Algebra & Number Theory

Volume 17
2023
No. 11

Fitting ideals of class groups for CM abelian extensions

Mahiro Atsuta and Takenori Kataoka

msp

ALGEBRA AND NUMBER THEORY 17:11 (2023)
https://doi.org/10.2140/ant.2023.17.1901

Fitting ideals of class groups for CM abelian extensions

Mahiro Atsuta and Takenori Kataoka

Let K be a finite abelian CM-extension of a totally real field k and T a suitable finite set of finite primes of k. We determine the Fitting ideal of the minus component of the T-ray class group of K, except for the 2-component, assuming the validity of the equivariant Tamagawa number conjecture. As an application, we give a necessary and sufficient condition for the Stickelberger element to lie in that Fitting ideal.

1. Introduction

In number theory, the relationship between class groups and special values of L-functions is of great importance. We discuss such a phenomenon for a finite abelian CM-extension K/k, that is, a finite abelian extension such that k is a totally real field and K is a CM-field. We focus on the minus components of the (ray) class groups of K, except for the 2-components, and study the Fitting ideals of them.

Let Cl_K denote the ideal class group of K. For a $\mathbb{Z}[\mathrm{Gal}(K/k)]$-module M, let M^- denote the minus component after inverting the multiplication by 2. When $k = \mathbb{Q}$, Kurihara and Miura [2011] succeeded in proving a conjecture of Kurihara [2003a] on a description of the Fitting ideal of Cl_K^- using the Stickelberger elements. However, for a general totally real field k, the problem to determine the Fitting ideal of Cl_K^- is still open.

There seems to be an agreement that the *Pontryagin duals* (denoted by $(-)^\vee$) of the class groups are easier to deal with; see Greither and Kurihara [2008]. Greither [2007] determined the Fitting ideal of $\mathrm{Cl}_K^{\vee,-}$, assuming that the minus component of the equivariant Tamagawa number conjecture for $\mathbb{G}_m$ (eTNC for short) holds and that the group of roots of unity in K is cohomologically trivial. Subsequently, Kurihara [2021] generalized the results of Greither on $\mathrm{Cl}_K^{\vee,-}$ to results on $\mathrm{Cl}_K^{T,\vee,-}$, where Cl_K^T denotes the T-ray class group, for a finite set T of finite primes of k. This enables us, by taking suitably large T, to remove the assumption that the group of roots of unity is cohomologically trivial, though we still need to assume the validity of the eTNC. In recent work Dasgupta and Kakde [2023] succeeded in proving *unconditionally* the same formula as Kurihara on the Fitting ideal of $\mathrm{Cl}_K^{T,\vee,-}$ (see (1-2) below for the formula).

In this paper, for a general totally real field k, we determine the Fitting ideal of $\mathrm{Cl}_K^{T,-}$ *without the Pontryagin dual*, assuming the eTNC, except for the 2-component. This problem has been considered to be harder than that on $\mathrