p-group and the order of Δ is prime to p. By using the above decomposition of $\mathbb{Z}_p[\Delta]$, we have

$$\mathbb{Z}_p[G] = \mathbb{Z}_p[\Delta][P] \simeq \bigoplus_{\chi} \mathbb{Z}_p[\chi]_{(\Delta)}[P].$$

2. Stickelberger ideals

In this section, we consider the analytic side. We study the Stickelberger elements, and define the Stickelberger ideal for a certain CM field.

Let k be a totally real number field, and F/k be a finite abelian extension. We define in the usual way the partial zeta function for $\sigma \in \mathrm{Gal}(F/k)$ by

$$\zeta(s, \sigma) = \sum_{(\mathfrak{a}, F/k) = \sigma} N(\mathfrak{a})^{-s}$$

for $\mathrm{Re}(s) > 1$ where the sum is taken over integral ideals $\mathfrak{a}$ of k which are prime to the conductor ideal $\mathfrak{f}_{F/k}$ such that the Artin symbol $(\mathfrak{a}, F/k)$ is equal to σ ($N(\mathfrak{a})$ is the norm of $\mathfrak{a}$). The partial zeta functions are meromorphically continued to the whole complex plane, and holomorphic except $s = 1$. We define

$$\theta_{F/k}(s) = \sum_{\sigma \in \mathrm{Gal}(F/k)} \zeta(s, \sigma)\sigma^{-1}.$$

So for $s \in \mathbb{C}\backslash\{1\}$, $\theta_{F/k}(s) \in \mathbb{C}[\mathrm{Gal}(F/k)]$ can be defined. We have

$$\theta_{F/k}(s) = \prod_{v \nmid \mathfrak{f}_{F/k}} \left(1 - \varphi_v^{-1} N(v)^{-s}\right)^{-1} \quad \text{for } \mathrm{Re}(s) > 1$$

where v ranges over prime ideals of k which are prime to $\mathfrak{f}_{F/k}$, and φ_v is the Frobenius at v in $\mathrm{Gal}(F/k)$ (Tate [45], Proposition 1.6, p. 86). By Klingen and Siegel, we know that $\theta_{F/k}(0)$ is in $\mathbb{Q}[\mathrm{Gal}(F/k)]$. We simply write θ_F for $\theta_{F/k}(0)$.

By the Euler product of θ_F as above, we have (cf. Tate [45], p. 86)

Lemma 2.1. *Assume that F/k is a finite abelian extension and M is a field such that $k \subset M \subset F$. We denote by S_F (resp. S_M) the set of finite primes of k ramifying in F/k (resp. M/k). Let*

$$c_{F/M} : \mathbb{Q}[\mathrm{Gal}(F/k)] \to \mathbb{Q}[\mathrm{Gal}(M/k)]$$

denote the natural homomorphism. Then we have

$$c_{F/M}(\theta_F) = \Big(\prod_{v \in S_F \setminus S_M} (1 - \varphi_v^{-1})\Big)\theta_M$$

where φ_v is the Frobenius of v in $\mathrm{Gal}(M/k)$.

Next, we define the Stickelberger ideal under a certain hypothesis. Let $\mathscr{L}_1, \dots, \mathscr{L}_r$ be all finite primes of k ramifying in F/k. We denote by $I_{\mathscr{L}_i}$ the inertia subgroup of $\mathscr{L}_i$ in $\mathrm{Gal}(F/k)$. We assume that

$$\text{(A)} \qquad \mathrm{Gal}(F/k) = I_{\mathscr{L}_1} \times \cdots \times I_{\mathscr{L}_r}.$$

A typical example is $k = \mathbb{Q}$ and $F = \mathbb{Q}(\mu_m)$. In fact, when we write $m = \ell_1^{e_1} \cdot \ldots \cdot \ell_r^{e_r}$, we have

$$\mathrm{Gal}\big(\mathbb{Q}(\mu_m)/\mathbb{Q}\big) = (\mathbb{Z}/m\mathbb{Z})^\times = (\mathbb{Z}/\ell_1^{e_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/\ell_r^{e_r}\mathbb{Z})^\times.$$

We define a set $\mathscr{H}_{F/k}$ of certain subgroups of $\mathrm{Gal}(F/k)$ by

$$\mathscr{H}_{F/k} = \{H_1 \times \cdots \times H_r \mid H_i \text{ is a subgroup of } I_{\mathscr{L}_i} \text{ for all } i \text{ such that } 1 \leqq i \leqq r\}.$$

We also define

$$\mathscr{M}_{F/k} = \{M \mid k \subset M \subset F, M \text{ is the fixed field of some } H \in \mathscr{H}_{F/k}\}.$$

For an intermediate field M of F/k, let

$$c_{F/M} : \mathbb{Q}[\mathrm{Gal}(F/k)] \to \mathbb{Q}[\mathrm{Gal}(M/k)]$$

and

$$\nu_{F/M} : \mathbb{Q}[\mathrm{Gal}(M/k)] \to \mathbb{Q}[\mathrm{Gal}(F/k)]$$

be as in 1.2. In this paper, we neglect the 2-primary component of ideal class groups. We put $\mathbb{Z}' = \mathbb{Z}[1/2]$. We define a $\mathbb{Z}'[\mathrm{Gal}(F/k)]$-module $\Theta'_{F/k}$ in $\mathbb{Q}[\mathrm{Gal}(F/k)]$ to be the $\mathbb{Z}'[\mathrm{Gal}(F/k)]$-module generated by $\nu_{F/M}(\theta_M)$ for all $M \in \mathscr{M}_{F/k}$, namely

$$\Theta'_{F/k} = \langle \{\nu_{F/M}(\theta_M) \mid M \in \mathscr{M}_{F/k}\} \rangle.$$

We remark we can check that for any intermediate field M of F/k, $\nu_{F/M}(\theta_M)$ is in $\Theta'_{F/k}$, though we do not use this fact in this paper.

We define our Stickelberger ideal by

$$\Theta_{F/k} = \Theta'_{F/k} \cap \mathbb{Z}'[\mathrm{Gal}(F/k)].$$

Suppose $M \in \mathscr{M}_{F/k}$. Then, M also satisfies the condition (A), and $\Theta'_{M/k}$ and $\Theta_{M/k}$ are defined.

Lemma 2.2. *For $M \in \mathscr{M}_{F/k}$, we have*

$$c_{F/M}(\Theta_{F/k}) \subset \Theta_{M/k} \quad \textit{and} \quad v_{F/M}(\Theta_{M/k}) \subset \Theta_{F/k}.$$

Proof. By the definition of $\Theta_{F/k}$ and $\Theta_{M/k}$, it is enough to show

$$c_{F/M}(\Theta'_{F/k}) \subset \Theta'_{M/k}$$

and

$$v_{F/M}(\Theta'_{M/k}) \subset \Theta'_{F/k}.$$

The first inclusion follows from Lemma 2.1, and the second inclusion follows from the definition of $\Theta'_{F/k}$.

Next, we consider a field F which does not necessarily satisfy the assumption (A). Instead of (A), we assume that there is a finite abelian extension F'/k such that $F \subset F'$, F' satisfies (A), and that F'/F is unramified at all finite primes. If $k = \mathbb{Q}$, for any abelian field F of finite degree, such F' exists uniquely for F by the next lemma. In this situation, we define the Stickelberger ideal $\Theta_{F/k}$ by

$$\Theta_{F/k} = c_{F'/F}(\Theta_{F'/k}).$$

Lemma 2.3. *Let $F/\mathbb{Q}$ be a finite abelian extension. Then, there exists uniquely an abelian extension $F'/\mathbb{Q}$ such that $F \subset F'$, F'/F is unramified at all finite primes, and that $F'/\mathbb{Q}$ satisfies the condition* (A).

Proof. This seems to be well known, for example, by genus theory, but we will give here a proof. Let m be the conductor of F, and $m = \ell_1^{e_1} \cdot \ldots \cdot \ell_r^{e_r}$ be its prime decomposition. We denote by I_{ℓ_i} the inertia group of ℓ_i in $\mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q})$. We have $\mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q}) = I_{\ell_1} \times \cdots \times I_{\ell_r}$. Let v_i be a prime of F lying over ℓ_i. We consider the extension $\mathbb{Q}(\mu_m)/F$, and denote by I_{v_i} the inertia group of v_i in $\mathrm{Gal}(\mathbb{Q}(\mu_m)/F)$. Since $F/\mathbb{Q}$ and $\mathbb{Q}(\mu_m)/\mathbb{Q}$ are abelian, I_{v_i} does not depend on the choice of v_i but only on ℓ_i. Consider the subgroup $H = I_{v_1} \times \cdots \times I_{v_r}$ of $\mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q})$ and the subfield F' which is fixed by H. Clearly, $F \subset F'$ and F'/F is unramified. Further, we have

$$\mathrm{Gal}(F'/\mathbb{Q}) = I_{\ell_1}/I_{v_1} \times \cdots \times I_{\ell_r}/I_{v_r},$$

so $F'/\mathbb{Q}$ satisfies the condition (A).

Next, we show the uniqueness. Suppose that F'' also satisfies the conditions. Put $\tilde{F} = F'F''$. Since $\tilde{F}/F'$ is unramified, the inertia group $I_{\ell_i}(\tilde{F}/\mathbb{Q})$

of ℓ_i in $\mathrm{Gal}(\tilde{F}/\mathbb{Q})$ is isomorphic to the inertia group of ℓ_i in $\mathrm{Gal}(F'/\mathbb{Q})$. Put $\mathscr{G} = I_{\ell_1}(\tilde{F}/\mathbb{Q}) \times \cdots \times I_{\ell_r}(\tilde{F}/\mathbb{Q}) \subset \mathrm{Gal}(\tilde{F}/\mathbb{Q})$. The natural map $\mathrm{Gal}(\tilde{F}/\mathbb{Q}) \to \mathrm{Gal}(F'/\mathbb{Q})$ induces an isomorphism $\mathscr{G} \xrightarrow{\simeq} \mathrm{Gal}(F'/\mathbb{Q})$. On the other hand, $\mathbb{Q}$ has no unramified extension, so we must have $\mathscr{G} = \mathrm{Gal}(\tilde{F}/\mathbb{Q})$. This shows that $\tilde{F} = F'$. Similarly, we have $\tilde{F} = F''$, so $F'' = F'$.

Suppose further that F is a CM field. We have the usual decomposition $\mathbb{Z}'[\mathrm{Gal}(F/k)] = \mathbb{Z}'[\mathrm{Gal}(F/k)]^+ \oplus \mathbb{Z}'[\mathrm{Gal}(F/k)]^-$ where $\mathbb{Z}'[\mathrm{Gal}(F/k)]^{\pm}$ is the $\pm$-eigenspace of the complex conjugation. Any $\mathbb{Z}'[\mathrm{Gal}(F/k)]$-module M is decomposed into $M = M^+ \oplus M^-$ by the above decomposition of $\mathbb{Z}'[\mathrm{Gal}(F/k)]$. In this paper, we are interested in $(\Theta_{F/k})^-$ in $\mathbb{Z}'[\mathrm{Gal}(F/k)]^-$.

Remark 2.4. For a finite abelian extension $F/\mathbb{Q}$, Sinnott defined the Stickelberger ideal S_F ([39], [40]) which is an ideal of $\mathbb{Z}[\mathrm{Gal}(F/\mathbb{Q})]$. If $F/\mathbb{Q}$ satisfies the condition (A), our $(\Theta_{F/\mathbb{Q}})^-$ coincides with $(S_F \otimes \mathbb{Z}')^-$ (cf. [39], Proposition 2.1 and [40], Theorem 5.4). So for example in the case $F = \mathbb{Q}(\mu_m)$, our $\Theta_{F/\mathbb{Q}}$ is obtained from Sinnott's ideal. But for a general abelian field F, our $\Theta_{F/\mathbb{Q}}$ slightly differs from the ideal obtained from the Sinnott's ideal in [40] (cf. [40], Theorem 5.4).

In the rest of this section, we fix an odd prime number p, and assume F/k satisfies the condition (A). Since $\Theta'_{F/k}$ is a free $\mathbb{Z}'$-module of finite rank, the following lemma is immediate.

Lemma 2.5. *In* $\mathbb{Q}_p[\mathrm{Gal}(F/k)]$, *we have*

$$(\Theta'_{F/k} \otimes \mathbb{Z}_p) \cap \mathbb{Z}_p[\mathrm{Gal}(F/k)] = \Theta_{F/k} \otimes \mathbb{Z}_p.$$

We consider a character $\chi : \mathrm{Gal}(F/k) \to \overline{\mathbb{Q}_p}^{\times}$. We denote by F_χ the subfield fixed by the kernel of χ in F, and by $\mathbb{Z}_p[\chi]$ (resp. $\mathbb{Q}_p(\chi)$) the ring generated by the image of χ over $\mathbb{Z}_p$ (resp. $\mathbb{Q}_p$). We extend χ to the ring homomorphism $\mathbb{Q}_p[\mathrm{Gal}(F/k)] \to \mathbb{Q}_p[\mathrm{Gal}(F_\chi/k)] \to \mathbb{Q}_p(\chi)$ which we also denote by χ.

Lemma 2.6. (1) *$\chi(\Theta'_{F/k} \otimes \mathbb{Z}_p)$ is contained in $\mathbb{Z}_p[\chi]\theta^{\chi}_{F_\chi}$ where $\theta^{\chi}_{F_\chi}$ is the image of θ_{F_χ} by the map χ.*

(2) *Let S_F (resp. S_{F_χ}) be the set of finite primes of k ramifying in F/k (resp. F_χ/k). We assume at least one of the following conditions.*

(i) *$S_F = S_{F_\chi}$.*

(ii) *$[F : k]$ is prime to p.*

Then, we have $\chi(\Theta'_{F/k} \otimes \mathbb{Z}_p) = \mathbb{Z}_p[\chi]\theta^{\chi}_{F_\chi}$.

Proof. (1) Let M be a field in $\mathscr{M}_{F/k}$. Suppose that M does not contain F_χ. Then $\mathrm{Ker}\,\chi$ does not contain $\mathrm{Gal}(F/M)$, and we have $\chi(v_{F/M}(x)) = 0$ for any $x \in \mathbb{Q}_p[\mathrm{Gal}(M/k)]$ because $\chi(N_{F/M}) = 0$ where $N_{F/M} = \sum_{\sigma \in \mathrm{Gal}(F/M)} \sigma$. So it is enough to consider $M \in \mathscr{M}_{F/k}$ such that $F_\chi \subset M$. For such M, it is clear that $\chi(v_{F/M}\theta_M) \in \mathbb{Z}_p[\mathrm{Image}\,\chi]\theta^{\chi}_{F_\chi}$ by Lemma 2.1.

(2) We first assume (i). Then, $c_{F/F_\chi}(\theta_F) = \theta_{F_\chi}$ by Lemma 2.1, so we get the conclusion. Next, we assume (ii). Let $M \in \mathscr{M}_{F/k}$ be a field such that $F_\chi \subset M$ and $S_M = S_{F_\chi}$ (S_M is the set of primes of k ramifying in M/k). Then, we have $\chi\big(v_{F/M}(\theta_M)\big) = [F : M]\theta_{F_\chi}^\chi$. By our assumption, $[F : M]$ is prime to p. So we get the conclusion.

3. Stickelberger ideals—cyclotomic $\mathbb{Z}_p$-extensions

In this section, we fix an odd prime number p, and define the Stickelberger ideals for cyclotomic $\mathbb{Z}_p$-extensions.

3.1. For a number field F, we denote by F_∞/F the cyclotomic $\mathbb{Z}_p$-extension. As in the previous section, we assume that k is a totally real number field, and that F is a CM field such that F/k is a finite abelian extension. Let F_n denote the n-th layer of F_∞/F, namely the intermediate field such that $[F_n : F] = p^n$. By Lemma 2.1, θ_{F_n}'s satisfy $c_{F_{n+1}/F_n}(\theta_{F_{n+1}}) = \theta_{F_n}$ for sufficiently large n, so become a projective system. More precisely, Deligne and Ribet [9] proved the existence of an element θ_{F_∞} of the total quotient ring of the completed group ring $\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/k)]]$, which satisfies the following properties (cf. [38], Theorem 1.15).

(i) The canonical map $c_{F_\infty/F_n} : \mathbb{Z}_p[[\mathrm{Gal}(F_\infty/k)]] \to \mathbb{Z}_p[\mathrm{Gal}(F_n/k)]$ extends to $\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/k)]]\theta_{F_\infty} \to \mathbb{Q}_p[\mathrm{Gal}(F_n/k)]$, and for a sufficiently large n, we have $c_{F_\infty/F_n}(\theta_{F_\infty}) = \theta_{F_n}$.

(ii) Suppose $\mu_p \subset F$. For any $\sigma \in \mathrm{Gal}(F_\infty/k)$, θ_{F_∞} satisfies

$$\big(1 - \kappa(\sigma)^{-1}\sigma\big)\theta_{F_\infty} \in \mathbb{Z}_p[[\mathrm{Gal}(F_\infty/k)]]$$

where $\kappa : \mathrm{Gal}(F_\infty/k) \to \mathbb{Z}_p^\times$ is the cyclotomic character.

(iii) Suppose that $\mu_p \subset F$ and $F \cap k_\infty = k$. Let γ be a generator of $\mathrm{Gal}(F_\infty/F)$ and define $N_{\mathrm{Gal}(F/k)}^{\omega^{-1}} = \sum_{\sigma \in \mathrm{Gal}(F/k)} \omega(\sigma)^{-1}\sigma$ where $\omega : \mathrm{Gal}(F/k) \to \mathrm{Gal}\big(k(\mu_p)/k\big) \to \mathbb{Z}_p^\times$ is the Teichmüller character. Then, θ_{F_∞} can be written as

$$\theta_{F_\infty} = \frac{cN_{\mathrm{Gal}(F/k)}^{\omega^{-1}}}{\kappa(\gamma) - \gamma} + \mu$$

for some $c \in \mathbb{Z}_p$ and $\mu \in \mathbb{Z}_p[[\mathrm{Gal}(F_\infty/k)]]$.

We assume the Leopoldt conjecture for k. So, in the above property (iii), $c \neq 0$ ([38] and [6]). Let $\mathscr{L}_1, \dots, \mathscr{L}_r$ be all finite primes of k ramifying in F/k. We denote by $P_{\mathscr{L}_i}$ the p-Sylow subgroup of the inertia subgroup $I_{\mathscr{L}_i}$ of $\mathscr{L}_i$ in $\mathrm{Gal}(F/k)$, and by $\mathrm{Gal}(F/k)\{p\}$ the p-Sylow subgroup of $\mathrm{Gal}(F/k)$. Instead of the condition (A) in §2, we assume that $F \cap k_\infty = k$, every prime of k above p is tamely ramified in F/k, and

$$(\mathrm{A}_p) \qquad \mathrm{Gal}(F/k)\{p\} = P_{\mathscr{L}_1} \times \cdots \times P_{\mathscr{L}_r}.$$

We write $G = \mathrm{Gal}(F/k)\{p\}$ and $\mathrm{Gal}(F/k) = \Delta \times G$ where Δ is of order prime to p. We define

$$(\mathscr{H}_{F/k})^{(p)} = \{H_0 \times H_1 \times \cdots \times H_r \mid H_0 \text{ is a subgroup of } \Delta \text{ and } H_i \text{ is a subgroup of } P_{\mathscr{L}_i} \text{ for all } i \text{ such that } 1 \leqq i \leqq r\}.$$

We also define

$$(\mathscr{M}_{F/k})^{(p)} = \{M \subset F \mid M \text{ is the fixed field of some } H \in (\mathscr{H}_{F/k})^{(p)}\}.$$

For a field $M \in (\mathscr{M}_{F/k})^{(p)}$, θ_{M_∞} can be defined by the same method. Let c_{F_∞/M_∞} be the natural map from the total quotient ring $Q(\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/k)]])$ of $\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/k)]]$ to the total quotient ring $Q(\mathbb{Z}_p[[\mathrm{Gal}(M_\infty/k)]])$ of $\mathbb{Z}_p[[\mathrm{Gal}(M_\infty/k)]]$, and $v_{F_\infty/M_\infty} : Q(\mathbb{Z}_p[[\mathrm{Gal}(M_\infty/k)]]) \to Q(\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/k)]])$ be the map induced by $\sigma \mapsto \sum_{c_{F_\infty/M_\infty}(\tau)=\sigma} \tau$. We define a $\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/k)]]$-module $(\Theta'_{F_\infty/k})^{(p)}$ by

$$(\Theta'_{F_\infty/k})^{(p)} = \langle \{v_{F_\infty/M_\infty}(\theta_{M_\infty}) \mid M \in (\mathscr{M}_{F/k})^{(p)}\} \rangle$$

which is contained in $Q(\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/k)]])$.

We define the Stickelberger ideal $(\Theta_{F_\infty/k})^{(p)}$ for F_∞/k by

$$(\Theta_{F_\infty/k})^{(p)} = (\Theta'_{F_\infty/k})^{(p)} \cap \mathbb{Z}_p[[\mathrm{Gal}(F_\infty/k)]].$$

We simply write $\Theta_{F_\infty/k}$ (resp. $\Theta'_{F_\infty/k}$) for $(\Theta_{F_\infty/k})^{(p)}$ (resp. $(\Theta'_{F_\infty/k})^{(p)}$) if no confusion arises.

This notation $(\Theta_{F_\infty/k})^{(p)}$ is justified by the following lemma. We define $(\overline{\Theta}'_{F/k})^{(p)}$ to be the sub $\mathbb{Z}_p[\mathrm{Gal}(F/k)]$-module of $\mathbb{Q}_p[\mathrm{Gal}(F/k)]$ generated by $v_{F/M}(\theta_M)$ for all $M \in (\mathscr{M}_{F/k})^{(p)}$, and define $(\overline{\Theta}_{F/k})^{(p)}$ by $(\overline{\Theta}_{F/k})^{(p)} = (\overline{\Theta}'_{F/k})^{(p)} \cap \mathbb{Z}_p[\mathrm{Gal}(F/k)]$.

Lemma 3.1. *Assume that there is an abelian extension F'/k satisfying the condition* (A) *in* §2 *such that $F' \supset F$, F'/F is unramified, and of degree prime to p. Then, $(\overline{\Theta}_{F/k})^{(p)} = \Theta_{F/k} \otimes \mathbb{Z}_p$.*

Proof. At first, we assume that F satisfies the condition (A). In order to show $(\overline{\Theta}_{F/k})^{(p)} = \Theta_{F/k} \otimes \mathbb{Z}_p$, it suffices to show $(\overline{\Theta}'_{F/k})^{(p)} = \Theta'_{F/k} \otimes \mathbb{Z}_p$ which we can check easily. Next, we consider the general case. It follows from what we showed above that $\Theta_{F/k} \otimes \mathbb{Z}_p = c_{F'/F}(\Theta_{F'/k} \otimes \mathbb{Z}_p) = c_{F'/F}((\overline{\Theta}_{F'/k})^{(p)})$. Since $[F' : F]$ is prime to p, by the norm argument, we get $c_{F'/F}((\overline{\Theta}_{F'/k})^{(p)}) = (\overline{\Theta}_{F/k})^{(p)}$. This completes the proof of this lemma.

Lemma 3.2. *Put $(\mathscr{M}_{F/k})_0^{(p)} = \{M \in (\mathscr{M}_{F/k})^{(p)} \mid$ there is a prime of k above p which is unramified in $M/k\}$. We can extend $c_{F_\infty/F}$ to $c_{F_\infty/F} : (\Theta'_{F_\infty/k})^{(p)} \to (\overline{\Theta}'_{F/k})^{(p)}$, and $(\overline{\Theta}'_{F/k})^{(p)}$ is generated by $c_{F_\infty/F}((\Theta'_{F_\infty/k})^{(p)})$ and $\{v_{F/M}(\theta_M) \mid M \in (\mathscr{M}_{F/k})_0^{(p)}\}$.*

Proof. By Lemma 2.1, we have $c_{M_\infty/M}(\theta_{M_\infty}) = \theta_M$ for $M \notin (\mathscr{M}_{F/k})_0^{(p)}$. So we obtain this lemma from the definitions of $(\Theta'_{F_\infty/k})^{(p)}$ and $(\overline{\Theta}'_{F/k})^{(p)}$.

By the same method as the proof of Lemma 2.2, we have

Lemma 3.3. *For $M \in (\mathscr{M}_{F/k})^{(p)}$, we have*

$$c_{F_\infty/M_\infty}\big((\Theta_{F_\infty/k})^{(p)}\big) \subset (\Theta_{M_\infty/k})^{(p)} \quad \textit{and} \quad v_{F_\infty/M_\infty}\big((\Theta_{M_\infty/k})^{(p)}\big) \subset (\Theta_{F_\infty/k})^{(p)}.$$

3.2. Next, we consider a finite abelian extension F/k with the following property. There is a finite abelian extension F'/k such that $F \subset F'$, F'/F is an unramified p-extension, and F'/k satisfies the above conditions of F/k (namely $F' \cap k_\infty = k$, every prime of k above p is tamely ramified in F'/k, and the extension F'/k satisfies the condition (A_p) in the previous subsection). For such F, we define $(\Theta_{F_\infty/k})^{(p)}$ by

$$(\Theta_{F_\infty/k})^{(p)} = c_{F'_\infty/F_\infty}\big((\Theta_{F'_\infty/k})^{(p)}\big).$$

This $(\Theta_{F_\infty/k})^{(p)}$ does not depend on the choice of F'. We will show this. Suppose that F'' also satisfies the conditions. Put $\tilde{F} = F'F''$. Let $P_{\mathscr{L}_i}(\tilde{F}/k)$ be the p-Sylow subgroup of the inertia group of $\mathscr{L}_i$ in $\mathrm{Gal}(\tilde{F}/k)$, and put $\mathscr{G} = P_{\mathscr{L}_1}(\tilde{F}/k) \times \cdots \times P_{\mathscr{L}_r}(\tilde{F}/k) \subset \mathrm{Gal}(\tilde{F}/k)$. The natural map $\mathrm{Gal}(\tilde{F}/k) \to \mathrm{Gal}(F'/k)$ induces an isomorphism $\mathscr{G} \xrightarrow{\simeq} \mathrm{Gal}(F'/k)\{p\}$. Using this isomorphism, we regard $H \in (\mathscr{H}_{F'/k})^{(p)}$ as a subgroup of $\mathrm{Gal}(\tilde{F}/k)$. We define $\tilde{\mathscr{M}}_{\tilde{F}/k} = \{M \mid M \text{ is the fixed field of } H \in (\mathscr{H}_{F'/k})^{(p)} \text{ in } \tilde{F}\}$, and

$$(\tilde{\Theta}'_{\tilde{F}_\infty/k})^{(p)} = \langle \{v_{\tilde{F}_\infty/M_\infty}(\theta_{M_\infty}) \mid M \in \tilde{\mathscr{M}}_{\tilde{F}/k}\} \rangle.$$

Since $\tilde{F}/F'$ is unramified, by Lemma 2.1 we have $c_{\tilde{F}_\infty/F'_\infty}\big((\tilde{\Theta}'_{\tilde{F}_\infty/k})^{(p)}\big) = (\Theta'_{F'_\infty/k})^{(p)}$. We define $(\tilde{\Theta}_{\tilde{F}_\infty/k})^{(p)} = (\tilde{\Theta}'_{\tilde{F}_\infty/k})^{(p)} \cap \mathbb{Z}_p[[\mathrm{Gal}(\tilde{F}_\infty/k)]]$. We will see $c_{\tilde{F}_\infty/F'_\infty}\big((\tilde{\Theta}_{\tilde{F}_\infty/k})^{(p)}\big) = (\Theta_{F'_\infty/k})^{(p)}$. We may assume $\mu_p \subset F$. Suppose that $x \in (\tilde{\Theta}'_{\tilde{F}_\infty/k})^{(p)}$. By the property (iii) in 3.1, x can be written as $x = cN^{\omega^{-1}}_{\mathrm{Gal}(\tilde{F}/k)}/\big(\kappa(\gamma) - \gamma\big) + \mu$ for some $c \in \mathbb{Z}_p$ and $\mu \in \mathbb{Z}_p[[\mathrm{Gal}(\tilde{F}_\infty/k)]]$. If $c_{\tilde{F}_\infty/F'_\infty}(x)$ is in $\mathbb{Z}_p[[\mathrm{Gal}(F'_\infty/k)]]$, then $[\tilde{F}_\infty : F'_\infty]c = 0$, so $c = 0$ and x is in $\mathbb{Z}_p[[\mathrm{Gal}(\tilde{F}_\infty/k)]]$. Hence, we get $c_{\tilde{F}_\infty/F'_\infty}\big((\tilde{\Theta}_{\tilde{F}_\infty/k})^{(p)}\big) = (\Theta_{F'_\infty/k})^{(p)}$. Thus, we have $(\Theta_{F_\infty/k})^{(p)} = c_{\tilde{F}_\infty/F_\infty}\big((\tilde{\Theta}_{\tilde{F}_\infty/k})^{(p)}\big)$, and it does not depend on the choice of F'.

We simply write $\Theta_{F_\infty/k}$ for $(\Theta_{F_\infty/k})^{(p)}$ when no confusion arises. We call this ideal $\Theta_{F_\infty/k}$ the Stickelberger ideal for F_∞/k.

3.3. In this subsection, we assume F satisfies the conditions in 3.1, so $\Theta'_{F_\infty/k}$ is defined. In the usual Iwasawa theory, we consider a character of $\mathrm{Gal}(F/k)$ and study the character-component of ideal class groups. Since we assumed $F \cap k_\infty = k$, we have $\mathrm{Gal}(F_\infty/k) = \mathrm{Gal}(F/k) \times \mathrm{Gal}(F_\infty/F)$. Let χ be a character of $\mathrm{Gal}(F/k)$ as in Lemma 2.6. We denote by F_χ the fixed field of $\mathrm{Ker}\,\chi$ in F. We extend χ to the ring homomorphism

$$Q\big(\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/k)]]\big) \to Q\big(\mathbb{Z}_p[\chi][[\mathrm{Gal}(F_\infty/F)]]\big) = Q\big(\mathbb{Z}_p[\chi][[\mathrm{Gal}(F_{\chi,\infty}/F_\chi)]]\big)$$

which we also denote by χ. By abuse of notation, the homomorphism

$$Q\big(\mathbb{Z}_p[[\mathrm{Gal}(F_{\chi,\infty}/k)]]\big) \to Q\big(\mathbb{Z}_p[\chi][[\mathrm{Gal}(F_{\chi,\infty}/F_\chi)]]\big)$$

which is induced by χ is also denoted by χ. We use the same notation as Lemma 2.6.

Lemma 3.4. *We assume $S_{F_\infty} = S_{F_{\chi,\infty}}$. ($S_{\mathscr{F}}$ is the set of primes of k ramifying in $\mathscr{F}/k$ for an algebraic extension $\mathscr{F}/k$.)*

(1) $\chi(\Theta'_{F_\infty/k}) = \mathbb{Z}_p[\chi][[\mathrm{Gal}(F_{\chi,\infty}/F_\chi)]]\theta^\chi_{F_{\chi,\infty}}$ *where* $\theta^\chi_{F_{\chi,\infty}} = \chi(\theta_{F_{\chi,\infty}})$.

(2) *We further assume $\chi \neq \omega$ where ω is the Teichmüller character. Then, $\chi(\Theta_{F_\infty/k}) = \chi(\Theta'_{F_\infty/k})$.*

Proof. (1) This can be proved by the same method as the proof of Lemma 2.6. We can easily see that $\chi(\Theta'_{F_\infty/k}) \subset \mathbb{Z}_p[\chi][[\mathrm{Gal}(F_{\chi,\infty}/F_\chi)]]\theta^\chi_{F_{\chi,\infty}}$. On the other hand, $\theta^\chi_{F_{\chi,\infty}} \in \chi(\Theta'_{F_\infty/k})$ follows from $c_{F_\infty/F_{\chi,\infty}}(\theta_{F_\infty}) = \theta_{F_{\chi,\infty}}$.

(2) By (1) and $\chi(\theta_{F_\infty}) = \chi(\theta_{F_{\chi,\infty}})$, it is enough to show $\chi(\theta_{F_\infty}) \in \chi(\Theta_{F_\infty/k})$. If a primitive p-th root of unity is not in F, F_n does not contain μ_p either, and we have $\theta_{F_n} \in \mathbb{Z}_p[\mathrm{Gal}(F_n/k)]$, so $\theta_{F_\infty} \in \mathbb{Z}_p[[\mathrm{Gal}(F_\infty/k)]]$. Thus, $\chi(\theta_{F_\infty}) \in \chi(\Theta_{F_\infty/k})$.

So we may assume $\mu_p \subset F$. We write $\mathrm{Gal}(F/k) = \Delta \times G$ where the order of Δ is prime to p and G is a p-group. Suppose at first the order of χ is prime to p. Then, putting $e_\chi = (\#\Delta)^{-1} \sum_{\sigma\in\Delta} \chi(\sigma)\sigma^{-1}$, by the property (iii) in 3.1 and $\chi \neq \omega$, we have $e_\chi\theta_{F_\infty} \in \Theta_{F_\infty/k}$. This implies $\chi(\theta_{F_\infty}) \in \chi(\Theta_{F_\infty/k})$.

Next, suppose the order of χ is divisible by p. Take $M = k(\mu_p) \in (\mathscr{M}_{F/k})^{(p)}$. Note that $M \neq F$ by our assumption that p divides the order of χ. We write $\theta_{F_\infty} = c_F N^{\omega^{-1}}_{\mathrm{Gal}(F/k)}/(\kappa(\gamma) - \gamma) + \mu_F$ with $c_F \in \mathbb{Z}_p$ and $\mu_F \in \mathbb{Z}_p[[\mathrm{Gal}(F_\infty/k)]]$ as in the property (iii) in 3.1. We define $c_M \in \mathbb{Z}_p$ similarly. Let $\mathscr{L}_1, \dots, \mathscr{L}_s$ be the ramifying primes in F/k, which are unramified in M/k. By Lemma 2.1, $c_{F_\infty/M_\infty}(\theta_{F_\infty}) = \prod_{i=1}^{s}(1 - \varphi_{\mathscr{L}_i}^{-1})\theta_{M_\infty}$. We have

$$c_{F_\infty/M_\infty}\big(N^{\omega^{-1}}_{\mathrm{Gal}(F/k)}/(\kappa(\gamma) - \gamma)\big) = [F : M] N^{\omega^{-1}}_{\mathrm{Gal}(M/k)}/(\kappa(\gamma) - \gamma)$$

and

$$\prod_i (1 - \varphi_{\mathscr{L}_i}^{-1}) N^{\omega^{-1}}_{\mathrm{Gal}(M/k)}/(\kappa(\gamma) - \gamma)$$
$$= \prod_i \big(1 - \kappa(\varphi_{\mathscr{L}_i})^{-1}\big) N^{\omega^{-1}}_{\mathrm{Gal}(M/k)}/(\kappa(\gamma) - \gamma) \bmod \mathbb{Z}_p[[\mathrm{Gal}(M_\infty/k)]].$$

Thus, we have

$$[F : M]c_F = \prod_{i=1}^{s}\big(1 - \kappa(\varphi_{\mathscr{L}_i})^{-1}\big)c_M.$$

Since

$$\mathrm{ord}_p([F : M]) = \mathrm{ord}_p([F : k]) = \sum_{i=1}^{r} \mathrm{ord}_p(\# P_{\mathscr{L}_i}) = \sum_{i=1}^{s} \mathrm{ord}_p(\# P_{\mathscr{L}_i})$$
$$\leqq \sum_{i=1}^{s} \mathrm{ord}_p\big(N(\mathscr{L}_i) - 1\big) = \sum_{i=1}^{s} \mathrm{ord}_p\big(1 - \kappa(\varphi_{\mathscr{L}_i})^{-1}\big)$$

(note that by our assumption the primes above p are tamely ramified in F/k), c_M divides c_F in $\mathbb{Z}_p$. Hence, there is $c \in \mathbb{Z}_p$ such that $\theta_{F_\infty} - c v_{F_\infty/M_\infty}(\theta_{M_\infty}) \in \mathbb{Z}_p[[\mathrm{Gal}(F_\infty/k)]]$. So we have $\theta_{F_\infty} - cv_{F_\infty/M_\infty}(\theta_{M_\infty}) \in \Theta_{F_\infty/k}$. Since the order of χ is divisible by p, χ is non trivial on $\mathrm{Gal}(F/M)$. Thus, $\chi(v_{F_\infty/M_\infty}(\theta_{M_\infty})) = 0$, and we get $\chi(\theta_{F_\infty}) \in \chi(\Theta_{F_\infty/k})$. This completes the proof.

Lemma 3.5. *Suppose that* $[F : k]$ *is prime to* p.

(1) $\chi(\Theta'_{F_\infty/k}) = \mathbb{Z}_p[\chi][[\mathrm{Gal}(F_{\chi,\infty}/F_\chi)]]\theta^\chi_{F_{\chi,\infty}}$ *where* $\theta^\chi_{F_{\chi,\infty}} = \chi(\theta_{F_{\chi,\infty}})$.

(2) *We further assume* $\chi \neq \omega$. *Then,* $\chi(\Theta_{F_\infty/k}) = \chi(\Theta'_{F_\infty/k})$.

Proof. (1) As in Lemma 3.4, it is enough to show $\theta^\chi_{F_{\chi,\infty}} \in \chi(\Theta'_{F_\infty/k})$. Since F_χ is in $(\mathscr{M}_{F/k})^{(p)}$ and $\chi(v_{F/F_\chi}(\theta_{F_{\chi,\infty}})) = [F : F_\chi]\theta^\chi_{F_{\chi,\infty}}$, we have $\theta^\chi_{F_{\chi,\infty}} \in \chi(\Theta'_{F_\infty/k})$ because $[F : F_\chi]$ is prime to p.

(2) Let e_χ be as above (note that $\Delta = \mathrm{Gal}(F/k)$ in our case). Since $e_\chi v_{F/F_\chi}(\theta_{F_{\chi,\infty}}) \in \Theta_{F_\infty/k}$, we have $\theta^\chi_{F_{\chi,\infty}} = \chi([F : F_\chi]^{-1} e_\chi v_{F/F_\chi}(\theta_{F_{\chi,\infty}})) \in \chi(\Theta_{F_\infty/k})$.

Remark 3.6. Let χ be an odd character. The element $\chi(\theta_{F_\infty})$ is essentially the p-adic L-function. We have the following interpolation property. Suppose $\mu_p \subset F$ and $\kappa : \mathrm{Gal}(F_\infty/k) \to \mathbb{Z}_p^\times$ is the cyclotomic character. For any positive integer $r > 0$, we have

$$\kappa^{-r}(\chi(\theta_{F_\infty/k})) = L_{\{p\}}(-r, \chi^{-1})$$

where $L_{\{p\}}(s, \chi^{-1})$ is the L-function obtained by removing the Euler factors of primes above p. Hence, by Lemma 3.4 we know that the usual main conjecture is obtained by taking the χ-quotient of Conjecture 0.8.

4. A preliminary lemma

The aim of this section is to prove Lemma 4.1 below. Let R be a complete discrete valuation ring of mixed characteristics $(0, p)$, and $\Lambda_R = R[[T]]$ be the ring of formal power series in one variable over R. In this section, we consider a finite abelian p-group G, and study a group ring $\Lambda_R[G]$.

Let ψ be a (p-adic) character of G, namely a homomorphism from G to the multiplicative group of an algebraic closure of the fraction field of R. We define

$$\psi_{\Lambda_R[G]} : \Lambda_R[G] \to \Lambda_R[\mathrm{Image}\,\psi] = \Lambda_{R[\mathrm{Image}\,\psi]}$$

to be the ring homomorphism induced by $\sigma \mapsto \psi(\sigma)$ for $\sigma \in G$.

Suppose that

$$G = G_1 \times \cdots \times G_r$$

where $G_1, \dots, G_r$ are cyclic groups. We define a set $\mathscr{H}$ of certain subgroups of G by

$$\mathscr{H} = \{H_1 \times \cdots \times H_r \mid H_i \text{ is a subgroup of } G_i \text{ for all } i \text{ such that } 1 \leqq i \leqq r\}.$$

For any subgroup $H = H_1 \times \cdots \times H_r \in \mathscr{H}$, we define a set of certain characters of G/H by

$$\Psi_{G/H} = \{\psi_1 \cdot \dots \cdot \psi_r \mid \psi_i \text{ is a faithful character of } G_i/H_i \text{ for all } i \text{ such that } 1 \leqq i \leqq r\}.$$

For $\psi = \psi_1 \cdot \dots \cdot \psi_r \in \Psi_{G/H}$, ψ_i is a faithful character of G_i/H_i by definition, but ψ itself is not a faithful character of G/H in general.

Lemma 4.1. *Let R, $\Lambda_R, \dots$ be as above. Suppose that for any subgroup $H \in \mathscr{H}$, an ideal $I_{G/H}$ of $\Lambda_R[G/H]$ and an element $x_{G/H}$ of $\Lambda_R[G/H]$ are given and satisfy the following properties.*

(i) *For any subgroup $H \in \mathscr{H}$, $x_{G/H}$ is the image of x_G by the canonical map $\Lambda_R[G] \to \Lambda_R[G/H]$.*

(ii) *For any subgroup $H \in \mathscr{H}$ and any character $\psi \in \Psi_{G/H}$,*

$$\psi_{\Lambda_R[G/H]}(x_{G/H}) \in \psi_{\Lambda_R[G/H]}(I_{G/H}).$$

(iii) *For any subgroup $H \in \mathscr{H}$ and any character ψ of $\Psi_{G/H}$, $\Lambda_R[\mathrm{Image}\,\psi]/\psi_{\Lambda_R[G/H]}(I_{G/H})$ is a free $R[\mathrm{Image}\,\psi]$-module of finite rank.*

(iv) *For any subgroups H and H' in $\mathscr{H}$ such that $H \subset H'$, we have*

$$c_{H,H'}(I_{G/H}) \subset I_{G/H'}$$

where $c_{H,H'} : \Lambda_R[G/H] \to \Lambda_R[G/H']$ is the canonical homomorphism induced by the natural map $G/H \to G/H'$.

(v) *For any subgroups H and H' in $\mathscr{H}$ such that $H \subset H'$, we have*

$$v_{H',H}(I_{G/H'}) \subset I_{G/H}$$

where $v_{H',H} : \Lambda_R[G/H'] \to \Lambda_R[G/H]$ is the map induced by $\sigma \mapsto \sum_{c_{H,H'}(\tau)=\sigma} \tau$ for $\sigma \in G/H'$.

Then, $\Lambda_R[G]/I_G$ is a free R-module of finite rank, and x_G is in I_G.

Proof. We prove this lemma by induction on the order of G. If $\# G = 1$, the conclusion is clear from the properties (ii) and (iii) by taking $\psi = 1$. Suppose $\# G > 1$ and $G_1 \neq \{1\}$. We denote by p^m the order of G_1.

Let $\psi_1 : G_1 \to R[\mathrm{Image}\,\psi_1]^\times$ be an injective homomorphism. Set $\mathscr{G} = G_2 \times \cdots \times G_r$ and $R' = R[\mathrm{Image}\,\psi_1]$. So, $G = G_1 \times \mathscr{G}$. We consider a homomorphism

$$(\psi_1)_{\Lambda_R[G], G_1} : \Lambda_R[G] = \Lambda_R[\mathscr{G}][G_1] \to \Lambda_R[\mathscr{G}][\mathrm{Image}\,\psi_1] = \Lambda_{R'}[\mathscr{G}]$$

which is the ring homomorphism induced by $\sigma \mapsto \psi_1(\sigma)$ for $\sigma \in G_1$. Let $\mathscr{H}'$ be the set of the subgroups of $\mathscr{G}$ of the form $H_2 \times \cdots \times H_r \subset \mathscr{G}$ where H_i is a subgroup of G_i. For a subgroup H' in $\mathscr{H}'$, we define an ideal $I_{\mathscr{G}/H'}$ of $\Lambda_{R'}[\mathscr{G}/H']$ by $I_{\mathscr{G}/H'} = (\psi_1)_{\Lambda_R[G], G_1}(I_{G/H})$, and an element $x_{\mathscr{G}/H'}$ by $x_{\mathscr{G}/H'} = (\psi_1)_{\Lambda_R[G], G_1}(x_{G/H})$ where $H = \{1\} \times H' \in \mathscr{H}$. Then, these ideals $I_{\mathscr{G}/H'}$ and elements $x_{\mathscr{G}/H'}$ satisfy the properties (i)–(v) for $\Lambda_{R'}[\mathscr{G}]$. Since $\#\mathscr{G} < \# G$, by the hypothesis of the induction, $\Lambda_{R'}[\mathscr{G}]/I_{\mathscr{G}} = (\psi_1)_{\Lambda_R[G], G_1}(\Lambda_R[G])/(\psi_1)_{\Lambda_R[G], G_1}(I_G)$ is a free R'-module of finite rank, and $(\psi_1)_{\Lambda_R[G], G_1}(x_G) \in (\psi_1)_{\Lambda_R[G], G_1}(I_G)$.

We consider

$$\bigoplus_{\psi_1} (\psi_1)_{\Lambda_R[G], G_1} : \Lambda_R[G] \to \bigoplus_{\psi_1} (\psi_1)_{\Lambda_R[G], G_1}(\Lambda_R[G])$$

where ψ_1 ranges over all $R[1/p]$-conjugate classes of the faithful characters of G_1 whose values are in an algebraic closure of $R[1/p]$. The kernel of the above map is $\left(\sum_{i=0}^{p-1} s^{p^{m-1}i}\right)\Lambda_R[G]$ where s is a generator of G_1. Hence, if we define the subgroup N by $N = G_1^{p^{m-1}} \times \{1\} \times \cdots \times \{1\} \subset G$ (so the order of N is p), then the kernel of the above map coincides with the image of $v_{N,\{1\}} : \Lambda_R[G/N] \to \Lambda_R[G]$ where $v_{N,\{1\}}$ is the map defined in the property (v) in Lemma 4.1. So we have an exact sequence

$$\Lambda_R[G/N]/I_{G/N} \xrightarrow{v_{N,\{1\}}} \Lambda_R[G]/I_G \longrightarrow \bigoplus_{\psi_1} (\psi_1)_{\Lambda_R[G],G_1}(\Lambda_R[G])/(\psi_1)_{\Lambda_R[G],G_1}(I_G).$$

By the hypothesis of the induction, we can apply the lemma for the group G/N instead of G, and know that $\Lambda_R[G/N]/I_{G/N}$ is a free R-module of finite rank, and $x_{G/N}$ is in $I_{G/N}$. We claim that the first map in the above sequence is injective. In order to show this, since $\Lambda_R[G/N]/I_{G/N}$ is a free R-module of finite rank, it suffices to show the injectivity of

$$v_{N,\{1\}} : (\Lambda_R[G/N]/I_{G/N}) \otimes \mathbb{Q} \to (\Lambda_R[G]/I_G) \otimes \mathbb{Q}.$$

But $v_{N,\{1\}}$ gives an injection from $\Lambda_R[G/N] \otimes \mathbb{Q}$ into a direct summand of $\Lambda_R[G] \otimes \mathbb{Q}$. In fact, if $c_{\{1\},N} : \Lambda_R[G] \otimes \mathbb{Q} \to \Lambda_R[G/N] \otimes \mathbb{Q}$ is the canonical map, $p^{-1}c_{\{1\},N} \circ v_{N,\{1\}}$ is the identity map on $\Lambda_R[G/N] \otimes \mathbb{Q}$. So by the property (iv), $v_{N,\{1\}} : (\Lambda_R[G/N]/I_{G/N}) \otimes \mathbb{Q} \to (\Lambda_R[G]/I_G) \otimes \mathbb{Q}$ is injective. Thus, we get an exact sequence

$$\begin{aligned} 0 \to \Lambda_R[G/N]/I_{G/N} &\to \Lambda_R[G]/I_G \\ &\to \bigoplus_{\psi_1} (\psi_1)_{\Lambda_R[G],G_1}(\Lambda_R[G])/(\psi_1)_{\Lambda_R[G],G_1}(I_G). \end{aligned}$$

Since both $\Lambda_R[G/N]/I_{G/N}$ and $\bigoplus_{\psi_1} (\psi_1)_{\Lambda_R[G],G_1}(\Lambda_R[G])/(\psi_1)_{\Lambda_R[G],G_1}(I_G)$ are free R-modules of finite rank, it follows from this exact sequence that $\Lambda_R[G]/I_G$ is free of finite rank as an R-module. By the hypothesis of the induction, $(\psi_1)_{\Lambda_R[G],G_1}(x_G)$ is in $(\psi_1)_{\Lambda_R[G],G_1}(I_G)$, so the above exact sequence tells us that there is $y \in \Lambda_{G/N}$ such that $x_G \equiv v_{N,\{1\}}(y) \pmod{I_G}$. Taking the projection to $\Lambda_R[G/N]$ of this equation, by the properties (i) and (iv) we obtain $x_{G/N} \equiv py \pmod{I_{G/N}}$. By the hypothesis of the induction, $x_{G/N}$ is in $I_{G/N}$, so this implies that $py \in I_{G/N}$. But $\Lambda_R[G/N]/I_{G/N}$ is a free R-module again by the hypothesis of the induction, so we get $y \in I_{G/N}$. This implies that $x_G \equiv v_{N,\{1\}}(y) \equiv 0 \pmod{I_G}$ by the property (v). Thus, we get $x_G \in I_G$. This completes the proof of Lemma 4.1.

From Lemma 4.1, we obtain

Corollary 4.2. *Suppose that for any subgroup $H \in \mathscr{H}$, two ideals $I_{G/H}$ and $J_{G/H}$ of $\Lambda_R[G/H]$ are given and satisfy the following properties.*

(i) *For any subgroup $H \in \mathscr{H}$ and any character ψ of $\Psi_{G/H}$,*

$$\psi_{\Lambda_R[G/H]}(I_{G/H}) = \psi_{\Lambda_R[G/H]}(J_{G/H}).$$

(ii) *For any subgroup $H \in \mathscr{H}$ and any character ψ of $\Psi_{G/H}$, $\Lambda_R[\mathrm{Image}\,\psi]/\psi_{\Lambda_R[G/H]}(I_{G/H})$ is a free $R[\mathrm{Image}\,\psi]$-module of finite rank.*

(iii) *For any subgroups H and H' in $\mathscr{H}$ such that $H \subset H'$, we have*

$$c_{H,H'}(I_{G/H}) \subset I_{G/H'} \quad \textit{and} \quad c_{H,H'}(J_{G/H}) \subset J_{G/H'}.$$

(iv) *For any subgroups H and H' in $\mathscr{H}$ such that $H \subset H'$, we have*

$$\nu_{H',H}(I_{G/H'}) \subset I_{G/H} \quad \textit{and} \quad \nu_{H',H}(J_{G/H'}) \subset J_{G/H}.$$

Then, we have $I_G = J_G$.

5. Ideal class groups

In this section we study the minus parts of ideal class groups of CM fields. We fix an odd prime number p.

Let k be a totally real number field, and L and K be two CM fields such that $k \subset K \subset L$, L/k is a finite abelian extension, and that L/K is a p-extension. We denote by A_K (resp. A_L) the p-Sylow subgroup of the ideal class group of K (resp. L). We consider their minus parts A_K^- and A_L^- on which the complex conjugation acts as -1. We put $G = \mathrm{Gal}(L/K)$.

Lemma 5.1. (1) *The norm map $A_L^- \to A_K^-$ is surjective.*

(2) *Let $\hat{H}^q(G,*)$ be the Tate cohomology* (*cf.* [36], *Chap.* 8). *We denote by P_L the set of all finite primes of L. Then, we have an exact sequence*

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

where E_L (*resp. E_{L_w}*) *is the unit group of L* (*resp. the local field L_w*).

Proof. (1) Let K'/K be the unramified extension of K corresponding to A_K^- by class field theory. Then the complex conjugation acts on $\mathrm{Gal}(K'/K)$ as -1, and acts on $\mathrm{Gal}(L/K)$ trivially because L/k is abelian. So, $K' \cap L = K$. Hence, $A_L^- \to A_K^-$ is surjective.

(2) Let $\mathscr{C}_L$ be the idele class group of L. We consider the Tate cohomology groups $\hat{H}^*(G,\mathscr{C}_L)$. By Tate-Nakayama's theorem ([36], Chap. 9, §8), we have $\hat{H}^0(G,\mathscr{C}_L) = \hat{H}^{-2}(G,\mathbb{Z}) = H_1(G,\mathbb{Z}) = G$, and $\hat{H}^{-1}(G,\mathscr{C}_L) = \hat{H}^{-3}(G,\mathbb{Z}) = H_2(G,\mathbb{Z}) = \bigwedge^2 G$. So, $\hat{H}^0(G,\mathscr{C}_L)^- = \hat{H}^{-1}(G,\mathscr{C}_L)^- = 0$. Note also that $H^1(G,\mathscr{C}_L) = 0$ by class field theory.

Consider an exact sequence

$$0 \to E_L \to \prod E_{L_w} \to \mathscr{C}_L \to Cl_L \to 0$$

where w ranges over all primes of L (if w is an infinite place, it is a complex place, and we define $E_{L_w} = L_w^\times$), and Cl_L is the ideal class group of L. Define M to be the kernel of $\mathscr{C}_L \to Cl_L$. Then, by the above calculation, $\hat{H}^q(G, Cl_L)^- = \hat{H}^q(G, A_L)^- = \hat{H}^{q+1}(G, M)^-$ for $q = 0$ and -1. Hence, taking the Tate cohomology of the exact sequence

$$0 \to E_L \to \prod E_{L_w} \to M \to 0,$$

we obtain the conclusion of Lemma 5.1 (2).

Proposition 5.2. *Let L/K be as above. For a prime $v \in P_K$, I_v denotes the inertia group of v in G. Let $\mu_{p^\infty}(K)$ be the p-primary component of the group of roots of unity in K. Then, we have an exact sequence*

$$\mu_{p^\infty}(K) \to \Big(\bigoplus_{v \in P_K} I_v\Big)^- \to (A_L^-)_G \xrightarrow{N} A_K^- \to 0$$

where $(A_L^-)_G$ is the G-coinvariant of A_L^-, and N is the map induced by the norm map.

Proof. First of all, we note that there is an exact sequence

$$0 \to \mathrm{Ker}\big((A_L)_G \to A_K\big) \to \hat{H}^{-1}(G, A_L) \to \mathrm{Ker}(A_K \to A_L).$$

This follows from the following commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \hat{H}^{-1}(G, A_L) \arrow[r] \arrow[d] & (A_L)_G \arrow[r, "N_G"] \arrow[d, "N"] & A_L \arrow[d, equal] \\
0 \arrow[r] & \mathrm{Ker}(A_K \to A_L) \arrow[r] & A_K \arrow[r] & A_L
\end{tikzcd}$$

where $N_G = \sum_{\sigma \in G} \sigma$ and N is the map induced by the norm map of ideal class groups. It is well known that the kernel of $H^1(G, E_L) \to H^1\Big(G, \prod_{w \in P_L} E_{L_w}\Big)$ coincides with $\mathrm{Ker}(A_K \to A_L)$ (cf. [22], Remark 2.2). Hence, the kernel of $(A_L^-)_G \to A_K^-$ coincides with $\mathrm{Ker}\big(\hat{H}^{-1}(G, A_L)^- \to H^1(G, E_L)^-\big)$ which is the cokernel of

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

by Lemma 5.1 (2).

By local class field theory, we have

$$\hat{H}^0\Big(G, \prod_{w \in P_L} E_{L_w}\Big) = \bigoplus_{v \in P_K} E_{K_v}/NE_{L_w} = \bigoplus_{v \in P_K} I_v.$$

Since K is a CM field, $H^0(G, E_L)^- \otimes \mathbb{Z}_p = \mu_{p^\infty}(K)$. Hence, we have $\mathrm{Ker}\big((A_L^-)_G \to A_K^-\big) = \mathrm{Coker}\big(\mu_{p^\infty}(K) \to (\bigoplus I_v)^-\big)$. Since $A_L^- \to A_K^-$ is surjective by Lemma 5.1 (1), we get the conclusion.

Let K_∞/K and L_∞/L be the cyclotomic $\mathbb{Z}_p$-extensions, and consider $X_{K_\infty} = \varprojlim A_{K_n}$ and $X_{L_\infty} = \varprojlim A_{L_n}$.

Corollary 5.3. *Let K, L, K_∞, and L_∞ be as above. We denote by P_{K_∞} the set of finite primes of K_∞, and by I_v the inertia group of v in $\mathrm{Gal}(L_\infty/K_\infty)$ for $v \in P_{K_\infty}$. The norm map from X_{L_∞} to X_{K_∞} induces an exact sequence of $\mathbb{Z}_p[[\mathrm{Gal}(K_\infty/k)]]$-modules*

$$T \to \Big(\bigoplus_{v \in P_{K_\infty}} I_v\Big)^- \to (X_{L_\infty}^-)_{\mathrm{Gal}(L_\infty/K_\infty)} \to X_{K_\infty}^- \to 0$$

where $T = \mathbb{Z}_p(1) = \varprojlim \mu_{p^n}$ if $\mu_p \subset K$, and $T = 0$ otherwise.

Proof. This is obtained by taking the projective limit of the exact sequence in Proposition 5.2.

Lemma 5.4. *Suppose that $\mathrm{Gal}(L_\infty/K_\infty)$ is cyclic, and that the μ-invariant of K_∞ vanishes (X_{K_∞} is a finitely generated $\mathbb{Z}_p$-module). We further assume that the primes above p are unramified in L_∞/K_∞, and there is a totally ramified prime in L_∞/K_∞. Then, the canonical map induces an isomorphism*

$$X_{K_\infty}^- \xrightarrow{\simeq} (X_{L_\infty}^-)^{\mathrm{Gal}(L_\infty/K_\infty)}.$$

Proof. First of all, since $X_{K_\infty}^-$ does not have a non-trivial finite $\mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]]$-submodule ([46], Proposition 13.28), $\mu = 0$ implies that $X_{K_\infty}^-$ is a free $\mathbb{Z}_p$-module. So the norm argument implies the injectivity.

Put $G = \mathrm{Gal}(L_\infty/K_\infty)$ and $\# G = p^m$. Let v_0 be a prime of K_∞ which is totally ramified in L_∞/K_∞, and w_0 be the prime of L lying over v_0. We may change K and L to sufficiently large number fields, and suppose that $\mathrm{Gal}(L/K) = \mathrm{Gal}(L_\infty/K_\infty)$ and $\mu_{p^\infty}(K) = \mu_{p^\infty}(K_{v_0})$ where K_{v_0} is the completion of K at the prime below v_0. Then, we have $\hat{H}^0(G, E_L)^- = \mu_{p^\infty}(K)/\mu_{p^\infty}(K)^{p^m}$, and $\hat{H}^0(G, E_{L_{w_0}}) = \mu_{p^\infty}(K_{v_0})/\mu_{p^\infty}(K_{v_0})^{p^m}$, so the map $\hat{H}^0(G, E_L)^- \to \hat{H}^0\Big(G, \prod_{w \in P_L} E_{L_w}\Big)^-$ is injective. Since this injectivity holds for all intermediate fields L_n and G is cyclic, the map $\varprojlim H^2(G, E_{L_n})^- \to \varprojlim H^2\Big(G, \prod_{w \in P_{L_n}} E_{L_{n,w}}\Big)^-$ is injective.

On the other hand, $H^1\Big(G, \prod_{w \in P_{L_n}} E_{(L_n)_w}\Big) = \bigoplus_{v \in P_{K_n}} \mathbb{Z}/e_v\mathbb{Z}$ where e_v is the ramification index of v in L_n/K_n. For a sufficiently large n, the norm map from L_{n+1} to L_n induces the multiplication by p on the right hand side, so $\varprojlim H^1\Big(G, \prod_{w \in P_{L_n}} E_{(L_n)_w}\Big) = 0$. Hence, by Lemma 5.1 (2) we get $\hat{H}^0(G, X_{L_\infty}^-) = 0$, which implies the conclusion of the lemma.

By this lemma, we obtain

Lemma 5.5. *In the situation of Lemma* 5.4, *for a faithful character* ψ *of* $G = \mathrm{Gal}(L_\infty/K_\infty)$, *we define* $(X_{L_\infty}^-)^\psi$ *by* $(X_{L_\infty}^-)^\psi = X_{L_\infty}^- \otimes_{\mathbb{Z}_p[G]} \mathbb{Z}_p[\psi]_{(G)}$ *where* $\mathbb{Z}_p[\psi]_{(G)}$ *is the G-module on which G acts via* ψ *(cf.* 1.3). *Then,* $(X_{L_\infty}^-)^\psi$ *does not have a non-trivial finite* $\mathbb{Z}_p[\psi][[\mathrm{Gal}(L_\infty/L)]]$*-submodule.*

Proof. Suppose that the order of G is p^m, and σ is a generator. Since $\mathbb{Z}_p[\psi] \simeq \mathbb{Z}_p[G]/(1+\sigma^{p^{m-1}}+\cdots+\sigma^{p^{m-1}(p-1)})$, if we denote by C the subgroup of order p of G and put $N_C = \sum_{s\in C} s$, we have $\mathbb{Z}_p[\psi] \simeq \mathbb{Z}_p[G]/N_C$. So $(X_{L_\infty}^-)^\psi = X_{L_\infty}^-/N_C X_{L_\infty}^-$. We denote by K' the fixed field of C in L. Put $s_0 = \sigma^{p^{m-1}}$ which is a generator of C. We will show that $s_0 - 1$ induces an injection

$$s_0 - 1 : X_{L_\infty}^-/N_C X_{L_\infty}^- \hookrightarrow X_{L_\infty}^-.$$

In fact, if $(s_0-1)(x) = 0$ for some $x \in X_{L_\infty}^-$, then $x \in (X_{L_\infty}^-)^C$, so x can be written as $x = i(y)$ for some $y \in X_{K'_\infty}^-$ by Lemma 5.4 where $i : X_{K'_\infty}^- \to X_{L_\infty}^-$ is the natural map. Since the norm map $X_{L_\infty}^- \to X_{K'_\infty}^-$ is surjective by Lemma 5.1 (1), we have $x = N_C(z)$ for some $z \in X_{L_\infty}^-$. This implies $X_{L_\infty}^-/N_C X_{L_\infty}^- \to X_{L_\infty}^-$ is injective. Hence, we get the conclusion of Lemma 5.5 because $X_{L_\infty}^-$ does not have a non-trivial finite $\mathbb{Z}_p[[\mathrm{Gal}(L_\infty/L)]]$-submodule ([46], Proposition 13.28).

6. Proof of the theorems I

We will prove Theorem 0.9 at first. We may assume that F satisfies the condition (A_p). In fact, suppose that F'/F is the unramified extension in 3.2, and $c = c_{F'_\infty/F_\infty} : \mathbb{Z}_p[[\mathrm{Gal}(F'_\infty/k)]] \to \mathbb{Z}_p[[\mathrm{Gal}(F_\infty/k)]]$ is the natural map. By Corollary 5.3, we have an isomorphism $(X_{F'}^-)_{\mathrm{Gal}(F'/F)} \xrightarrow{\simeq} X_F^-$. Hence, we have

$$c\big(\mathrm{Fitt}_{0,\mathbb{Z}_p[[\mathrm{Gal}(F'_\infty/k)]]}(X_{F'}^-)^-\big) = \mathrm{Fitt}_{0,\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/k)]]}(X_F^-)^-.$$

On the other hand, by definition, we have $c(\Theta_{F'_\infty/k}) = \Theta_{F_\infty/k}$. Hence, Conjecture 0.8 for F' implies Conjecture 0.8 for F.

We write $\mathrm{Gal}(F/k) = \Delta \times G$ where the order of Δ is prime to p, and G is a p-group. Let K be the fixed field of G in F (so $\mathrm{Gal}(F/K) = G$). We have the decomposition $\mathbb{Z}_p[\Delta] = \bigoplus_\chi \mathbb{Z}_p[\chi]$ as in 1.4, and have

$$\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/k)]] = \bigoplus_\chi \mathbb{Z}_p[\chi][[\mathrm{Gal}(F_\infty/K)]].$$

So in order to prove this theorem, it suffices to show the equality

$$\big(\mathrm{Fitt}_{0,\mathbb{Z}_p[\chi][[\mathrm{Gal}(F_\infty/K)]]}(X_{F_\infty}^\chi)\big)_{(\Delta)}^\chi = (\Theta_{F_\infty/k})_{(\Delta)}^\chi$$

as ideals of $\mathbb{Z}_p[\chi][[\mathrm{Gal}(F_\infty/K)]]$ for each odd character χ of Δ.

We take an odd character χ of Δ. We denote by Δ_χ the kernel of χ, and by K_χ (resp. F_χ) the fixed field of Δ_χ in K (resp. F). So $\mathrm{Gal}(K_\chi/k) = \mathrm{Image}\,\chi$ and $\mathrm{Gal}(F_\chi/K_\chi) = G$. Recall that we assumed F/k satisfies the condition (A_p), so

$$G = P_{\mathscr{L}_1} \times \cdots \times P_{\mathscr{L}_r}$$

where $P_{\mathscr{L}_i}$ is the p-Sylow subgroup of the inertia group of $\mathscr{L}_i$. We define

$$\mathscr{H} = \{H_1 \times \cdots \times H_r \mid H_i \text{ is a subgroup of } P_{\mathscr{L}_i} \text{ for all } i \text{ such that } 1 \leqq i \leqq r\}$$

and

$$\mathscr{M} = \{M \mid K \subset M \subset F,\ M \text{ is the fixed field of some } H \in \mathscr{H} \text{ in } F\}.$$

We note that $P_{\mathscr{L}_i}$ is cyclic since we assumed a prime over p is tamely ramified in F/k. As in §4, for $H = H_1 \times \cdots \times H_r \in \mathscr{H}$ we define

$$\Psi_{G/H} = \{\psi_1 \cdot \ldots \cdot \psi_r \mid \psi_i \text{ is a faithful character of } P_{\mathscr{L}_i}/H_i \text{ for all } i \text{ such that } 1 \leqq i \leqq r\}.$$

For $H \in \mathscr{H}$, let M be the subfield in F fixed by H (so $M \in \mathscr{M}$). We write M_χ the fixed field of Δ_χ in M. Put $\Lambda = \mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]]^\chi_{(\Delta)} = \mathbb{Z}_p[\chi][[\mathrm{Gal}(K_{\chi,\infty}/K_\chi)]]$. Then, $\mathbb{Z}_p[[\mathrm{Gal}(M_\infty/K)]]^\chi_{(\Delta)} = \mathbb{Z}_p[\chi][[\mathrm{Gal}(M_{\chi,\infty}/K_\chi)]]^\chi = \Lambda[G/H]$. We regard $(\Theta_{M_\infty/k})^\chi$ $(=(\Theta_{M_\infty/k})^\chi_{(\Delta)})$ as a $\Lambda[G/H]$-module. We define two ideals $I_{G/H}$ and $J_{G/H}$ of $\Lambda[G/H]$ by

$$I_{G/H} = (\Theta_{M_\infty/k})^\chi$$

and

$$J_{G/H} = \bigl(\mathrm{Fitt}_{0,\Lambda[G/H]}(X^\chi_{M_\infty})\bigr)^\chi.$$

Since $[M : M_\chi]$ is prime to p, we easily see $c_{M_\infty/(M_\chi)_\infty}(\Theta_{M_\infty/k}) = \Theta_{(M_\chi)_\infty/k}$ by the norm argument. Hence, we have $I_{G/H} = (\Theta_{M_\infty/k})^\chi = (\Theta_{(M_\chi)_\infty/k})^\chi$.

Let ψ be a character in $\Psi_{G/H}$. We regard $\chi\psi$ as a character of $\mathrm{Gal}(M/k)$, and denote by $M_{\chi\psi}$ the fixed field of the kernel of $\chi\psi$ in M. So $K_\chi \subset M_{\chi\psi} \subset M_\chi$, and $\mathrm{Gal}(M_{\chi\psi}/K_\chi) = \mathrm{Image}\,\psi$. Since ψ is a product of faithful characters ψ_i of some quotient of $P_{\mathscr{L}_i}$ ($\psi \in \Psi_{G/H}$), we have $S_{M_{\chi\psi,\infty}} = S_{M_{\chi,\infty}}$ (where $S_{\mathscr{F}}$ is the set of primes of k ramifying in $\mathscr{F}/k$ as in Lemma 2.6). So we can apply Lemma 3.4 to the field M_χ which satisfies the condition (A_p) and to a character $\chi\psi$ of $\mathrm{Gal}(M_\chi/k)$. If $\chi \neq \omega$ or $\psi \neq 1$, by Lemma 3.4, we have

$$\psi_{\Lambda[G/H]}(I_{G/H}) = \psi_{\Lambda[G/H]}\bigl((\Theta_{(M_\chi)_\infty/k})^\chi\bigr) = \chi\psi(\Theta_{(M_\chi)_\infty/k}) = (\theta^{\chi\psi}_{M_{\chi\psi,\infty}})$$

in $\mathbb{Z}_p[\chi\psi][[\mathrm{Gal}(M_{\chi\psi,\infty}/M_{\chi\psi})]]$ where $\psi_{\Lambda[G/H]}$ is as in §4.

On the other hand, for $J_{G/H}$, we have $(X_{M_\infty})_{\mathrm{Gal}(M_\infty/M_{\chi,\infty})} \simeq X_{M_{\chi,\infty}}$ by the norm argument since $[M : M_\chi]$ is prime to p. Further, by the definition of $\Psi_{G/H}$, $\psi \in \Psi_{G/H}$ implies that $M_\chi/M_{\chi\psi}$ is unramified. So by Corollary 5.3, $(X^-_{M_\infty})_{\mathrm{Gal}(M_\infty/M_{\chi\psi,\infty})} \xrightarrow{\simeq} X^-_{M_{\chi\psi,\infty}}$ is bijective. Hence, we obtain

$$\psi_{\Lambda[G/H]}(J_{G/H}) = \mathrm{Fitt}_{0,\mathbb{Z}_p[\chi\psi][[\mathrm{Gal}(M_{\chi\psi,\infty}/M_{\chi\psi})]]}(X^{\chi\psi}_{M_{\chi\psi,\infty}}).$$

We note that ψ is a faithful character of $\mathrm{Gal}(M_{\chi\psi}/K_\chi)$. Since we assumed the μ-invariant vanishes, the extension $M_{\chi\psi,\infty}/K_{\chi,\infty}$ and the character ψ satisfy the conditions of Lemma 5.5, and we can apply this lemma. Thus, we know that $X^{\chi\psi}_{M_{\chi\psi,\infty}}$ is a free $\mathbb{Z}_p[\chi\psi]$-module of finite rank. Hence, $\psi_{\Lambda[G/H]}(J_{G/H}) = \mathrm{Fitt}_{0,\mathbb{Z}_p[\chi\psi][[\mathrm{Gal}(M_{\chi\psi,\infty}/M_{\chi\psi})]]}(X^{\chi\psi}_{M_{\chi\psi,\infty}})$ is the characteristic ideal of $X_{M_{\chi\psi,\infty}}^{\chi\psi}$. If $\chi \neq \omega$ or $\psi \neq 1$, by the Iwasawa main conjecture proved by Wiles [47], we have

$$\mathrm{Fitt}_{0,\mathbb{Z}_p[\chi\psi][[\mathrm{Gal}(M_{\chi\psi,\infty}/M_{\chi\psi})]]}(X_{M_{\chi\psi,\infty}}^{\chi\psi}) = (\theta_{M_{\chi\psi,\infty}}^{\chi\psi}).$$

Hence, we get $\psi_{\Lambda[G/H]}(I_{G/H}) = \psi_{\Lambda[G/H]}(J_{G/H})$ in this case.

Suppose $\chi = \omega$ and $\psi = 1$. Then, by the definition of $\Psi_{G/H}$, we have $G = H$, $M = K$, and $M_\chi = K_\omega = k(\mu_p)$. By Lemma 3.5, $(\Theta'_{K_\infty/k})^\omega$ is generated by $\theta_{K_{\omega,\infty}}^\omega$. Since we assumed the Leopoldt conjecture holds for k, $\theta_{K_{\omega,\infty}}^\omega$ is not in Λ, and $\Theta_{K_\infty/k}^\omega = (\Theta'_{K_{\omega,\infty}/k})^\omega \cap \Lambda$ is generated by the numerator of $\theta_{K_{\omega,\infty}}^\omega$. Therefore, the Iwasawa main conjecture proved by Wiles also implies that $\psi_{\Lambda[G/H]}(I_{G/H}) = \psi_{\Lambda[G/H]}(J_{G/H})$.

So we have checked the properties (i) and (ii) of Corollary 4.2. The properties (iii) and (iv) of Corollary 4.2 for $I_{G/H}$ follow from Lemma 3.3. We will show the properties (iii) and (iv) for $J_{G/H}$. We denote by M and M' the subfields of F corresponding to H and H', respectively. By induction we may assume that $\mathrm{Gal}(M/M')$ is cyclic, and that there is a prime $\mathscr{L}$ of k such that only primes above $\mathscr{L}$ are ramified in M/M'. Corollary 5.3 yields an exact sequence

$$\Big(\bigoplus_{v|\mathscr{L}} I_v\Big)^\chi \xrightarrow{a} (X_{M_\infty}^\chi)_{\mathrm{Gal}(M_\infty/M'_\infty)} \xrightarrow{b} X_{M'_\infty}^\chi \to 0$$

where I_v is the inertia group of v in $\mathrm{Gal}(M_\infty/M'_\infty)$ for a prime v above $\mathscr{L}$. The surjectivity of b implies $c_{H,H'}(J_{G/H}) \subset J_{G/H'}$.

Since I_v is cyclic and only primes above $\mathscr{L}$ are ramified, the image of a is cyclic as a $\Lambda[G/H']$-module. We take generators $e_1, \dots, e_s$ of $X_{M_\infty}^\chi$ as a $\Lambda[G/H]$-module such that the image of e_1 in $(X_{M_\infty}^\chi)_{\mathrm{Gal}(M_\infty/M'_\infty)}$ generates the image of a. Put $N = \sum_{\sigma \in \mathrm{Gal}(M_\infty/M'_\infty)} \sigma$. Since b is induced by the norm map, by the above exact sequence, we have $Ne_1 = 0$. Let $\overline{e_2}, \dots, \overline{e_s}$ denote the image of $e_2, \dots, e_s$ in $X_{M'_\infty}^\chi$ by the map b. Suppose $\sum_{i=2}^s a_{ij}\overline{e_i} = 0$ $(j = 2, 3, \dots)$ are relations of $X_{M'_\infty}^\chi$. We may suppose $\sum_{i=1}^s \tilde{a}_{ij} e_i = 0$ $(j = 1, 2, \dots)$ such that $c_{H,H'}(\tilde{a}_{ij}) = a_{ij}$ for $i, j \geqq 2$, $\tilde{a}_{11} = N$, and $\tilde{a}_{21} = \cdots = \tilde{a}_{s1} = 0$, are relations of $X_{M_\infty}^\chi$. Hence, if x is an $(s-1) \times (s-1)$ minor of the relation matrix of $X_{M'_\infty}^\chi$, we have $N\tilde{x} \in J_{G/H} = \mathrm{Fitt}_{0,\Lambda[G/H]}(X_{M_\infty}^\chi)$ for some $\tilde{x}$ with $c_{H,H'}(\tilde{x}) = x$. But $N\tilde{x} = v_{H',H}(x)$. Hence, $v_{H',H}(J_{G/H'}) \subset J_{G/H}$.

Therefore, we can apply Corollary 4.2 to obtain $I_G = J_G$. This completes the proof of Theorem 0.9.

Remark 6.1. We remark that we did not use the Leopoldt conjecture to prove $\big(\mathrm{Fitt}_{0,\mathbb{Z}_p[\chi][[\mathrm{Gal}(F_\infty/K)]]}(X_{F_\infty}^\chi)\big)_{(\Delta)}^\chi = (\Theta_{F_\infty/k})_{(\Delta)}^\chi$ for $\chi \neq \omega$.

Next, we will prove Corollary 0.10. Put $k = \mathbb{Q}$. The Leopoldt conjecture of course holds for $\mathbb{Q}$. For any abelian extension $F/\mathbb{Q}$, we can take an abelian extension $F''/\mathbb{Q}$ such that $F_\infty = F''_\infty$, p is tamely ramified in F'', and $F'' \cap \mathbb{Q}_\infty = \mathbb{Q}$. So we may assume F satisfies the above conditions. Using (a variant of) Lemma 2.3, we can take F' as in the subsection 3.2 in §3. Hence, F satisfies all conditions in the subsection 3.2. Further, by

Ferrero and Washington [10], we know $\mu = 0$ for any abelian field, so Theorem 0.9 implies Corollary 0.10.

Corollary 6.2. *Let F be an arbitrary abelian number field such that p is ramified in $F/\mathbb{Q}$. Suppose that $\mathrm{Gal}(F/\mathbb{Q}) = \Delta \times G$ where $\#\Delta$ is prime to p, and G is a p-group. Then for a character χ of Δ such that $\chi \neq \omega$, we have*

$$\theta_F^\chi \in \mathrm{Fitt}_{0,\mathbb{Z}_p[\chi][G]}\big((A_F)^\chi_{(\Delta)}\big).$$

This follows from Theorem 0.9, the surjectivity of $X_{F_\infty}^\chi \to A_F^\chi$, and $\theta_F^\chi \in c_{F_\infty/F}(\Theta_{F_\infty/\mathbb{Q}}^\chi)$.

Next, we will prove Theorem 0.4. Using (a variant of) Lemma 2.3, we can take an abelian field F' such that F'/F is an unramified p-extension and F' satisfies (A_p). Since F'/F is a p-extension, no prime above p splits in $F'/(F')^+$. Hence, as in the proof of Theorem 0.9, it is enough to show this theorem for F'. So we may assume F satisfies the assumption (A_p). Let $I_v(F_\infty/F)$ be the inertia group of v in $\mathrm{Gal}(F_\infty/F)$. Our assumption that no prime of F^+ over p splits in F/F^+ implies that the complex conjugation acts trivially on $\bigoplus\limits_{v|p} I_v(F_\infty/F)$ where the sum is taken over the primes of F above p. Hence, $\Big(\bigoplus\limits_{v|p} I_v(F_\infty/F)\Big)^- = 0$. By Proposition 5.2, this implies that $(X_{F_\infty}^-)_{\mathrm{Gal}(F_\infty/F)} \xrightarrow{\simeq} A_F^-$ is an isomorphism. Let $c_{F_\infty/F} : \mathbb{Z}_p[[\mathrm{Gal}(F_\infty/\mathbb{Q})]] \to \mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})]$ be the natural map. By Theorem 0.9 and the above isomorphism, we have

$$\begin{aligned}\mathrm{Fitt}_{0,\mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})]}(A_F^-) &= c_{F_\infty/F}\big(\mathrm{Fitt}_{0,\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/\mathbb{Q})]]}(X_{F_\infty}^-)\big)\\ &= c_{F_\infty/F}(\Theta_{F_\infty/\mathbb{Q}}^-).\end{aligned}$$

Hence, $\mathrm{Fitt}_{0,\mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})]}(A_F^-)^- \subset \Theta_{F/\mathbb{Q}}^- \otimes \mathbb{Z}_p$ by Lemmas 3.1 and 3.2.

It follows from the following Lemma 6.3 that

$$\#A_F^- \geqq \big(\mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})]^- : \mathrm{Fitt}_{0,\mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})]}(A_F^-)^-\big) \geqq \big(\mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})]^- : \Theta_{F/\mathbb{Q}}^- \otimes \mathbb{Z}_p\big).$$

On the other hand, by Sinnott's theorem ([40], Theorems 2.1 and 5.4), we have $\big(\mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})]^- : \Theta_{F/\mathbb{Q}}^- \otimes \mathbb{Z}_p\big) = \#A_F^-$. (Let F' be the abelian field satisfying the condition (A) such that F'/F is unramified and of degree prime to p. In the notation of [40], $R_{F'} = U_{F'}$ by Theorem 5.4 in [40], which implies $R_F \otimes \mathbb{Z}_p = U_F \otimes \mathbb{Z}_p$, hence by Theorem 2.1 in [40] we get the above equality.) Thus, we get

$$\mathrm{Fitt}_{0,\mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})]}(A_F^-)^- = \Theta_{F/\mathbb{Q}}^- \otimes \mathbb{Z}_p.$$

Lemma 6.3.

$$\big(\mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})]^- : \mathrm{Fitt}_{0,\mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})]}(A_F^-)^-\big) \leqq \#A_F^-.$$

To prove Lemma 6.3, we need the following lemma.

Lemma 6.4. *Let $G = G_1 \times \cdots \times G_r$ be a finite abelian p-group such that G_i's are cyclic for all i. Put $c = \#G$. Let R be a semi-local ring such that $R = R_1 \times \cdots \times R_q$ where*

R_j's are rings of integers of local fields of mixed characteristics $(0, p)$, and $\mu_c \subset R_j^\times$ for all j. We use the notation $\mathscr{H}$ and $\Psi_{G/H}$ in §4. For $\psi \in \Psi_{G/H}$, the ring homomorphism $R[G/H] \to R$ induced by ψ is also denoted by ψ. Suppose that for any subgroup $H \in \mathscr{H}$, an ideal $I_{G/H}$ of $R[G/H]$ is given, and for any $H \in \mathscr{H}$ and $\psi \in \Psi_{G/H}$, an element $x_\psi \in R$ is given, and that they satisfy the following properties.

(i) *For any subgroup $H \in \mathscr{H}$ and any character $\psi \in \Psi_{G/H}$, we have*

$$\big(R : \psi(I_{G/H})\big) \leqq \big(R : (x_\psi)\big).$$

(ii) *For any subgroups H and H' in $\mathscr{H}$ such that $H \subset H'$, we have*

$$c_{H,H'}(I_{G/H}) \subset I_{G/H'} \quad \textit{and} \quad v_{H',H}(I_{G/H'}) \subset I_{G/H}$$

where $c_{H,H'} : R[G/H] \to R[G/H']$ and $v_{H',H} : R[G/H'] \to R[G/H]$ are defined as in Lemma 4.1.

Then, we have

$$(R[G] : I_G) \leqq \left(R : \Big(\prod_{H \in \mathscr{H}} \prod_{\psi \in \Psi_{G/H}} x_\psi\Big)\right) = \left(R : \Big(\prod_{\psi \in \hat{G}} x_\psi\Big)\right).$$

Proof of Lemma 6.4. We prove this lemma by the same method as Lemma 4.1, namely by induction on $\#G$. We may assume $\#G > 1$ and $\#G_1 = p^m$ with $m \geqq 1$. Put $N = G_1^{p^{m-1}} \times \{1\} \times \cdots \times \{1\}$ and $\mathscr{G} = G_2 \times \cdots \times G_r$. For a character ψ_1 of G_1, the ring homomorphism $R[G] \to R[\mathscr{G}]$ induced by ψ_1 is denoted by ψ_{1,G_1}. Consider an exact sequence

$$R[G/N]/I_{G/N} \xrightarrow{v_{N,\{1\}}} \Lambda_R[G]/I_G \longrightarrow \bigoplus_{\psi_1} \psi_{1,G_1}(R[G])/\big(\psi_{1,G_1}(I_G)\big)$$

where ψ_1 ranges over faithful characters of G_1.

By the hypothesis of the induction, we can apply this lemma for the group G/N instead of G, and get $(R[G/N] : I_{G/N}) \leqq \left(R : \Big(\prod_{\psi \in (G/N)^\wedge} x_\psi\Big)\right)$. We define $\mathscr{H}'$ as in the proof of Lemma 4.1. For $H' \in \mathscr{H}'$, we define $I_{\mathscr{G}/H'} = \psi_{1,G_1}(I_{G/\{1\}\times H'})$ and $x_{\psi'} = x_{\psi_1\psi'}$ for $\psi' \in \Psi_{\mathscr{G}/H'}$. Then, by the hypothesis of the induction, we obtain $\big(\psi_{1,G_1}(R[G]) : \psi_{1,G_1}(I_G)\big) = (R[\mathscr{G}] : I_{\mathscr{G}}) \leqq \left(R : \Big(\prod_{\psi' \in \hat{\mathscr{G}}} x_{\psi_1\psi'}\Big)\right)$. Hence, by the above exact sequence, we obtain

$$(R[G] : I_G) \leqq \left(R : \Big(\prod_{\psi \in \hat{G}} x_\psi\Big)\right).$$

Proof of Lemma 6.3. Suppose that $\mathrm{Gal}(F/\mathbb{Q}) = \Delta \times G$ where G is a p-group and $\#\Delta$ is prime to p, and that K is the subfield of F fixed by G. Put $c = [F : \mathbb{Q}]$, and $R = \mathbb{Z}_p[\mu_c][\Delta]$. We have $\mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})] \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\mu_c] = R[G]$. To prove this lemma, it is enough to show $\big(R[G]^- : \mathrm{Fitt}_{0,R[G]}(A_F^- \otimes \mathbb{Z}_p[\mu_c])^-\big) \leqq \big(\mathbb{Z}_p[\mu_c] : (\#A_F^-)\big)$.

We use the notation of Lemma 6.4. For $H \in \mathscr{H}$, we denote by M the subfield of F fixed by H. We define $I_{G/H}$ by $I^{+}_{G/H} = (1)$ and $I^{-}_{G/H} = \mathrm{Fitt}_{0,R[G/H]}(A^{-}_{M} \otimes \mathbb{Z}_p[\mu_c])^{-}$. Note that $R = \bigoplus_{\chi} \mathbb{Z}_p[\mu_c]^{\chi}$ where the sum is taken over characters of Δ. We denote an element a of R by $a = (a^{\chi})$ where a^{χ} is the χ-component. Suppose $H \in \mathscr{H}$, and $\psi \in \Psi_{G/H}$. Let $M_{\chi\psi}$ be the subfield of M fixed by $\mathrm{Ker}(\chi\psi)$. We take $x_{\psi} = \big((x_{\psi})^{\chi}\big) \in R$ such that $(x_{\psi})^{\chi} = 1$ if χ is even, and $\#\mathbb{Z}_p[\mu_c]/\big((x_{\psi})^{\chi}\big) = \#(A_{M_{\chi\psi}} \otimes \mathbb{Z}_p[\mu_c])^{\chi\psi}$ if χ is odd (for example, we can take $(x_{\psi})^{\chi} = B_{1,(\chi\psi)^{-1}}$ if χ is odd $\neq \omega$ by Solomon's theorem [42] where $B_{1,(\chi\psi)^{-1}}$ is the first generalized Bernoulli number).

We define M_{χ} as in the proof of Theorem 0.9, then $[M : M_{\chi}]$ is prime to p and $M_{\chi}/M_{\chi\psi}$ is unramified. Hence, as in the proof of Theorem 0.9, by Proposition 5.2, we have an isomorphism $(A^{-}_{M})_{\mathrm{Gal}(M/M_{\chi\psi})} \simeq A^{-}_{M_{\chi\psi}}$. Therefore, we have $\psi(I_{G/H})^{-} = \mathrm{Fitt}_{0,R[\psi]}\big((A^{-}_{M} \otimes \mathbb{Z}_p[\mu_c])^{\psi}_{(G/H)}\big) = \mathrm{Fitt}_{0,R[\psi]}\big(((A^{-}_{M_{\chi\psi}} \otimes \mathbb{Z}_p[\mu_c])^{\chi\psi})\big) = (x_{\psi})$. So the property (i) of Lemma 6.4 is satisfied. The property (ii) of Lemma 6.4 can be checked by the same method as in the proof of Theorem 0.9. So by Lemma 6.4 we have

$$\begin{aligned}\#\big(R[G]/\mathrm{Fitt}_{0,R[G]}(A^{-}_{F} \otimes \mathbb{Z}_p[\mu_c])\big)^{-} &\leqq \#\Big(R/\Big(\prod_{\psi} x_{\psi}\Big)\Big)\\ &= \#\Big(\mathbb{Z}_p[\mu_c]/\prod_{\chi\psi}(x_{\psi})^{\chi}\Big)\\ &= \#\big(\mathbb{Z}_p[\mu_c]/(\#A^{-}_{F})\big).\end{aligned}$$

This completes the proof of Lemma 6.3.

Next, we prove Theorem 0.5. We write $\Delta = \mathrm{Gal}(K/\mathbb{Q})$ and $G = \mathrm{Gal}(F/K)$, then $\mathrm{Gal}(F/\mathbb{Q}) = \Delta \times G$. By our assumption, $G \neq \{1\}$. As in 1.4, we have

$$\mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})] = \bigoplus_{\chi} \mathbb{Z}_p[\chi][G].$$

We put $\mathscr{F}_F = \mathrm{Fitt}_{0,\mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})]}(A^{-}_{F})$, $\Theta_F = \Theta_{F/\mathbb{Q}} \otimes \mathbb{Z}_p$, and $\Theta'_F = (\overline{\Theta}'_{F/\mathbb{Q}})^{(p)}$ ($(\overline{\Theta}'_{F/\mathbb{Q}})^{(p)}$ was defined before Lemma 3.1). Let $(\mathscr{F}_F)^{\chi}$ (resp. $(\Theta_F)^{\chi}$, $(\Theta'_F)^{\chi}$) be the χ-component of $\mathscr{F}_F$ (resp. Θ_F, Θ'_F). Our aim is to show $(\mathscr{F}_F)^{\chi} = (\Theta_F)^{\chi}$ for all odd χ.

Lemma 6.5. *Let K_{χ} be the fixed field of* $\mathrm{Ker}\,\chi$ *in K, and $F_{\chi} = K_{\chi,n}$. We denote by $\theta^{\chi}_{F_{\chi}}$ (resp. $\theta^{\chi}_{K_{\chi}}$) the image of $\theta_{F_{\chi}}$ (resp. $\theta_{K_{\chi}}$) by the map*

$$\mathbb{Q}_p[\mathrm{Gal}(F_{\chi}/\mathbb{Q})] = \mathbb{Q}_p[\mathrm{Gal}(K_{\chi}/\mathbb{Q})][G] \to \mathbb{Q}_p(\chi)[G] \quad (\textit{resp. } \mathbb{Q}_p[\mathrm{Gal}(K_{\chi}/\mathbb{Q})] \to \mathbb{Q}_p(\chi))$$

induced by χ. Then, $(\Theta'_F)^{\chi}$ is generated by $v_{F_{\chi}/K_{\chi}}\theta^{\chi}_{K_{\chi}}$ and $\theta^{\chi}_{F_{\chi}}$ as a $\mathbb{Z}_p[\chi][G]$-module.

Proof. By the same method as Lemma 2.6 (2) (ii), we know that $(\Theta'_F)^{\chi}$ is generated by $v_{F_{\chi}/K_{\chi,m}}\theta^{\chi}_{K_{\chi,m}}$'s with $0 \leqq m \leqq n$. If $m > 0$, then p is ramified in K_m, so $c_{F_{\chi}/K_{\chi,m}}(\theta^{\chi}_{F_{\chi}}) = \theta^{\chi}_{K_{\chi,m}}$. Hence, $v_{F_{\chi}/K_{\chi,m}}(\theta^{\chi}_{K_{\chi,m}})$ is a multiple of $\theta^{\chi}_{F_{\chi}}$. This completes the proof of the lemma.

We go back to the proof of Theorem 0.5. First of all, if $\chi = \omega$, by the above lemma we have $(\mathscr{F}_F)^{\chi} = (\Theta_F)^{\chi} = (1)$. So we may assume $\chi \neq \omega$. We consider

$$\mathbb{Z}_p[[\mathrm{Gal}(K_\infty/\mathbb{Q})]] = \bigoplus_{\chi} \mathbb{Z}_p[\chi][[\mathrm{Gal}(K_\infty/K)]].$$

Let $(\mathscr{F}_{K_\infty})^\chi$ (resp. $(\Theta_{K_\infty})^\chi$) be the χ-component of $\mathrm{Fitt}_{0,\mathbb{Z}_p[[\mathrm{Gal}(K_\infty/\mathbb{Q})]]}(X_{K_\infty}^-)$ (resp. $\Theta_{K_\infty/\mathbb{Q}}$).

We first assume $\chi(p) \neq 1$. Since $c_{F_\chi/K_\chi}(\theta_{F_\chi}^\chi) = (1-\chi(p)^{-1})\theta_{K_\chi}^\chi$ and $1-\chi(p)^{-1}$ is a unit (the order of χ is prime to p), $\theta_{K_\chi}^\chi$ is a multiple of $c_{F_\chi/K_\chi}(\theta_{F_\chi}^\chi)$, and $v_{F_\chi/K_\chi}\theta_{K_\chi}^\chi$ is a multiple of $\theta_{F_\chi}^\chi$. Hence, $(\Theta_F)^\chi$ is generated by $\theta_{F_\chi}^\chi$ by Lemma 6.5 (note that $(\Theta_F')^\chi = (\Theta_F)^\chi$ because $\chi \neq \omega$). So we have $c_{K_\infty/F}((\Theta_{K_\infty})^\chi) = (\Theta_F)^\chi$ by Lemma 3.5.

On the other hand, by Proposition 5.2 and $\chi(p) \neq 1$, $(X_{K_\infty}^\chi)_{\mathrm{Gal}(K_\infty/F)} \xrightarrow{\simeq} A_F^\chi$ is bijective. Hence, $c_{K_\infty/F}((\mathscr{F}_{K_\infty})^\chi) = (\mathscr{F}_F)^\chi$. So Theorem 0.9 (the usual Iwasawa main conjecture) implies $(\mathscr{F}_F)^\chi = (\Theta_F)^\chi$.

Next, we assume $\chi(p) = 1$. By Proposition 5.2, we have an exact sequence

$$(*) \qquad 0 \to \mathbb{Z}_p[\chi] \otimes_{\mathbb{Z}_p} \mathrm{Gal}(K_\infty/F) \xrightarrow{\alpha_1} (X_{K_\infty}^\chi)_{\mathrm{Gal}(K_\infty/F)} \to A_F^\chi \to 0.$$

Recall that $G = \mathrm{Gal}(F/K)$ is cyclic of order p^n. Put $N = N_G = \sum_{\sigma \in G} \sigma$, and for a $\mathbb{Z}_p[\chi][G]$-module M, we write $M^{N=0}$ (resp. $M/(N)$) for the kernel (resp. the cokernel) of $N : M \to M$.

Lemma 6.6. *$(X_{K_\infty}^\chi)_{\mathrm{Gal}(K_\infty/F)}/(N) \xrightarrow{\simeq} A_F^\chi/(N)$ is an isomorphism.*

Proof. The exact sequence $(*)$ yields an exact sequence

$$(A_F^\chi)^{N=0} \xrightarrow{\delta} (\mathbb{Z}_p[\chi]/p^n) \otimes_{\mathbb{Z}_p} \mathrm{Gal}(K_\infty/F) \to ((X_{K_\infty}^\chi)_{\mathrm{Gal}(K_\infty/F)})/(N) \to A_F^\chi/(N) \to 0.$$

We will compute the boundary homomorphism δ, and show its surjectivity. Applying Proposition 5.2 to K_∞/F and K_∞/K, we have a commutative diagram of exact sequences

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z}_p[\chi] \otimes_{\mathbb{Z}_p} \mathrm{Gal}(K_\infty/F) \arrow[r, "\alpha_1"] \arrow[d] & (X_{K_\infty}^\chi)_{\mathrm{Gal}(K_\infty/F)} \arrow[r] \arrow[d] & A_F^\chi \arrow[r] \arrow[d, "N_{F/K}"] & 0 \\
0 \arrow[r] & \mathbb{Z}_p[\chi] \otimes_{\mathbb{Z}_p} \mathrm{Gal}(K_\infty/K) \arrow[r, "\alpha_2"] & (X_{K_\infty}^\chi)_{\mathrm{Gal}(K_\infty/K)} \arrow[r] & A_K^\chi \arrow[r] & 0.
\end{tikzcd}$$

Let σ_0 be a generator of $\mathrm{Gal}(K_\infty/K)$, and put $x = \alpha_2(1 \otimes \sigma_0)$ (α_2 is the map in the above diagram). We take an element $y \in (X_{K_\infty}^\chi)_{\mathrm{Gal}(K_\infty/F)}$ which is mapped to x, and define z to be the image of y in A_F^χ. Since $N_{F/K}(z) = 0$, z is in $(A_F^\chi)^{N=0}$. We will compute $\delta(z)$. Since both Ny and $\alpha_1(1 \otimes p^n\sigma_0)$ are mapped to $p^n x$ in $(X_{K_\infty}^\chi)_{\mathrm{Gal}(K_\infty/K)}$ and Ny is in the image of α_1, we have $Ny = \alpha_1(1 \otimes p^n\sigma_0)$. This shows that $\delta(z) = 1 \otimes p^n\sigma_0$. Since $p^n\sigma_0$ is a generator of $\mathrm{Gal}(K_\infty/F)$, δ is surjective and we obtain the conclusion of this lemma.

Since $\mathrm{Fitt}_{0,\mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]]}(X_{K_\infty}^\chi) = (\theta_{K_\infty}^\chi)$ by the Iwasawa main conjecture, this lemma implies that $\mathrm{Fitt}_{0,\mathbb{Z}_p[\chi][G]/(N)}(A_F^\chi/(N)) = (\theta_{F_\chi}^\chi)$. From the surjectivity of $X_{K_\infty}^\chi \to A_F^\chi$, $\theta_{F_\chi}^\chi$ belongs to $\mathscr{F}_F^\chi$, so the above says that $\mathscr{F}_F^\chi$ is generated by $\theta_{F_\chi}^\chi$ and some elements of the form Nx. Using the exact sequence

$$0 \to \mathbb{Z}_p[\chi]/p^n \otimes_{\mathbb{Z}_p} \mathrm{Gal}(F/K) \to (A_F^\chi)_{\mathrm{Gal}(F/K)} \to A_K^\chi \to 0$$

which is obtained from Proposition 5.2, we know $\nu_{F_\chi/K_\chi}(\mathrm{Fitt}_{0,\mathbb{Z}_p[\chi]}(A_K^\chi)) \subset \mathscr{F}_F^\chi$ by the same method as in the proof of Theorem 0.9. By the calculation of the order of A_K^χ by Mazur and Wiles [26], Chap. 1, §10, Theorem 2, we have $\mathrm{Fitt}_{0,\mathbb{Z}_p[\chi]}(A_K^\chi) = (\theta_{K_\chi}^\chi)$. So $\nu_{F_\chi/K_\chi}(\theta_{K_\chi}^\chi) \in \mathscr{F}_F^\chi$. Suppose that Nx belongs to $\mathscr{F}_F^\chi$. This implies that $p^n c_{F/K}(x)$ is in $\mathrm{Fitt}_{0,\mathbb{Z}_p[\chi]}((A_F^\chi)_{\mathrm{Gal}(F/K)})$ which is equal to $(p^n\theta_{K_\chi}^\chi)$ by the above exact sequence. Hence, $c_{F/K}(x)$ is a multiple of $\theta_{K_\chi}^\chi$. Thus, Nx is a multiple of $\nu_{F_\chi/K_\chi}(\theta_{K_\chi}^\chi)$, and we know that $\mathscr{F}_F^\chi$ is generated by $\theta_{F_\chi}^\chi$ and $\nu_{F_\chi/K_\chi}(\theta_{K_\chi}^\chi)$. Hence, by Lemma 6.5 we have $\mathscr{F}_F^\chi = \Theta_F^\chi$. This completes the proof of Theorem 0.5.

7. Proof of the theorems II

In this section, we prove Theorem 0.6. We use the argument of Wiles and Greither [48], [14], namely the argument of avoiding the trivial zeros. I learned the method here from Greither [14], §4.

First of all, using (a variant of) Lemma 2.3, we can take an abelian field F' such that F'/F is an unramified p-extension and F' satisfies (A_p). Since F'/F is a p-extension, $\mu_p \not\subset F'$. We know p is tamely ramified in F' because F'/F is unramified. So it suffices to show this theorem for F', and we may assume F satisfies the condition (A_p).

We first prove this theorem under the assumption that p is unramified in $F/\mathbb{Q}$. We fix a positive integer N and take a prime number r such that

(i) r is unramified in $F/\mathbb{Q}$,

(ii) $r \equiv 1 \pmod{p^N}$,

(iii) no prime above r splits in F/F^+,

(iv) if we denote by k_{r,p^N} the subfield of $\mathbb{Q}(\mu_r)$ with degree p^N, the Frobenius φ_p of p in $\mathrm{Gal}(k_{r,p^N}/\mathbb{Q})$ generates $\mathrm{Gal}(k_{r,p^N}/\mathbb{Q})$.

The existence of r follows from Proposition 4.1 in Greither [14], which was proved by using Chebotarev density theorem. Put $E = Fk_{r,p^N}$. We use the notation A_F, A_E, X_{E_∞}, etc. as in the previous section. Since p is unramified in E, $\bigoplus_{v|p} \mathbb{Z}_p$ (v ranges over primes of E above p) is isomorphic to $\mathbb{Z}_p[\mathrm{Gal}(E/\mathbb{Q})]/(\varphi_p - 1)$ where $\varphi_p \in \mathrm{Gal}(E/\mathbb{Q})$ is the Frobenius of p. By Proposition 5.2, we have an exact sequence

$$\left(\mathbb{Z}_p[\mathrm{Gal}(E/\mathbb{Q})]/(\varphi_p - 1)\right)^- \to (X_{E_\infty})^-_{\mathrm{Gal}(E_\infty/E)} \to A_E^- \to 0.$$

We take N and M sufficiently large such that p^{N-M} is greater than the p-component of $\#\mathrm{Gal}(F/\mathbb{Q})$, and put $\nu = \sum_{i=0}^{p^M-1} \sigma^{ip^{N-M}}$ where σ is a generator of $\mathrm{Gal}(k_{r,p^N}/\mathbb{Q})$. Put $R_E = \mathbb{Z}_p[\mathrm{Gal}(E/\mathbb{Q})]$, $\mathscr{R} = R_E/(\nu)$, and $R_F = \mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})]$.

The next lemma is a fundamental property of Fitting ideals, which can be easily proved ([28], p. 61, Exercise 2).

Lemma 7.1. *Let R be a commutative ring. If $M_1 \to M_2 \to M_3 \to 0$ is an exact sequence of finitely generated R-modules, we have*

$$\mathrm{Fitt}_{0,R}(M_1)\,\mathrm{Fitt}_{0,R}(M_3) \subset \mathrm{Fitt}_{0,R}(M_2).$$

Applying Lemma 7.1 to the above exact sequence tensoring $\otimes_{R_E} \mathscr{R}$, we have

$$(\varphi_p - 1)\,\mathrm{Fitt}_{0,\mathscr{R}}\big(A_E^-/(v)\big) \subset \mathrm{Fitt}_{0,\mathscr{R}}\big(((X_{E_\infty}^-)_{\mathrm{Gal}(E_\infty/E)})/(v)\big).$$

By Theorem 0.9, we have $\mathrm{Fitt}_{0,\mathbb{Z}_p[[\mathrm{Gal}(E_\infty/\mathbb{Q})]]}(X_{E_\infty}^-)^- = \Theta_{E_\infty/\mathbb{Q}}^-$. Note that E satisfies the condition (A_p) because we assumed F satisfies (A_p). Since p is unramified in $E/\mathbb{Q}$, μ_p is not contained in E, hence $\mu_p \not\subset E_n$ for $n \geqq 0$. This implies $(\overline{\Theta}'_{E_n/\mathbb{Q}})^{(p)} \subset \mathbb{Z}_p[\mathrm{Gal}(E_n/\mathbb{Q})]$ $((\overline{\Theta}'_{E_n/\mathbb{Q}})^{(p)}$ was defined before Lemma 3.1) and $(\Theta'_{E_\infty/\mathbb{Q}})^{(p)} \subset \mathbb{Z}_p[[\mathrm{Gal}(E_\infty/\mathbb{Q})]]$. So $(\Theta'_{E_\infty/\mathbb{Q}})^{(p)} = \Theta_{E_\infty/\mathbb{Q}}$, and $(\overline{\Theta}'_{E_n/\mathbb{Q}})^{(p)} = (\overline{\Theta}_{E_n/\mathbb{Q}})^{(p)}$. Since p is unramified in $E/\mathbb{Q}$, by Lemma 2.1 and the definitions of $(\Theta'_{E_\infty/\mathbb{Q}})^{(p)}$ and $(\overline{\Theta}'_{E/\mathbb{Q}})^{(p)}$, we get

$$\begin{aligned} c_{E_\infty/E}\big((\Theta'_{E_\infty/\mathbb{Q}})^{(p)}\big) &= (1-\varphi_p^{-1})(\overline{\Theta}'_{E/\mathbb{Q}})^{(p)} = (1-\varphi_p^{-1})(\overline{\Theta}_{E/\mathbb{Q}})^{(p)} \\ &= (1-\varphi_p^{-1})\Theta_{E/\mathbb{Q}} \otimes \mathbb{Z}_p \end{aligned}$$

where the last equality follows from Lemma 3.1. Therefore, we have

$$(\varphi_p - 1)\,\mathrm{Fitt}_{0,\mathscr{R}}\big(A_E^-/(v)\big)^- \subset (\varphi_p - 1)(\Theta_{E/\mathbb{Q}} \otimes \mathbb{Z}_p)^- \bmod (v).$$

Since we took N and M such that p^{N-M} is greater than the p-component of $\#\mathrm{Gal}(F/\mathbb{Q})$, $\varphi_p - 1$ is a nonzero divisor in $\mathscr{R}$. Hence, we obtain

$$\mathrm{Fitt}_{0,\mathscr{R}}\big(A_E^-/(v)\big) \subset (\Theta_{E/\mathbb{Q}} \otimes \mathbb{Z}_p)^- \bmod (v).$$

Let φ_r be the Frobenius of r in $\mathrm{Gal}(F/\mathbb{Q})$. Since no prime above r splits in F/F^+, $(\varphi_r - 1)^-$ is a unit in $\mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})]^-$. Hence, by Lemma 2.1 we have $c_{E/F}\big((\Theta_{E/\mathbb{Q}} \otimes \mathbb{Z}_p)^-\big) = (\Theta_{F/\mathbb{Q}} \otimes \mathbb{Z}_p)^-$ (note that the ramifying primes in E/F are the primes above r). We also have

$$\Big(\bigoplus_{v|r} \mathbb{Z}/p^N\Big)^- \ (v \text{ ranges over primes of } F \text{ above } r) \simeq \big(\mathbb{Z}/p^N[\mathrm{Gal}(F/\mathbb{Q})]/(\varphi_r - 1)\big)^- = 0.$$

Hence by Proposition 5.2, we get an isomorphism $(A_E^-)_{\mathrm{Gal}(E/F)} \simeq A_F^-$, so an isomorphism $\big(A_E^-/(v)\big)_{\mathrm{Gal}(E/F)} \simeq A_F^-/p^M$. Consider the map $\mathscr{R} \to R_F/p^M$ defined by $\sigma \mapsto 1$. The above inclusion for the Fitting ideal of $A_E^-/(v)$ implies

$$\mathrm{Fitt}_{0,R_F/p^M}(A_F^-/p^M)^- \subset (\Theta_{F/\mathbb{Q}} \otimes \mathbb{Z}/p^M)^-.$$

This holds for any M, hence we obtain $\mathrm{Fitt}_{0,R_F}(A_F^-)^- \subset (\Theta_{F/\mathbb{Q}} \otimes \mathbb{Z}_p)^-$.

On the other hand, by the same method as the proof of Theorem 0.4, we have

$$\big(R_F^- : \mathrm{Fitt}_{0,R_F}(A_F^-)^-\big) = (R_F^- : \Theta_{F/\mathbb{Q}}^- \otimes \mathbb{Z}_p) = \#A_F^-.$$

Hence, the inclusion $\mathrm{Fitt}_{0,R_F}(A_F^-)^- \subset (\Theta_{F/\mathbb{Q}} \otimes \mathbb{Z}_p)^-$ implies the equality. This completes the proof in the case p is unramified.

Next, we prove Theorem 0.6 under the assumption that p is tamely ramified and $\mu_p \not\subset F$. As in the proof of Theorem 0.9, we write $\mathrm{Gal}(F/\mathbb{Q}) = \Delta \times G$ where $\#\Delta$ is prime to p and G is a p-group. It is enough to show $\mathrm{Fitt}_{0,R_F}(A_F)^\chi = (\Theta_{F/\mathbb{Q}} \otimes \mathbb{Z}_p)^\chi$ for all odd characters χ of Δ. As in the proof of Theorem 0.9, we denote by F_χ (resp. K_χ) the fixed field of the kernel of χ (resp. the fixed field of $\mathrm{Ker}\,\chi \times G$) in F. Let I_p (resp. D_p) be the inertia group (resp. the decomposition group) of p in $\mathrm{Gal}(F/\mathbb{Q})$. By our assumption, I_p is a subgroup of Δ.

Case (i). Suppose that $\chi_{|I_p} \neq 1$. Then,

$$\Bigl(\bigoplus_{v|p} \mathbb{Z}_p\Bigr)^\chi \text{ (v ranges over primes of F above p)} \simeq \mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})/D_p]^\chi = 0$$

because there is $\sigma \in D_p$ such that $\chi(\sigma) - 1$ is a unit. It follows from Proposition 5.2 that $(X_{F_\infty}^\chi)_{\mathrm{Gal}(F_\infty/F)} \simeq A_F^\chi$ is an isomorphism. Hence,

$$c_{F_\infty/F}\bigl(\mathrm{Fitt}_{0,\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/\mathbb{Q})]]}(X_{F_\infty}^\chi)\bigr) = \mathrm{Fitt}_{0,R_F}(A_F^\chi).$$

On the other hand, we will show

$$c_{F_\infty/F}\bigl((\Theta_{F_\infty/\mathbb{Q}})^\chi\bigr) = (\Theta_{F/\mathbb{Q}} \otimes \mathbb{Z}_p)^\chi.$$

Suppose $M \in (\mathcal{M}_{F/\mathbb{Q}})^{(p)}$ and p is unramified in $M/\mathbb{Q}$. Then, $I_p \subset \mathrm{Gal}(F/M)$, so $\bigl(v_{F/M}(\theta_M)\bigr)^\chi = 0$. Hence, by Lemma 3.2 we have $c_{F_\infty/F}\bigl((\Theta'_{F_\infty/\mathbb{Q}})^\chi\bigr) = (\overline{\Theta}'_{F/\mathbb{Q}})^\chi$. Further, by our assumption $\mu_p \not\subset F$, we have $(\overline{\Theta}'_{F/\mathbb{Q}})^{(p)} \subset R_F$ and $(\Theta'_{F_\infty/\mathbb{Q}})^{(p)} \subset \mathbb{Z}_p[[\mathrm{Gal}(F_\infty/\mathbb{Q})]]$. Hence, $(\Theta'_{F_\infty/\mathbb{Q}})^{(p)} = \Theta_{F_\infty/\mathbb{Q}}$ and $(\overline{\Theta}'_{F/\mathbb{Q}})^{(p)} = (\overline{\Theta}_{F/\mathbb{Q}})^{(p)} = \Theta_{F/\mathbb{Q}} \otimes \mathbb{Z}_p$ by Lemma 3.1. Thus, we obtained $c_{F_\infty/F}\bigl((\Theta_{F_\infty/\mathbb{Q}})^\chi\bigr) = (\Theta_{F/\mathbb{Q}} \otimes \mathbb{Z}_p)^\chi$. Therefore, Theorem 0.9 implies $\mathrm{Fitt}_{0,R_F}(A_F)^\chi = (\Theta_{F/\mathbb{Q}} \otimes \mathbb{Z}_p)^\chi$.

Case (ii). Suppose that $\chi_{|I_p} = 1$. Since $[F : F_\chi]$ is prime to p, $(A_F)_{\mathrm{Gal}(F/F_\chi)} \simeq (A_{F_\chi})$ is bijective. So, $\mathrm{Fitt}_{0,R_F}(A_F)^\chi = \mathrm{Fitt}_{0,R_{F_\chi}}(A_{F_\chi})^\chi$.

On the other hand, by the same method as Lemma 2.6, using that $[F : F_\chi]$ is prime to p, we can check that $(\Theta_{F/\mathbb{Q}} \otimes \mathbb{Z}_p)^\chi = (\Theta_{F_\chi/\mathbb{Q}} \otimes \mathbb{Z}_p)^\chi$. So this case is reduced to Theorem 0.6 for F_χ. But since p is unramified in $F_\chi/\mathbb{Q}$, we have already proved that Theorem 0.6 is true for F_χ. This completes the proof of Theorem 0.6.

8. Higher Fitting ideals

Let F/k be as in Theorem 0.9. In this section we study the higher Fitting ideals $\mathrm{Fitt}_{i,\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/k)]]}(X_{F_\infty})^-$. (For more about the higher Fitting ideals of ideal class groups, see [24].)

Suppose that F/k satisfies the conditions in the subsection 3.2 in §3. We consider an abelian extension L/k such that $F \subset L$, $\mathrm{Gal}(L/k) = \mathrm{Gal}(F/k) \times \mathrm{Gal}(L/F)$, $[L : F]$ is a power of p, and L/k satisfies the conditions of F/k in the subsection 3.2. Put $G = \mathrm{Gal}(L/F)$, $\Lambda_{F_\infty} = \mathbb{Z}_p[[\mathrm{Gal}(F_\infty/k)]]$, and

$$\Lambda_{L_\infty} = \mathbb{Z}_p[[\mathrm{Gal}(L_\infty/k)]] = \Lambda_{F_\infty}[G].$$

We fix an isomorphism

$$G \simeq \mathbb{Z}/p^{n_1} \times \cdots \times \mathbb{Z}/p^{n_r}$$

and take generators $\sigma_1, \dots, \sigma_r$ of order p^{n_i} of G, which correspond to the above decomposition. We have a non canonical isomorphism

$$\Lambda_{L_\infty} = \Lambda_{F_\infty}[G] \simeq \Lambda_{F_\infty}[S_1, \dots, S_r]/\big((1+S_1)^{p^{n_1}} - 1, \dots, (1+S_r)^{p^{n_r}} - 1\big)$$

where S_i's are indeterminates, and σ_i corresponds to $1 + S_i$. For $x \in \Lambda_{L_\infty}$, we write

$$x = \sum \delta_{i_1,\dots,i_r}(x) S_1^{i_1} \dots S_r^{i_r} \mod I$$

where $I = \big((1+S_1)^{p^{n_1}} - 1, \dots, (1+S_r)^{p^{n_r}} - 1\big)$ and $\delta_{i_1,\dots,i_r}(x)$'s are in Λ_{F_∞}.

We take N sufficiently large, and choose L such that $n_1, \dots, n_r \geqq N$. We consider $i_1, \dots, i_r$, and s such that $0 \leqq s < N$, and $i_1, \dots, i_r < p^{s+1}$. For $i < p^{s+1}$, one can easily check that $\mathrm{ord}_p\left(\binom{p^N}{i}\right) = \mathrm{ord}_p\big(p^N!/\big(i!(p^N - i)!\big)\big) \geqq N - s$. So $\delta_{i_1,\dots,i_r}(x)$ is well defined $\mathrm{mod}\, p^{N-s}$. This $\delta_{i_1,\dots,i_r}(x)$ does depend on the choice of the generators $\sigma_1, \dots, \sigma_r$.

Theorem 8.1. *Assume that L_∞ satisfies the conditions of Theorem* 0.9 *for F_∞. For any $x \in (\Theta_{L_\infty/k})^-$, $\delta_{i_1,\dots,i_r}(x) \bmod p^{N-s}$ is in $\mathrm{Fitt}_{i,\Lambda_{F_\infty/p^{N-s}}}(X_{F_\infty}/p^{N-s})^-$ where $i = i_1 + \cdots + i_r$.*

Proof. By Theorem 0.9, we have $x \in \mathrm{Fitt}_{0,\Lambda_{L_\infty}}(X_{L_\infty})^-$. Since $X_{L_\infty} \to (X_{L_\infty})_G$ is surjective, we have $\mathrm{Fitt}_{0,\Lambda_{L_\infty}}(X_{L_\infty}) \subset \mathrm{Fitt}_{0,\Lambda_{L_\infty}}\big((X_{L_\infty})_G\big)$, and $x \in \mathrm{Fitt}_{0,\Lambda_{L_\infty}}\big((X_{L_\infty})_G\big)^-$. On the other hand, since S_i's act on $(X_{L_\infty})_G$ as zero, $\mathrm{Fitt}_{0,\Lambda_{L_\infty}}\big((X_{L_\infty})_G\big)$ can be written as

$$\begin{aligned} \mathrm{Fitt}_{0,\Lambda_{L_\infty}}\big((X_{L_\infty})_G\big) = {} & \mathrm{Fitt}_{0,\Lambda_{F_\infty}}\big((X_{L_\infty})_G\big) + \mathrm{Fitt}_{1,\Lambda_{F_\infty}}\big((X_{L_\infty})_G\big)J \\ & + \mathrm{Fitt}_{2,\Lambda_{F_\infty}}\big((X_{L_\infty})_G\big)J^2 + \cdots \end{aligned}$$

where $J = (S_1, \dots, S_r)$. This fact together with $x \in \mathrm{Fitt}_{0,\Lambda_{F_\infty}}\big((X_{L_\infty}^-)_G\big)$ implies that $\delta_{i_1,\dots,i_r}(x) \bmod p^{N-s}$ is in $\mathrm{Fitt}_{i,\Lambda_{F_\infty}/p^{N-s}}\big((X_{L_\infty})_G/p^{N-s}\big)^-$. Since the norm map induces a surjective homomorphism

$$(X_{L_\infty}^-)_G/p^{N-s} \to X_{F_\infty}^-/p^{N-s},$$

we obtain $\delta_{i_1,\dots,i_r}(x) \bmod p^{N-s} \in \mathrm{Fitt}_{i,\Lambda_{F_\infty}/p^{N-s}}(X_{F_\infty}^-/p^{N-s})^-$. □

We can define $\delta_{i_1,\dots,i_r}(x)$ for $x \in \Theta_{L/k}^-$ similarly. For a character χ of $\mathrm{Gal}(F/\mathbb{Q})$ whose order is prime to p, the element $\delta_{1,\dots,1}(\theta_L^\chi)$ appears in the argument of the Euler systems after some computation of the "derivative" operator. The statement like Theorem 8.1 is usually obtained by the argument of Euler system.

Using the Euler system of the Gauss sums, Rubin determined the structure of $A_{\mathbb{Q}(\mu_p)}^-$ in [32], Theorem 4.4 (cf. also Kolyvagin [21], Theorem 7). By using Fitting ideals, his theorem can be written as

Theorem (Rubin). *For $F = \mathbb{Q}(\mu_p)$, $\mathrm{Fitt}_{i,\mathbb{Z}/p^N[\mathrm{Gal}(F/\mathbb{Q})]}(Cl_F^-/p^N)^-$ is generated by $\Theta_{F/\mathbb{Q}}^-$ and $\delta_{1,\dots,1}(x)$'s where x ranges over elements of $(\Theta_{L/\mathbb{Q}} \otimes \mathbb{Z}_p)^-$ and L ranges over the abelian fields as above.*

It is also remarked in Rubin [32] that the same result is true for $\mathbb{Q}(\mu_m)$ as long as p does not divide $[\mathbb{Q}(\mu_m) : \mathbb{Q}]$. For a generalization to CM fields, see [24].

Let χ be an odd Dirichlet character, and F be the fixed field of $\mathrm{Ker}(\chi)$ (so $\mathrm{Gal}(F/\mathbb{Q}) \simeq \mathrm{Image}(\chi)$). Put $\Lambda_\chi = \Lambda_{F_\infty}^\chi = \mathbb{Z}_p[\chi][[\mathrm{Gal}(F_\infty/F)]]$. We consider the χ-quotient $X_{F_\infty}^\chi$ which is a Λ_χ-module. We assume that the order of χ is prime to p and $\chi(p) \neq 1$.

Conjecture 8.2. *We take N and s such that N, s, and $N - s$ are large enough. For any $i > 0$, the higher Fitting ideal $\mathrm{Fitt}_{i,\Lambda_\chi/p^{N-s}}(X_{F_\infty}^\chi/p^{N-s})$ is generated by $\Theta_{F_\infty/\mathbb{Q}}^\chi$ and $\delta_{i_1,\dots,i_r}(x)$'s where*

(i) *L ranges over all abelian fields such that $L \cap F_\infty = F$,*

$$\mathrm{Gal}(L/\mathbb{Q}) = \mathrm{Gal}(F/\mathbb{Q}) \times \mathrm{Gal}(L/F),$$

and $\mathrm{Gal}(L/F)$ is a p-group with $\mathrm{Gal}(L/F) \simeq \mathbb{Z}/p^{n_1} \times \cdots \times \mathbb{Z}/p^{n_r}$ where $n_1, \dots, n_r \geqq N$ as above,

(ii) *x ranges over all elements of $(\Theta_{L_\infty/\mathbb{Q}})_{(\Delta)}^\chi$, and*

(iii) *$(i_1, \dots, i_r)$ ranges over all integers satisfying $i_1, \dots, i_r < p^{s+1}$ and $i_1 + \cdots + i_r \leqq i$.*

Remark 8.3. Schoof asked an interesting question on a certain initial Fitting ideal concerning the minus part of the ideal class group of an abelian field, which is related to the above conjecture, before the argument of the Euler system was discovered [34]. (His question itself has not yet been answered because he considers only cyclic extensions L/F.) An idea to study the initial Fitting ideal of $(X_{L_\infty})_G$ as a Λ_{L_∞}-module, which I used in the proof of Theorem 8.1, was originally in Schoof [34].

Concerning Conjecture 8.2, in this paper we only show

Theorem 8.4. *In the situation of Conjecture 8.2, we fix $N > 0$, and put $\mathscr{S} = \{\ell : \text{prime number} \mid \ell \equiv 1 \pmod{p^N} \text{ and } \ell \text{ is unramified in } F/\mathbb{Q}\}$, and $\mathscr{L} = \{L : \text{the subfield of } F(\mu_\ell) \text{ such that } [L : F] = p^N \mid \ell \in \mathscr{S}\}$. Then, the ideal $\mathrm{Fitt}_{1,\Lambda_\chi/p^N}(X_{F_\infty}^\chi/p^N)$ is generated by $\theta_{F_\infty}^\chi$ and $\delta_1(\theta_{L_\infty}^\chi)$'s for all $L \in \mathscr{L}$. Namely, Conjecture 8.2 is true for $i = 1$.*

Proof. We may assume $\chi \neq \omega$. Let $\mathscr{F}$ be the ideal generated by $\theta_{F_\infty}^\chi$ and $\delta_1(\theta_{L_\infty}^\chi)$'s. By Theorem 8.1 we have $\mathscr{F} \subset \mathrm{Fitt}_{1,\Lambda_\chi/p^N}(X_{F_\infty}^\chi/p^N)$, hence it is enough to show $\mathrm{Fitt}_{1,\Lambda_\chi/p^N}(X_{F_\infty}^\chi/p^N) \subset \mathscr{F}$.

We first remark some properties of $X_{F_\infty}^\chi$ and $A_{F_n}^\chi$. Since $X_{F_\infty}^\chi$ is a free $\mathbb{Z}_p[\chi]$-module of finite rank, if there is a surjective homomorphism $(\Lambda_\chi)^m \to X_{F_\infty}^\chi$, its kernel is a free Λ_χ-module of rank m (because $X_{F_\infty}^\chi$ is an elementary Λ_χ-module in the sense of Northcott [28], p. 80). We take generators of $X_{F_\infty}^\chi$ and consider an exact sequence

$$0 \to (\Lambda_\chi)^m \xrightarrow{f} (\Lambda_\chi)^m \xrightarrow{g} X_{F_\infty}^\chi \to 0$$

of Λ_χ-modules. We denote by $A \in M_m(\Lambda_\chi)$ the matrix corresponding to the Λ_χ-homomorphism f.

For $n > 0$, we put $\Gamma_n = \mathrm{Gal}(F_\infty/F_n)$, and $\Lambda_n = \mathbb{Z}_p[\chi][\mathrm{Gal}(F_n/F)]$. By our assumption $\chi(p) \neq 1$, $(X_{F_\infty}^\chi)_{\Gamma_n} \xrightarrow{\simeq} A_{F_n}^\chi$ is an isomorphism. The map g defines generators of $X_{F_\infty}^\chi$ and $A_{F_n}^\chi$. We take n sufficiently large. Let Div_{F_n} be the group of fractional ideals of F_n. We consider an exact sequence

$$(F_n^\times \otimes \mathbb{Z}_p)^\chi \xrightarrow{\mathrm{div}} (\mathrm{Div}_{F_n} \otimes \mathbb{Z}_p)^\chi \to A_{F_n}^\chi \to 0.$$

We choose primes $v_1, \dots, v_m$ of degree 1 by Chebotarev density theorem such that the subgroup M generated by $v_1, \dots, v_m$ in $(\mathrm{Div}_{F_n} \otimes \mathbb{Z}_p)^\chi$ is a free Λ_n-module of rank m, and that the classes of $v_1, \dots, v_m$ correspond to the generators of $A_{F_n}^\chi \simeq (X_{F_\infty}^\chi)_{\Gamma_n}$ which we took. Namely, the map $M \simeq (\Lambda_n)^m \to A_{F_n}^\chi$ is induced by the above map g. Since $M \simeq (\Lambda_n)^m \to A_{F_n}^\chi$ is surjective and $(X_{F_\infty}^\chi)^{\Gamma_n} = 0$, its kernel M' is a free Λ_n-module of rank m.

We choose basis of M' and take an isomorphism $M' \simeq (\Lambda_n)^m$ such that $M' \simeq (\Lambda_n)^m \to M \simeq (\Lambda_n)^m$ is induced by f. We have an exact sequence

$$0 \to M' \xrightarrow{\bar{f}} M \to A_{F_n}^\chi \to 0.$$

Since $\mathrm{Fitt}_{0,\Lambda_\chi}(X_{F_\infty}^\chi)$ is generated by $\det A$ and is equal to the characteristic ideal $\mathrm{char}_{\Lambda_\chi}(X_{F_\infty}^\chi)$, by the usual main conjecture we have $(\det A) = (\theta_{F_\infty}^\chi)$ as ideals of Λ_χ. By changing the basis, we may assume that $\det A = \theta_{F_\infty}^\chi$.

Put $\mathscr{K} = \{x \in (F_n^\times \otimes \mathbb{Z}_p)^\chi \mid \mathrm{div}(x) \in M\}$. Then, we have a homomorphism $\varepsilon : \mathscr{K} \to M'$ such that $\mathrm{div} : \mathscr{K} \to M$ satisfies $\mathrm{div} = \bar{f} \circ \varepsilon$. We denote an element of M and M' by a column vector of the form ${}^t(a_1, \dots, a_m)$. By the argument of Euler system of Gauss sums (cf. Rubin [32], Theorems 2.4 and 3.1), for any i and j such that $1 \leqq i, j \leqq m$, we can take a cyclic extension $L \in \mathscr{L}$, and can construct an element $g_i \in \mathscr{K}$ such that

(1) $\mathrm{div}(g_i) = {}^t(0, \dots, 0, \theta_{F_n}^\chi, 0, \dots, 0)$ ($\theta_{F_n}^\chi$ is in the i-th coordinate),

(2) when we write $\varepsilon(g_i) = {}^t(a_1, \dots, a_m)$, we have $a_j \equiv u\delta_1(\theta_{L_n}^\chi) \pmod{p^N, \theta_{F_n}^\chi}$ for some unit $u \in \Lambda_n^\times$.

Put $\tilde{a}_{i,j} = (-1)^{i+j} \det A_{i,j}$ where $A_{i,j}$ is the matrix obtained by crossing out the i-th row and the j-th column of A. The above properties of g_i imply that $\bar{A}\,{}^t(a_1, \dots, a_m) = {}^t(0, \dots, 0, \theta_{F_n}^\chi, 0, \dots, 0)$ (where $\bar{A}$ corresponds to $\bar{f}$), hence

$$c_{F_\infty/F_n}(\tilde{a}_{i,j})\theta_{F_n}^\chi = a_j \theta_{F_n}^\chi.$$

Since $\chi(p) \neq 1$, $\theta_{F_n}^\chi$ is a nonzero divisor. Hence, $c_{F_\infty/F_n}(\tilde{a}_{i,j}) = a_j$. From the property (2), we know that $c_{F_\infty/F_n}(\tilde{a}_{i,j}) \bmod p^N$ belongs to the ideal generated by $\theta_{F_n}^\chi$ and $\delta_1(\theta_{L_n}^\chi)$. Hence, $\tilde{a}_{i,j} \bmod p^N$ is in $\theta_{F_\infty}^\chi \Lambda_\chi/p^N + \delta_1(\theta_{L_\infty}^\chi)\Lambda_\chi/p^N$. This implies $\mathrm{Fitt}_{1,\Lambda_\chi/p^N}(X_{F_\infty}^\chi/p^N) \subset \mathscr{F}$, and we have completed the proof of Theorem 8.4.

9. Example—the case $\lambda = 2$

In this section, we assume that F is an imaginary abelian field, and χ is an odd character of $\mathrm{Gal}(F/\mathbb{Q})$ such that $\chi \neq \omega$, and that the conductor of χ is equal to the conductor of F. We study the case that $X_{F_\infty}^{\chi}$ is a free $\mathbb{Z}_p[\chi]$-module of rank 2.

We begin with a preparation of linear algebra. Let R be a complete discrete valuation ring of mixed characteristics $(0, p)$ $(p \neq 2)$ with maximal ideal m_R. Let π be a prime element of R (namely $m_R = (\pi)$), and v_R is an additive valuation such that $v_R(\pi) = 1$. Let $\Lambda = R[[T]]$ be the formal power series ring over R. We consider a finitely generated Λ-module M which is not cyclic (not generated by one element as a Λ-module). We further assume that as an R-module, M is free of rank 2, namely $M \simeq R \oplus R$. Then, the characteristic ideal of M is generated by the distinguished polynomial $F_M(T)$ of degree 2.

Lemma 9.1. *We write*

$$F_M(T) = (T - \alpha)(T - \beta).$$

(1) *Suppose α and β belong to R. Then, we have an exact sequence of Λ-modules*

$$0 \to \Lambda^2 \xrightarrow{f} \Lambda^2 \to M \to 0$$

such that the matrix $A_f \in M_2(\Lambda)$ which corresponds to the Λ-homomorphism f is of the form

$$A_f = \begin{pmatrix} T - \alpha & \pi^i \\ 0 & T - \beta \end{pmatrix}$$

for some i such that $0 < i \leqq v_R(\alpha - \beta)$. Here, if $\alpha = \beta$, $i = \infty$ is allowed (in this case $\pi^\infty = 0$). Further, the isomorphism class of M is determined by the value i.

(2) *Suppose $F_M(T)$ does not have a root in R. We define*

$$a = \frac{\alpha + \beta}{2}.$$

Then, we have an exact sequence of Λ-modules

$$0 \to \Lambda^2 \xrightarrow{f} \Lambda^2 \to M \to 0$$

such that the matrix $A_f \in M_2(\Lambda)$ which corresponds to the Λ-homomorphism f is of the form

$$A_f = \begin{pmatrix} T - a & \pi^i \\ c & T - a \end{pmatrix}$$

for some i such that $0 < i \leqq v_R(\alpha - \beta)$, and some $c \in R$ with $v_R(c) \geqq i$. Further, the isomorphism class of M is determined by the value i.

Proof. Since M is a free R-module of rank 2, we have an exact sequence $0 \to \Lambda^2 \xrightarrow{f} \Lambda^2 \to M \to 0$ such that $\det(f) = F_M(T)$ (Proposition 2 in the appendix of

[26]). By elementary operations of the matrices, one can transform the matrix of f into the above form. For example, we consider the case (1). By the usual theory of elementary divisors, one can take $A_f = \begin{pmatrix} a(T) & b(T) \\ c(T) & d(T) \end{pmatrix}$ such that $a(\alpha) = b(\alpha) = c(\alpha) = 0$. Since $F_M(T)$ is of degree 2, either at least $a'(0)$ or $c'(0)$ is a unit. We may assume that $a'(0)$ is a unit by adding the second row to the first row if it is needed. So we may assume $a(T)$ is a polynomial of degree 1, and $a(T) = T - \alpha$. Since $T - \alpha \mid c(T)$, we can take $c(T) = 0$. Then, $d(T) = T - \beta$, and we can take $b(T)$ to be a constant, and $b(T) = \pi^i$ with $0 < i \leqq v_R(\alpha - \beta)$. (If $i \geqq v_R(\alpha - \beta)$, one can take $b(T) = 0$.) One can show (2) by the same method.

The isomorphism class of M is determined by i because it determines the 1-st Fitting ideal $\mathrm{Fitt}_{1,\Lambda}(M)$.

Remark 9.2. (1) Lemma 9.1 says that the Fitting ideals $\mathrm{Fitt}_{i,\Lambda}(M)$ for $i \geqq 0$ determine the isomorphism class of M in this case. But in general (in the case $\mathrm{rank}_R(M) \geqq 3$), it is not true.

(2) H. Sumida [44] and M. Koike [20] classified the isomorphism classes of these Λ-modules by different methods. They computed X_{F_∞} for many examples.

Let F be as above. By Lemma 9.1, we get

Corollary 9.3. *Suppose that $X_{F_\infty}^\chi$ is a free $\mathbb{Z}_p[\chi]$-module of rank 2. Then, the isomorphism class of $X_{F_\infty}^\chi$ is determined by* $\mathrm{Fitt}_{i,\Lambda_\chi}(X_{F_\infty}^\chi)$ *for $i = 0, 1$.*

By this corollary together with Theorem 8.4, we know that the isomorphism class of $X_{F_\infty}^\chi$ is determined by the Stickelberger elements at least in the case $\chi(p) \neq 1$ and $p \nmid [F : \mathbb{Q}]$. We will explain more explicitly.

Let $N > 0$ be a positive integer, and ℓ be a prime number such that $\ell \equiv 1 \pmod{p^N}$, and ℓ is unramified in $F/\mathbb{Q}$. Let L be the subfield of $F(\mu_\ell)$ such that $[L : F] = p^N$. We identify $\Lambda_\chi = \mathbb{Z}_p[\chi][[\mathrm{Gal}(F_\infty/F)]]$ with $\mathbb{Z}_p[\chi][[T]]$ by identifying a generator γ of $\mathrm{Gal}(F_\infty/F)$ with $1 + T$. Similarly, identifying a generator of $\mathrm{Gal}(L/F)$ with $1 + S$, we identify

$$\mathbb{Z}_p[\chi][[\mathrm{Gal}(L_\infty/F)]] = \Lambda_\chi[\mathrm{Gal}(L/F)] \simeq \Lambda_\chi[S]/\big((1+S)^{p^N} - 1\big).$$

We write $\theta_{L_\infty}^\chi \in \Lambda_\chi[\mathrm{Gal}(L/F)]$ as

$$\theta_{L_\infty}^\chi = \delta_0^\ell(T) + \delta_1^\ell(T)S + \delta_2^\ell(T)S^2 + \cdots.$$

(So $\delta_i^\ell(T) = \delta_i(\theta_{L_\infty}^\chi)$ in the notation of §8.) Note that $\delta_1^\ell(T)$ is well defined in Λ_χ/p^N. By Theorem 8.1, $\delta_1^\ell(T)$ is in $\mathrm{Fitt}_{1,\Lambda}(X_{F_\infty}^\chi) \bmod p^N$. Theorem 8.4 says that $\mathrm{Fitt}_{1,\Lambda}(X_{F_\infty}^\chi)$ is generated by $\theta_{F_\infty}^\chi$ and these $\delta_1^\ell(T)$'s (ℓ ranges over all prime numbers satisfying the conditions). Namely, we can determine the isomorphism class of $X_{F_\infty}^\chi$ in principle by this method.

Example 9.4. We take $F = \mathbb{Q}(\sqrt{-6910})$, $p = 3$, and $\chi =$ the nontrivial character of $\mathrm{Gal}(F/\mathbb{Q})$. So $\Lambda_\chi = \Lambda_{F_\infty} \simeq \mathbb{Z}_3[[T]]$. In this case, $X_{F_\infty} = \mathbb{Z}_3 \oplus \mathbb{Z}_3$, and it is not generated by one element as a Λ_{F_∞}-module. We compute $\theta^{\chi}_{F_\infty} \in \mathbb{Z}_3[[T]]$ and know that $\theta^{\chi}_{F_\infty}$ does not have a root in $\mathbb{Z}_3$. Hence, we are in the case (2) of Lemma 9.1. We calculate $\delta_1^{\ell}(T)$.

ℓ	$\delta_1^{\ell}(T) \bmod (1+T)^3-1$
109	T^2+5T+3
163	$5T^2+2T+6$

(This is an example of the calculation done by Y. Yamazaki [49].) These polynomials are well defined modulo $\big(9, (1+T)^3-1\big)$. So for any $a \in 3\mathbb{Z}_3$, $f_1^{\ell}(a) \bmod 9$ is well defined. We have $f_1^{109}(a) \equiv 0 \pmod 9 \Leftrightarrow a \equiv 3 \pmod 9$ and $f_1^{163}(a) \equiv 0 \pmod 9 \Leftrightarrow a \equiv 6 \pmod 9$. This shows that the ideal $\big(T-a, f_1^{109}(T), f_1^{163}(T)\big)$ of $\Lambda/\big(9, (1+T)^3-1\big)$ must contain 3 for any $a \in 3\mathbb{Z}_3$. Hence, $\mathrm{Fitt}_{1,\Lambda_{F_\infty}}(X_{F_\infty})$ contains 3. So X_{F_∞} corresponds to the matrix $\begin{pmatrix} T-a & 3 \\ c & T-a \end{pmatrix}$ (cf. also Koike [20], p. 392, Table 2).

10. Elliptic curve with ordinary reduction at p

In this section, we study the Selmer group of a modular elliptic curve with good ordinary reduction at p by the above method.

Let E be an elliptic curve defined over $\mathbb{Q}$ (so a modular elliptic curve) such that E has good ordinary reduction at p. We assume that $p \geqq 5$.

For $\mathbb{Q}(\mu_m)^+$, we denote by $\theta^E_{\mathbb{Q}(\mu_m)^+}$ the modular element defined by Mazur and Tate [25], so $\theta^E_{\mathbb{Q}(\mu_m)^+} = \frac{1}{2}\sum [a/m]^+_E \sigma_a \in \mathbb{Q}\big[\mathrm{Gal}\big(\mathbb{Q}(\mu_m)^+/\mathbb{Q}\big)\big]$. (Here, $[a/b]^+_E$ is defined in the following way. Let $f(z) = \sum a_n \exp(2\pi i n z)$ be the modular form corresponding to E. We define $[a/b]^+_E$ by $2\pi \int_0^\infty f\left(\frac{a}{b} + iy\right) dy = [a/b]^+_E \Omega^+_E + [a/b]^-_E \Omega^-_E$ where $\Omega^{\pm}_E$ are the Néron periods. cf. [25], p. 716.) For a real abelian field F with conductor m, we define θ^E_F to be the image of $\theta^E_{\mathbb{Q}(\mu_m)^+}$ by the natural map $\mathbb{Q}\big[\mathrm{Gal}\big(\mathbb{Q}(\mu_m)^+/\mathbb{Q}\big)\big] \to \mathbb{Q}[\mathrm{Gal}(F/\mathbb{Q})]$.

As before, F_∞/F denotes the cyclotomic $\mathbb{Z}_p$-extension, and F_n the n-th layer. Let α be the unique solution of $T^2 - a_p T + p = 0$ such that $\mathrm{ord}_p(\alpha) = 0$ where $a_p = p + 1 - \#E(\mathbf{F}_p)$. For $n \geqq 1$, we define $\vartheta_{F_n} = \alpha^{-n}\big(\alpha\theta^E_{F_n} - \nu_{F_n/F_{n-1}}(\theta^E_{F_{n-1}})\big)$. Then, for $n \gg 0$ ϑ_{F_n}'s become a projective system with respect to the natural maps.

In the following, we assume that p is tamely ramified in $F/\mathbb{Q}$, $E(F)$ does not contain a point of order p, and p does not divide the Manin constant of E. Then, by Stevens [43], Theorem 4.6, ϑ_{F_n} is in $\mathbb{Z}_p[\mathrm{Gal}(F_n/\mathbb{Q})]$ and (ϑ_{F_n}) defines an element $\vartheta_{F_\infty} \in \mathbb{Z}_p[[\mathrm{Gal}(F_\infty/\mathbb{Q})]]$.

We first assume that the extension $F/\mathbb{Q}$ satisfies the condition (A_p) in §3. For a prime v of F, $e_{v,F/\mathbb{Q}}$ denotes the ramification index of v in $F/\mathbb{Q}$, and $\kappa(v)$ denotes the residue field of v. We assume that $\#E\big(\kappa(v)\big)[p] \neq p^2$ for any good reduction prime v with $p | e_{v,F/\mathbb{Q}}$. Using the notation in §2 and §3, we define $\Theta_{F_\infty,E}$ to be the ideal of $\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/\mathbb{Q})]]$ generated by $\nu_{F_\infty/M_\infty}(\vartheta_{M_\infty})$ for all $M \in (\mathscr{M}_{F/\mathbb{Q}})^{(p)}$.

Next, we consider a real abelian field F such that p is tamely ramified, and $E(F)[p] = 0$. Using (a variant of) Lemma 2.3, we can take a real abelian field $F' \supset F$ such that F'/F is an unramified p-extension and F' satisfies the condition (A_p). Note that p is tamely ramified in F' and $E(F')[p] = 0$. We again assume that $\# E(\kappa(v))[p] \neq p^2$ for any good reduction prime v of F' with $p | e_{v,F'/\mathbb{Q}}$. For such F, we define $\Theta_{F_\infty,E}$ by $\Theta_{F_\infty,E} = c_{F'_\infty/F_\infty}(\Theta_{F'_\infty,E})$.

For any algebraic extension $\mathscr{F}/\mathbb{Q}$, we denote by $\mathrm{Sel}(E/\mathscr{F})$ the Selmer group of E over $\mathscr{F}$ with respect to $E[p^\infty]$, namely

$$\mathrm{Sel}(E/\mathscr{F}) = \mathrm{Ker}\big(H^1(\mathscr{F}, E[p^\infty]) \to \prod_v H^1(\mathscr{F}_v, E[p^\infty])/\big(E(\mathscr{F}_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p\big)\big)$$

where v ranges over all primes of $\mathscr{F}$. For an abelian field F as above, we consider the Pontrjagin dual $\mathrm{Sel}(E/F_\infty)^\vee$ of the Selmer group, which is a finitely generated torsion $\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/\mathbb{Q})]]$-module by Kato's theorem [19].

Conjecture 10.1.

$$\mathrm{Fitt}_{0,\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/\mathbb{Q})]]}\big(\mathrm{Sel}(E/F_\infty)^\vee\big) = \Theta_{F_\infty,E}.$$

Theorem 10.2. *Assume that F satisfies the above conditions, and the* (*algebraic*) *μ-invariant of F_∞ for E vanishes, namely* $\mathrm{Sel}(E/F_\infty)^\vee$ *is a finitely generated $\mathbb{Z}_p$-module. Then, we have*

$$\mathrm{Fitt}_{0,\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/\mathbb{Q})]]}\big(\mathrm{Sel}(E/F_\infty)^\vee\big) \supset \Theta_{F_\infty,E}.$$

We will prove this theorem in the next section.

Corollary 10.3. *Suppose that p^2 does not divide m. We assume that $F = \mathbb{Q}(\mu_m)^+$ satisfies the conditions in Theorem* 10.2. *We further assume that $a_p \not\equiv 1 \pmod{p}$* (*not anomalous*). *Then, we have*

$$\theta^E_{\mathbb{Q}(\mu_m)^+} \in \mathrm{Fitt}_{0,\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\mu_m)^+/\mathbb{Q})]}\big(\mathrm{Sel}\big(E/\mathbb{Q}(\mu_m)^+\big)^\vee\big).$$

Mazur and Tate conjectured $\theta^E_{\mathbb{Q}(\mu_m)^+} \in \mathrm{Fitt}_{0,\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\mu_m)^+/\mathbb{Q})]}\big(\mathrm{Sel}\big(E/\mathbb{Q}(\mu_m)^+\big)^\vee\big)$ in general (Conjecture 3 in [25]).

Theorem 10.2 immediately implies Corollary 10.3. We will give here the proof. We first assume $(m,p) = 1$. By the property (1) in [25], 1.3, we have

$$c_{F_\infty/F}(\vartheta_{F_\infty}) = \big(\alpha^2 - \alpha(\varphi_p + \varphi_p^{-1}) + 1\big)\theta^E_F$$

where φ_p is the Frobenius of p in $\mathrm{Gal}(F/\mathbb{Q})$. By our assumption $a_p \not\equiv 1 \pmod{p}$, $\alpha \not\equiv 1 \pmod{p}$. Since $\alpha^2 - \alpha(\varphi_p + \varphi_p^{-1}) + 1 = (\alpha - 1)^2 + \alpha(\varphi_p - 1)(\varphi_p^{-1} - 1)$, it is a unit. Hence, the surjectivity of $\mathrm{Sel}(E/F_\infty)^\vee \to \mathrm{Sel}(E/F)^\vee$ with

$$\vartheta_{F_\infty} \in \mathrm{Fitt}_{0,\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/\mathbb{Q})]]}\big(\mathrm{Sel}(E/F_\infty)^\vee\big)$$

implies $\theta^E_F \in \mathrm{Fitt}_{0,\mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})]}\big(\mathrm{Sel}(E/F)^\vee\big)$.

Next, suppose $m = pm'$ and $(m', p) = 1$. Put $K = \mathbb{Q}(\mu_{m'})^+$. As above, the property (4) in [25], 1.3, and $\vartheta_{F_\infty} \in \mathrm{Fitt}_{0, \mathbb{Z}_p[[\mathrm{Gal}(F_\infty/\mathbb{Q})]]}(\mathrm{Sel}(E/F_\infty)^\vee)$ imply

$$\alpha\theta_F^E - \nu_{F/K}(\theta_K^E) \in \mathrm{Fitt}_{0, \mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})]}(\mathrm{Sel}(E/F)^\vee).$$

Since $[F : K]$ is prime to p, $\theta_K^E \in \mathrm{Fitt}_{0, \mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})]}(\mathrm{Sel}(E/K)^\vee)$ implies

$$\nu_{F/K}(\theta_K^E) \in \mathrm{Fitt}_{0, \mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})]}(\mathrm{Sel}(E/F)^\vee).$$

Thus, we get $\theta_F^E \in \mathrm{Fitt}_{0, \mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})]}(\mathrm{Sel}(E/F)^\vee)$.

Theorem 10.2 (and Corollary 10.3) implies a similar statement as Theorem 8.1 on the higher Fitting ideal.

We use the same notation as §8. Let $\ell_1, \dots, \ell_r$ be prime numbers such that $\ell_i \equiv 1 \pmod{p^N}$ and ℓ_i's are unramified in $F/\mathbb{Q}$. We take L to be the maximal p-extension of F in $F(\mu_{\ell_1 \dots \ell_r})$. We put $\Lambda_{F_\infty} = \mathbb{Z}_p[[\mathrm{Gal}(F_\infty/\mathbb{Q})]]$ and $\Lambda_{L_\infty} = \mathbb{Z}_p[[\mathrm{Gal}(L_\infty/\mathbb{Q})]]$, and take $n_1, \dots, n_r$, s as in §8. We can define $\delta_{i_1, \dots, i_r}(x) \in \Lambda_{F_\infty}/p^{N-s}$ for $x \in \Theta_{L_\infty, E}$. We assume L satisfies the assumptions of Theorem 10.2.

From Theorem 10.2, as in §8, we obtain

Corollary 10.4. *$\delta_{i_1, \dots, i_r}(x) \bmod p^{N-s}$ is in $\mathrm{Fitt}_{i, \Lambda_F/p^{N-s}}(\mathrm{Sel}(E/F_\infty)^\vee/p^{N-s})$ for $x \in \Theta_{L_\infty, E}$ where $i = i_1 + \cdots + i_r$.*

Remark 10.5. We get a similar statement for $\delta_{i_1, \dots, i_r}(\theta_{\mathbb{Q}(\mu_m)^+}^E)$ by using Corollary 10.3. Corollary 10.4 (and also the statement for $\theta_{\mathbb{Q}(\mu_m)^+}^E$) gives information on the upper bound of the Mordell-Weil rank of E over F. (Concerning the Mordell-Weil rank, see also Proposition 3 in Chap. 1 of Mazur and Tate [25].)

11. Proof of Theorem 10.2

Theorem 10.2 can be proved by the same method as Theorem 0.9. Instead of Corollary 5.3, we have

Proposition 11.1. *Suppose that L is a real abelian field of finite degree, and K is a subfield of L such that L/K is a p-extension. We assume that $E(L)[p] = 0$. We denote by P'_{K_∞} the set of all finite primes of K_∞ which are prime to p. Then, we have an exact sequence of $\mathbb{Z}_p[[\mathrm{Gal}(K_\infty/\mathbb{Q})]]$-modules*

$$0 \to \bigoplus_{v \in T_1} T_p(E) \otimes \mathbb{Z}_p/e_v\mathbb{Z}_p \oplus \bigoplus_{v \in T_2} \mathbb{Z}/e_v\mathbb{Z}(1) \to (\mathrm{Sel}(E/L_\infty)^\vee)_{\mathrm{Gal}(L_\infty/K_\infty)}$$
$$\to \mathrm{Sel}(E/K_\infty)^\vee \to 0$$

where

$$T_1 = \{v \in P'_{K_\infty} \mid E \text{ has good reduction at } v, v \text{ is ramified in } L_\infty/K_\infty,$$
$$\text{and } E(K_{\infty,v}) \text{ has a point of order } p\},$$

$$T_2 = \{v \in P'_{K_\infty} \mid E \text{ has split multiplicative reduction at } v \text{ and } v \text{ is ramified in } L_\infty/K_\infty\},$$

e_v is the ramification index of v in L_∞/K_∞, and $T_p(E)$ is the Tate module of E.

Instead of Lemmas 5.4 and 5.5, we have

Lemma 11.2. *In the situation of Proposition* 11.1, *we further assume that the* (*algebraic*) *μ-invariant of K_∞ for E is zero. Then, the natural map*

$$\mathrm{Sel}(E/K_\infty)^\vee \xrightarrow{\simeq} \big(\mathrm{Sel}(E/L_\infty)^\vee\big)^{\mathrm{Gal}(L_\infty/K_\infty)}$$

is an isomorphism.

Lemma 11.3. *In the situation of Lemma* 11.2, *suppose that $G = \mathrm{Gal}(L_\infty/K_\infty)$ is cyclic, and ψ is a faithful character of G. Then, $\big(\mathrm{Sel}(E/L_\infty)^\vee\big)^\psi = \mathrm{Sel}(E/L_\infty)^\vee \otimes_{\mathbb{Z}_p[G]} \mathbb{Z}_p[\psi]$ does not have a non-trivial finite $\mathbb{Z}_p[\psi][[\mathrm{Gal}(L_\infty/L)]]$-submodule.*

Proof of Theorem 10.2. Let χ be a character of $\mathrm{Gal}(F/\mathbb{Q})$ (whose order is not necessarily prime to p), and F_χ be the subfield of F which is fixed by the kernel of χ. Then, by Kato's theorem [19], the characteristic power series of $\big(\mathrm{Sel}(E/F_{\chi,\infty})^\vee\big)^\chi$ divides $\vartheta^\chi_{F_{\chi,\infty}}$. (Note that we assumed the algebraic μ-invariant vanishes, so the ambiguity of the μ-invariant in Kato's theorem disappears.) Hence, applying Lemma 4.1 we obtain Theorem 10.2 by the same method as the proof of Theorem 0.9, by using Proposition 11.1 and Lemmas 11.2 and 11.3 instead of Corollary 5.3, and Lemmas 5.4 and 5.5, respectively. Suppose that v is a good reduction prime of F with $p|e_{v,F/\mathbb{Q}}$ and ℓ is a prime of $\mathbb{Q}$ below v. Then, by our assumption, $\bigoplus_{w|\ell} T_p(E)$ is cyclic as a $\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/\mathbb{Q})]]$-module where w ranges over all primes of F_∞ above ℓ. This property is needed to check the property (v) of Lemma 4.1.

Proof of Proposition 11.1. Let S be the set of the primes of K_∞ which lie above p, or ramified in L_∞/K_∞, or bad reduction primes. We denote by $O_{K_\infty}[1/S]$ the ring of S-integers (the set of elements whose valuations at primes outside S are non-negative). By the definition of the Selmer group, we have an exact sequence

$$0 \to \mathrm{Sel}(E/K_\infty) \to H^1_{\mathrm{et}}(O_{K_\infty}[1/S], E[p^\infty]) \to \bigoplus_{v\in S} H^1(K_{\infty,v}, E)[p^\infty].$$

(For an abelian group A, $A[p^\infty]$ denotes the subgroup of elements whose orders are powers of p.) Since $\mathrm{Sel}(E/K_\infty)^\vee$ is a torsion $\mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]]$-module by Kato's theorem [19], the last map in the above exact sequence is surjective (cf. Greenberg [12], Lemma 4.6 or [11], Consequence 2).

Let $O_{L_\infty}[1/S]$ be the integral closure of $O_{K_\infty}[1/S]$ in L_∞. By our assumption $E(L)[p] = 0$, we have $E(L_\infty)[p] = 0$, hence

$$H^1_{\mathrm{et}}(O_{K_\infty}[1/S], E[p^\infty]) \to H^1_{\mathrm{et}}(O_{L_\infty}[1/S], E[p^\infty])^{\mathrm{Gal}(L_\infty/K_\infty)}$$

is bijective. We consider the same exact sequence as above for L_∞, and apply the snake lemma. Then, by the above consideration, what we have to show is the Pontrjagin dual of the kernel of

$$\bigoplus_{v\in S} H^1(K_{\infty,v}, E)[p^\infty] \to \bigoplus_{w\in\tilde{S}} H^1(L_{\infty,w}, E)[p^\infty]$$

is isomorphic to $\bigoplus_{v\in T_1} T_p(E) \otimes \mathbb{Z}_p/e_v\mathbb{Z}_p \oplus \bigoplus_{v\in T_2} \mathbb{Z}/e_v(1)$ (where $\tilde{S}$ is the set of primes of L_∞ lying over S).

If v divides p, by Coates and Greenberg [4], Theorem 3.1 and Lang's theorem, $H^1(L_{\infty,w}/K_{\infty,v}, E(L_{\infty,w})) = 0$, hence $H^1(K_{\infty,v}, E)[p^\infty] \to H^1(L_{\infty,w}, E)[p^\infty]$ is injective. If E has non-split multiplicative reduction or additive reduction at v, we also have $H^1(L_{\infty,w}/K_{\infty,v}, E(L_{\infty,w}))[p^\infty] = H^1(L_{\infty,w}/K_{\infty,v}, E(L_{\infty,w})[p^\infty]) = 0$ by [16], Proposition 5.1. So we get the same conclusion. In the case $E(K_{\infty,v})[p] = 0$, we have $E(L_{\infty,w})[p^\infty] = 0$, and also get the same conclusion. Hence, it is enough to show the next lemma.

Lemma 11.4. *Suppose that $\ell \neq p$, $\mathfrak{K}$ is a finite extension of $\mathbb{Q}_\ell$, $\mathfrak{K}_\infty$ is the cyclotomic $\mathbb{Z}_p$-extension of $\mathfrak{K}$, and $\mathfrak{K}'_\infty/\mathfrak{K}_\infty$ is an abelian extension of degree p^n (so totally ramified). Let E be an elliptic curve over $\mathfrak{K}$.*

(i) *If E has good reduction over $\mathfrak{K}_\infty$ and $E(\mathfrak{K}_\infty)[p] \neq 0$, the Pontrjagin dual of $H^1(\mathfrak{K}'_\infty/\mathfrak{K}_\infty, E(\mathfrak{K}'_\infty))$ is isomorphic to $E[p^n]$.*

(ii) *If E has split multiplicative reduction over $\mathfrak{K}_\infty$, the Pontrjagin dual of $H^1(\mathfrak{K}'_\infty/\mathfrak{K}_\infty, E(\mathfrak{K}'_\infty))$ is isomorphic to $\mathbb{Z}/p^n\mathbb{Z}(1)$.*

Proof of Lemma 11.4. By Tate's local duality, the Pontrjagin dual of $H^1(\mathfrak{K}'_\infty/\mathfrak{K}_\infty, E(\mathfrak{K}'_\infty))$ is isomorphic to $\varprojlim E(\mathfrak{K}_m)/NE(\mathfrak{K}'_m)$ where $N : E(\mathfrak{K}'_m) \to E(\mathfrak{K}_m)$ is the norm map. Since $\mathfrak{K}'_\infty/\mathfrak{K}_\infty$ is totally ramified, we may assume that $\mathfrak{K}'_m/\mathfrak{K}_m$ is totally ramified of degree p^n. We may assume $n > 0$.

(i) Let κ_m be the residue field of $\mathfrak{K}_m$. Since $E(\mathfrak{K}_\infty)[p] \neq 0$ implies $E(\mathfrak{K}_\infty)[p^\infty] = E[p^\infty]$ ([16], Proposition 5.1), considering the usual filtration on $E(\mathfrak{K}_n)$, we have $E(\mathfrak{K}_m)/NE(\mathfrak{K}'_m) \simeq E(\kappa_m) \otimes \mathbb{Z}/p^n \simeq E(\kappa_m)[p^n] \simeq E[p^n]$ for sufficiently large m. Hence, we get the conclusion.

This can be also checked in the following way. As in the proof of Hachimori and Matsuno [16], Corollary 5.2, we have

$$H^1(\mathfrak{K}'_\infty/\mathfrak{K}_\infty, E(\mathfrak{K}'_{\infty,})) = \mathrm{Hom}(\mathrm{Gal}(\mathfrak{K}'_\infty/\mathfrak{K}_\infty), E[p^\infty]) = \mathrm{Hom}(\mathbb{Z}/p^n(1), E[p^\infty]).$$

Since the Weil pairing induces $E[p^n]^\vee \simeq E[p^n](-1)$, the above implies the conclusion.

(ii) Since E is a Tate curve, we can write $E(\mathfrak{K}_m) = \mathfrak{K}_m^\times/q^\mathbb{Z}$ for some q. Hence, $E(\mathfrak{K}_m)/NE(\mathfrak{K}'_m) \simeq \mathrm{Gal}(\mathfrak{K}'_m/\mathfrak{K}_m)$ by local class field theory. Thus,

$$\varprojlim E(\mathfrak{K}_m)/NE(\mathfrak{K}'_m) \simeq \mathrm{Gal}(\mathfrak{K}'_\infty/\mathfrak{K}_\infty) \simeq \mathbb{Z}/p^n\mathbb{Z}(1).$$

Proof of Lemma 11.2. By Kato's theorem ([19]), $\mathrm{Sel}(E/K_\infty)^\vee$ is a finitely generated torsion $\mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]]$-module, and by Greenberg's theorem (Greenberg [12], Proposition 4.14), it does not have a non-trivial finite $\mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]]$-submodule. Hence, it is a free $\mathbb{Z}_p$-module. So the injectivity follows. The surjectivity follows from Hachimori and Matsuno [16], Theorem 6.3.

Proof of Lemma 11.3. By using Lemma 11.2, this can be proved by the same method as Lemma 5.5.

12. Cohomology of $\mathbb{Z}_p(r)$

In this section, we study the etale cohomology group

$$H^2(O_F[1/p], \mathbb{Z}_p(r)) = H^2_{\mathrm{et}}(O_F[1/p], \mathbb{Z}_p(r))$$

for a totally real number field F and a positive even integer r. It is isomorphic to $H^2(G_{F,p}, \mathbb{Z}_p(r))$ where $G_{F,p} = \mathrm{Gal}(F^{\max,p}/F)$ is the Galois group of the maximal extension of F unramified outside p over F.

Let k be a totally real number field and F/k a finite abelian extension. For a positive even integer r, we consider $\theta_{F/k}(1-r) \in \mathbb{Q}[\mathrm{Gal}(F/k)]$ where $\theta_{F/k}(s)$ is as in §2. We use the notation in §2. By the same method as Lemma 2.1, we have

Lemma 12.1. *In the situation of Lemma* 2.1, *we have*

$$c_{F/M}(\theta_F(1-r)) = \Big(\prod_{v \in S_F \setminus S_M} (1 - N(v)^{r-1}\varphi_v^{-1})\Big)\theta_M(1-r)$$

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

Let F_∞/F be the cyclotomic $\mathbb{Z}_p$-extension. By this lemma, we know that $(\theta_{F_n/k}(1-r))$ becomes a projective system for $n \gg 0$, and we can define $\theta_{F_\infty/k}(1-r)$. Let θ_{F_∞} be as in §3, and $\tau : Q(\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/k)]]) \to Q(\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/k)]])$ be the ring homomorphism defined by $\sigma \mapsto \kappa(\sigma)\sigma$ for $\sigma \in \mathrm{Gal}(F_\infty/k)$ ($\kappa : \mathrm{Gal}(F_\infty/k) \to \mathbb{Z}_p^\times$ is the cyclotomic character). If $\mu_p \subset F$, we have ([26], Chap. I, §5, Proposition 1)

$$\theta_{F_\infty/k}(1-r) = \tau^{1-r}\theta_{F_\infty}.$$

We assume that F satisfies the conditions in the subsection 3.1, especially the condition (A_p). As in 3.1 we define

$$(\Theta_{F_\infty/k}(1-r)')^{(p)} = \langle \{ v_{F_\infty/M_\infty}(\theta_{M_\infty/k}(1-r)) \mid M \in (\mathscr{M}_{F/k})^{(p)} \} \rangle$$

and

$$(\Theta_{F_\infty/k}(1-r))^{(p)} = (\Theta_{F_\infty/k}(1-r)')^{(p)} \cap \mathbb{Z}_p[[\mathrm{Gal}(F_\infty/k)]].$$

Next, we assume that F satisfies the conditions in the subsection 3.2. We define

$$(\Theta_{F_\infty/k}(1-r))^{(p)} = c_{F'_\infty/F_\infty}((\Theta_{F'_\infty/k}(1-r))^{(p)}).$$

We also define

$$\mathbb{H}^2(O_{F_\infty}[1/p], \mathbb{Z}_p(r)) = \varprojlim H^2(O_{F_n}[1/p], \mathbb{Z}_p(r))$$

which we regard as a $\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/k)]]$-module.

Theorem 12.2. *Suppose that F is a totally real number field, and satisfies the conditions in the subsection* 3.2. *We also assume that the Iwasawa μ-invariant of $F_\infty(\mu_p)$ is zero. Then, we have*

$$\mathrm{Fitt}_{0,\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/k)]]}(\mathbb{H}^2(O_{F_\infty}[1/p], \mathbb{Z}_p(r))) = (\Theta_{F_\infty/k}(1-r))^{(p)}.$$

In particular, $(\Theta_{F_\infty/k}(1-r))^{(p)}$ annihilates $\mathbb{H}^2(O_{F_\infty}[1/p], \mathbb{Z}_p(r))$.

We will prove this theorem later. In the same way as Corollary 0.10, we have

Corollary 12.3. *For any real abelian field F, we have*

$$\mathrm{Fitt}_{0,\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/\mathbb{Q})]]}\big(\mathbb{H}^2\big(O_{F_\infty}[1/p],\mathbb{Z}_p(r)\big)\big) = \big(\Theta_{F_\infty/\mathbb{Q}}(1-r)\big)^{(p)}.$$

Since the p-cohomological dimension of $O_F[1/p]$ is 2, for any $n>0$ and any Galois extension L/F which is unramified outside p, by [37], Chap. I, Prop. 17, $H^2\big(O_L[1/p],\mathbb{Z}/p^n(r)\big)_{\mathrm{Gal}(L/F)} \xrightarrow{\simeq} H^2\big(O_F[1/p],\mathbb{Z}/p^n(r)\big)$ is bijective. Hence,

$$\mathbb{H}^2\big(O_{F_\infty}[1/p],\mathbb{Z}_p(r)\big)_{\mathrm{Gal}(F_\infty/F)} \simeq H^2\big(O_F[1/p],\mathbb{Z}_p(r)\big)$$

is an isomorphism. Therefore, by Corollary 12.3 we have

Corollary 12.4. *For any real abelian field F, we have*

$$\mathrm{Fitt}_{0,\mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})]}\big(H^2\big(O_F[1/p],\mathbb{Z}_p(r)\big)\big) = c_{F_\infty/F}\big(\big(\Theta_{F_\infty/\mathbb{Q}}(1-r)\big)^{(p)}\big).$$

Let F be a real abelian field of finite degree with conductor m. Following Coates and Sinnott [5], for a positive integer b with $(b,m)=1$, we put

$$S_r(b) = w_r(\mathbb{Q})(b^r - \varphi_b)\theta_{F/\mathbb{Q}}(1-r)$$

where $w_r(\mathbb{Q}) = \sharp H^0\big(\mathbb{Q},\mathbb{Q}/\mathbb{Z}(r)\big)$, and $\varphi_b = (b, F/\mathbb{Q})$. We have $S_r(b) \in \mathbb{Z}[\mathrm{Gal}(F/\mathbb{Q})]$ ([5], Theorem 1.2).

We define

$$H^2\big(O_F,\mathbb{Z}'(r)\big) = \prod_{p \neq 2} H^2\big(O_F[1/p],\mathbb{Z}_p(r)\big)$$

where p ranges over all odd prime numbers. A well known conjecture by Quillen-Lichtenbaum claims that $H^2\big(O_F,\mathbb{Z}'(r)\big)$ is isomorphic to the K-group $K_{2r-2}(O_F)\otimes\mathbb{Z}'$.

Corollary 12.5. *For any real abelian field F, we have*

$$S_r(b) \in \mathrm{Fitt}_{0,\mathbb{Z}'[\mathrm{Gal}(F/\mathbb{Q})]}\big(H^2\big(O_F,\mathbb{Z}'(r)\big)\big).$$

Conjecture 1 in Coates and Sinnott [5] claims that $S_r(b)K_{2r-2}(O_F)=0$, so it would imply $S_r(b)H^2\big(O_F,\mathbb{Z}'(r)\big)=0$. Hence, we can regard Corollary 12.5 as a refinement of their conjecture because Corollary 12.5 says that $S_r(b)$ is not only in the annihilator of $H^2\big(O_F,\mathbb{Z}'(r)\big)$, but also in the Fitting ideal. Cornacchia and Østvær proved in [6] this corollary for F with prime power conductor.

Proof of Corollary 12.5. By Corollary 12.4, it is enough to show $S_r(b) \in c_{F_\infty/F}\big(\Theta_{F_\infty/\mathbb{Q}}(1-r)\big)$ for each odd prime p.

First of all, note that $c_{F_\infty/F}\big(\theta_{F_\infty}(1-r)\big)/\theta_F(1-r)$ is a unit by Lemma 12.1 because $1-p^{r-1}\varphi_p^{-1}$ is a unit. Put $L=F(\mu_p)$. Since $\tau^{r-1}\big(\theta_{L_\infty/\mathbb{Q}}(1-r)\big)=\theta_{L_\infty}$, by the property (ii) in 3.1, $\big(1-\kappa(\sigma)^{-r}\sigma\big)\theta_{L_\infty/\mathbb{Q}}(1-r)$ is in $\mathbb{Z}_p[[\mathrm{Gal}(L_\infty/\mathbb{Q})]]$ for any $\sigma\in\mathrm{Gal}(L_\infty/\mathbb{Q})$. So $\big(1-\kappa(\sigma)^{-r}\sigma_{|F_\infty}\big)\theta_{F_\infty/\mathbb{Q}}(1-r) \in \big(\Theta_{F_\infty/\mathbb{Q}}(1-r)\big)^{(p)}$ for any $\sigma\in\mathrm{Gal}(L_\infty/\mathbb{Q})$.

If b is prime to p, taking $\sigma = (b, L_\infty/\mathbb{Q})$, we know

$$(b^r - \varphi_b)\theta_{F/\mathbb{Q}}(1-r) \in c_{F_\infty/F}\big(\Theta_{F_\infty/\mathbb{Q}}(1-r)\big).$$

Hence, in this case we have the conclusion of Corollary 12.5.

Next, suppose that p divides b. Then, m is prime to p. Let γ be a generator of $\mathrm{Gal}(L_\infty/L)$. Then, $c_{F_\infty/F}\big(1-\kappa(\gamma)^{-r}\gamma\big) \in \mathbb{Z}_p$ satisfies

$$\mathrm{ord}_p\big(c_{F_\infty/F}\big(1-\kappa(\gamma)^{-r}\gamma\big)\big) = \mathrm{ord}_p(r) + 1 = \mathrm{ord}_p\big(w_r(\mathbb{Q})\big).$$

Hence, we have $w_r(\mathbb{Q})\theta_{F/\mathbb{Q}}(1-r) \in c_{F_\infty/F}\big(\Theta_{F_\infty/\mathbb{Q}}(1-r)\big)$. This completes the proof of Corollary 12.5.

Remark 12.6. In the above proof of Corollary 12.5, we showed

$$\big(1-\kappa(\sigma)^{-r}\sigma_{|_F}\big)\theta_{F/\mathbb{Q}}(1-r) \in \mathrm{Fitt}_{0,\mathbb{Z}_p[\mathrm{Gal}(F/\mathbb{Q})]}\big(H^2\big(O_F[1/p], \mathbb{Z}_p(r)\big)\big)$$

for $\sigma \in \mathrm{Gal}(L_\infty/\mathbb{Q})$. This implies

$$\mathrm{Ann}_{\mathbb{Z}'[\mathrm{Gal}(F/\mathbb{Q})]}\big(H^0\big(F, \mathbb{Q}/\mathbb{Z}(r)\big) \otimes \mathbb{Z}'\big)\theta_{F/\mathbb{Q}}(1-r) \subset \mathrm{Fitt}_{0,\mathbb{Z}'[\mathrm{Gal}(F/\mathbb{Q})]}\big(H^2\big(O_F, \mathbb{Z}'(r)\big)\big).$$

Burns and Greither proved in [2] this inclusion in the case $F/\mathbb{Q}$ is cyclic by a different method. They obtained this inclusion by proving a beautiful result on the Fitting ideal of $H^2\big(O_F[1/S], \mathbb{Z}_p(r)\big)$ for a general CM field F and any $r > 0$ where S is a set of primes containing ramifying primes in F/k and primes above p. For the Fitting ideal of $H^2\big(O_F[1/S], \mathbb{Z}_p(r)\big)$, see also Snaith [41] and Nguyen Quang Do [27].

Proof of Theorem 12.2. We can prove Theorem 12.2 by the same method as the proof of Theorem 0.9. Instead of Proposition 5.2, we have

Lemma 12.7. *Suppose that L/K is a Galois extension of number fields of finite degree with Galois group G. Let S be the set of the primes of K which are above p or ramified in L/K. We denote by $\tilde{S}'$ the set of ramifying primes of L in L/K which are prime to p. We denote by $O_L[1/S]$ the ring of S-integers. Then, we have an exact sequence*

$$H_1\big(G, H^2\big(O_L[1/S], \mathbb{Z}_p(r)\big)\big) \to H_1\Big(G, \bigoplus_{w \in \tilde{S}'} H^2\big(L_w, \mathbb{Z}_p(r)\big)\Big)$$
$$\to H^2\big(O_L[1/p], \mathbb{Z}_p(r)\big)_G \to H^2\big(O_K[1/p], \mathbb{Z}_p(r)\big) \to 0.$$

Proof of Lemma 12.7. By the localizing sequence,

$$0 \to H^2\big(O_L[1/p], \mathbb{Z}_p(r)\big) \to H^2\big(O_L[1/S], \mathbb{Z}_p(r)\big) \to \bigoplus_{w \in \tilde{S}'} H^2\big(L_w, \mathbb{Z}_p(r)\big) \to 0$$

is exact. Similarly,

$$0 \to H^2\big(O_K[1/p], \mathbb{Z}_p(r)\big) \to H^2\big(O_K[1/S], \mathbb{Z}_p(r)\big) \to \bigoplus_{v \in S'} H^2\big(K_v, \mathbb{Z}_p(r)\big) \to 0$$

is exact where S' is the set of primes of K below $\tilde{S}'$. Since both

$$H^2\big(O_L[1/S], \mathbb{Z}_p(r)\big)_G \xrightarrow{\simeq} H^2\big(O_K[1/S], \mathbb{Z}_p(r)\big)$$

and

$$\Big(\bigoplus_{w \in \tilde{S}'} H^2\big(L_w, \mathbb{Z}_p(r)\big)\Big)_G \xrightarrow{\simeq} \bigoplus_{v \in S'} H^2\big(K_v, \mathbb{Z}_p(r)\big)$$

are bijective (the p-cohomological dimensions of $O_K[1/S]$ and K_v are 2), taking the homology of the first exact sequence, we obtain Lemma 12.7.

In several cases, it is not difficult to compute $H_1\Big(G, \bigoplus_{w \in \tilde{S}'} H^2\big(L_w, \mathbb{Z}_p(r)\big)\Big)$. For example, instead of Corollary 5.3 we have

Lemma 12.8. *Suppose that L/k is a finite abelian extension, and K is a subfield of L such that L/K is a p-extension. We assume that the primes above p are tamely ramified in L/k. We denote by S' the set of the primes of K_∞ ramifying in L_∞/K_∞. Then, the sequence*

$$\begin{aligned} &H_1\big(L_\infty/K_\infty, \mathbb{H}^2\big(O_{L_\infty}[1/S], \mathbb{Z}_p(r)\big)\big) \to \bigoplus_{v \in S'} \mathbb{Z}/e_v\mathbb{Z}(r) \\ &\quad \to \mathbb{H}^2\big(O_{L_\infty}[1/p], \mathbb{Z}_p(r)\big)_{\mathrm{Gal}(L_\infty/K_\infty)} \to \mathbb{H}^2\big(O_{K_\infty}[1/p], \mathbb{Z}_p(r)\big) \to 0 \end{aligned}$$

is exact where e_v is the ramification index of v in L_∞/K_∞.

Proof of Lemma 12.8. It is enough to compute

$$H_1\Big(L_\infty/K_\infty, \bigoplus_{w \in \tilde{S}'} \mathbb{H}^2\big(L_{\infty,w}, \mathbb{Z}_p(r)\big)\Big) = \bigoplus_{v \in S'} H_1\big(L_{\infty,w}/K_{\infty,v}, \mathbb{H}^2\big(L_{\infty,w}, \mathbb{Z}_p(r)\big)\big).$$

Let v be a prime in S', w a prime above v, and ℓ the characteristic of the residue field of v. By our assumption, we have $\ell \neq p$. Hence, $L_{\infty,w}/K_{\infty,v}$ is totally ramified and cyclic. Since $L_{\infty,w} \neq K_{\infty,v}$, by local class field theory the residue field of v contains a primitive p-th root of unity. Thus, by Tate duality

$$\mathbb{H}^2\big(L_{\infty,w}, \mathbb{Z}_p(r)\big) = H^0\big(L_{\infty,w}, \mathbb{Q}_p/\mathbb{Z}_p(1-r)\big)^\vee = \mathbb{Q}_p/\mathbb{Z}_p(1-r)^\vee = \mathbb{Z}_p(r-1).$$

Hence, we have

$$\begin{aligned} &H_1\big(L_{\infty,w}/K_{\infty,v}, \mathbb{H}^2\big(L_{\infty,w}, \mathbb{Z}_p(r)\big)\big) = \hat{H}^{-2}\big(L_{\infty,w}/K_{\infty,v}, \mathbb{Z}_p(r-1)\big) \\ &\quad = \hat{H}^0\big(L_{\infty,w}/K_{\infty,v}, \mathbb{Z}_p(r-1)\big)(1) = \mathbb{Z}/e_v\mathbb{Z}(r) \end{aligned}$$

because $L_{\infty,w}/K_{\infty,v}$ is cyclic.

Instead of Lemma 5.4, we have

Lemma 12.9. *In the situation of Lemma* 12.8, *we assume that L is totally real,* $\mathrm{Gal}(L_\infty/K_\infty)$ *is cyclic, there is a totally ramified prime in L_∞/K_∞, and the Iwasawa μ-invariant of $K(\mu_p)_\infty$ vanishes. Then, the natural map*

$$\mathbb{H}^2(O_{K_\infty}[1/p], \mathbb{Z}_p(r)) \overset{\simeq}{\to} \mathbb{H}^2(O_{L_\infty}[1/p], \mathbb{Z}_p(r))^{\mathrm{Gal}(L_\infty/K_\infty)}$$

is bijective.

We first need the following lemma.

Lemma 12.10. *For a totally real number field K, $\mathbb{H}^2(O_{K_\infty}[1/p], \mathbb{Z}_p(r))$ does not have a non-trivial finite $\mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]]$-submodule.*

Proof of Lemma 12.10. By Coates [3], Theorem 11,

$$H^2(O_{K_n}[1/p], \mathbb{Z}_p(r)) \to H^2(O_{K_{n+1}}[1/p], \mathbb{Z}_p(r))$$

is injective for all n. Since

$$\mathbb{H}^2(O_{K_\infty}[1/p], \mathbb{Z}_p(r))_{\mathrm{Gal}(K_\infty/K_n)} \overset{\simeq}{\to} H^2(O_{K_n}[1/p], \mathbb{Z}_p(r))$$

is bijective, the conclusion of Lemma 12.10 follows from the above injectivity.

Proof of Lemma 12.9. By Lemma 12.10 and our assumption $\mu = 0$, $\mathbb{H}^2(O_{K_\infty}[1/p], \mathbb{Z}_p(r))$ is a free $\mathbb{Z}_p$-module. Hence, the injectivity follows by the norm argument.

Consider an exact sequence

$$(*) \qquad 0 \to \mathbb{H}^2(O_{L_\infty}[1/p], \mathbb{Z}_p(r)) \to \mathbb{H}^2(O_{L_\infty}[1/S], \mathbb{Z}_p(r)) \to \bigoplus_{w \in \tilde{S}'} \mathbb{H}^2(L_{\infty,w}, \mathbb{Z}_p(r)) \to 0$$

which is obtained from the localizing sequence. Put $G = \mathrm{Gal}(L_\infty/K_\infty)$. Using the Serre-Hochschild spectral sequence, we have

$$\begin{aligned} H^2(G, \mathbb{H}^2(O_{L_\infty}[1/S], \mathbb{Z}_p(r))) &\simeq H^4(G, \mathbb{H}^1(O_{L_\infty}[1/S], \mathbb{Z}_p(r))) \\ &\simeq H^2(G, \mathbb{H}^0(L_\infty, \mathbb{Q}_p/\mathbb{Z}_p(r))(-1)). \end{aligned}$$

Let v_0 be a prime which is totally ramified in L_∞/K_∞, and w_0 be the prime above v_0. Similarly, we have

$$H^2(G, \mathbb{H}^2(L_{\infty,w_0}, \mathbb{Z}_p(r))) \simeq H^2(G, \mathbb{H}^0(L_{\infty,w_0}, \mathbb{Q}_p/\mathbb{Z}_p(r-1))).$$

Hence,

$$H^2(G, \mathbb{H}^2(O_{L_\infty}[1/S], \mathbb{Z}_p(r))) \to H^2\Big(G, \bigoplus_{w \in \tilde{S}'} \mathbb{H}^2(L_{\infty,w}, \mathbb{Z}_p(r))\Big)$$

is injective.

On the other hand, from the isomorphism

$$\Big(\bigoplus_{w\in\tilde{S}'}\mathbb{H}^2\big(L_{\infty,w},\mathbb{Z}_p(r)\big)\Big)_G \xrightarrow{\simeq} \bigoplus_{v\in S'}\mathbb{H}^2\big(K_{\infty,v},\mathbb{Z}_p(r)\big),$$

we have $H^1\Big(G,\bigoplus_{w\in\tilde{S}'}\mathbb{H}^2\big(L_{\infty,w},\mathbb{Z}_p(r)\big)\Big)=0$. Hence, taking the cohomology of the above exact sequence $(*)$, we get $H^2\big(G,\mathbb{H}^2\big(O_{L_\infty}[1/p],\mathbb{Z}_p(r)\big)\big)=0$. This shows the surjectivity of the map in Lemma 12.9.

Lemmas 12.9 and 12.10 imply the following lemma which corresponds to Lemma 5.5.

Lemma 12.11. *In the situation of Lemma* 12.9, *for a faithful character* ψ *of* $\mathrm{Gal}(L_\infty/K_\infty)$, $\mathbb{H}^2\big(O_{L_\infty}[1/p],\mathbb{Z}_p(r)\big)^\psi=\mathbb{H}^2\big(O_{L_\infty}[1/p],\mathbb{Z}_p(r)\big)\otimes_{\mathbb{Z}_p[G]}\mathbb{Z}_p[\psi]$ *does not have a non-trivial finite* $\mathbb{Z}_p[\psi][[\mathrm{Gal}(L_\infty/L)]]$*-submodule.*

We go back to the proof of Theorem 12.2. Let χ be a character of $\mathrm{Gal}(F/k)$ (whose order is not necessarily prime to p), and F_χ be the subfield of F which is fixed by the kernel of χ. Consider a $\mathbb{Z}_p[\chi][[\mathrm{Gal}(F_{\chi,\infty}/F_\chi)]]$-module $\mathbb{H}^2\big(O_{F_{\chi,\infty}}[1/p],\mathbb{Z}_p(r)\big)^\chi$. Suppose $\chi\neq\omega^r$. The main conjecture proved by Wiles [47] implies that the characteristic ideal of $\mathbb{H}^2\big(O_{F_{\chi,\infty}}[1/p],\mathbb{Z}_p(r)\big)^\chi$ is equal to $\big(\theta_{F_{\chi,\infty}/k}(1-r)^\chi\big)$. For $\chi=\omega^r$, the main conjecture implies that the characteristic ideal is generated by the numerator of $\theta_{F_{\chi,\infty}/k}(1-r)^\chi$. Hence, using above lemmas and Corollary 4.2, we obtain Theorem 12.2 by the same method as the proof of Theorem 0.9.

References

[1] *Burns, D.* and *Greither, C.*, On the equivariant Tamagawa number conjecture for Tate motives, Invent. math., to appear.

[2] *Burns, D.* and *Greither, C.*, Equivariant Weierstrass preparation and values of L-functions at negative integers, preprint.

[3] *Coates, J.*, On K_2 and some classical conjectures in algebraic number theory, Ann. Math. **95** (1972), 99–116.

[4] *Coates, J.* and *Greenberg, R.*, Kummer theory for abelian varieties over local fields, Invent. math. **124** (1996), 129–174.

[5] *Coates, J.* and *Sinnott, W.*, An analogue of Stickelberger's theorem for the higher K-groups, Invent. math. **24** (1974), 149–161.

[6] *Colmez, P.*, Résidu en $s=1$ des fonctions zêta p-adiques, Invent. math. **91** (1988), 371–398.

[7] *Cornacchia, P.* and *Østvær, P. A.*, On the Coates-Sinnott conjecture, K-Theory **19** (2000), 195–209.

[8] *Cornacchia, P.* and *Greither, C.*, Fitting ideals of class groups of real fields with prime power conductor, J. Number Th. **73** (1998), 459–471.

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

[10] *Ferrero, B.* and *Washington, L.*, The Iwasawa invariant μ_p vanishes for abelian number fields, Ann. Math. **109** (1979), 377–395.

[11] *Greenberg, R.*, The structure of Selmer groups, Proc. Nat. Acad. Sci. USA **94** (1997), 11125–11128.

[12] *Greenberg, R.*, Iwasawa theory for elliptic curves, in: Arithmetic theory of elliptic curves, Cetraro, Italy 1997, Springer Lect. Notes Math. **1716** (1999), 51–144.

[13] *Greither, C.*, The structure of some minus class groups, and Chinburg's third conjecture for abelian fields, Math. Z. **229** (1998), 107–136.

[14] *Greither, C.*, Some cases of Brumer's conjecture for abelian CM extensions of totally real fields, Math. Z. **233** (2000), 515–534.

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

[16] *Hachimori, Y.* and *Matsuno, K.*, An analogue of Kida's formula for the Selmer groups of elliptic curves, J. Alg. Geom. **8** (1999), 581–601.

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

[18] *Kato, K.*, Lectures on the approach to Iwasawa theory for Hasse-Weil L-functions via B_{dR}, in: Arithmetic Algebraic Geometry (Trento 1991), Springer Lect. Notes Math. **1553** (1993), 50–163.

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

[20] *Koike, M.*, On the isomorphism classes of Iwasawa modules associated to imaginary quadratic fields with $\lambda = 2$, J. Math. Sci. Univ. Tokyo **6** (1999), 371–396.

[21] *Kolyvagin, V. A.*, Euler systems, The Grothendieck Festschrift Vol. II (1990), 435–483.

[22] *Kurihara, M.*, On the ideal class groups of the maximal real subfields of number fields with all roots of unity, J. Europ. Math. Soc. **1** (1999), 35–49.

[23] *Kurihara, M.*, On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction I, Invent. math. **149** (2002), 195–224.

[24] *Kurihara, M.*, On the structure of ideal class groups of CM fields, Docum. Math., to appear.

[25] *Mazur, B.* and *Tate, J.*, Refined conjectures of the "Birch and Swinnerton-Dyer type", Duke Math. J. **54** No 2 (1987), 711–750.

[26] *Mazur, B.* and *Wiles, A.*, Class fields of abelian extensions of $\mathbb{Q}$, Invent. math. **76** (1984), 179–330.

[27] *Nguyen Quang Do, T.*, Quelques applications de la conjecture principale équivariante, preprint.

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

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

[30] *Ritter, J.* and *Weiss, A.*, The lifted root number conjecture and Iwasawa theory, Mem. Amer. Math. Soc. **157** (2002).

[31] *Ritter, J.* and *Weiss, A.*, Toward equivariant Iwasawa theory, Manuscr. Math. **109** (2002), 131–146.

[32] *Rubin, K.*, Kolyvagin's system of Gauss sums, in: Arithmetic Algebraic Geometry, G. van der Geer et al., eds., Progr. Math. **89** (1991), 309–324.

[33] *Rubin, K.*, Euler systems, Ann. Math. Stud. **147**, Princeton Univ. Press, 2000.

[34] *Schoof, R.*, The structure of the minus class groups of abelian number fields, Sém. de Théorie des Nombres Paris 1988–89, Birkhäuser, Boston (1990), 185–204.

[35] *Schoof, R.*, Minus class groups of the fields of the ℓ-th roots of unity, Math. Comput. **67** No. 223 (1998), 1225–1245.

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

[37] *Serre, J.-P.*, Cohomologie galoisienne, Lect. Notes Math. **5**, Springer-Verlag, 1973 (quatrième édition).

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

[39] *Sinnott, W.*, On the Stickelberger ideal and the circular units of a cyclotomic field, Ann. Math. **108** (1978), 107–134.

[40] *Sinnott, W.*, On the Stickelberger ideal and the circular units of an abelian field, Invent. math. **62** (1980), 181–234.

[41] *Snaith, V.*, Relative K_0, Fitting ideals and the Stickelberger phenomenon, preprint.

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

[43] *Stevens, G.*, Stickelberger elements and modular parametrizations of elliptic curves, Invent. math. **98** (1989), 75–106.

[44] *Sumida, H.*, Greenberg's conjecture and the Iwasawa polynomial, J. Math. Soc. Japan **49** (1997), 689–711.

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

[46] *Washington, L.*, Introduction to cyclotomic fields, Grad. Texts Math. **83**, Springer-Verlag, 1982.

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

[48] *Wiles, A.*, On a conjecture of Brumer, Ann. Math. **131** (1990), 555–565.

[49] *Yamazaki, Y.*, On the Stickelberger elements and ideal class groups (in Japanese), Master's thesis, Tokyo Metropolitan Univ., 1998.

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

Eingegangen 27. September 2001, in revidierter Fassung 27. August 2002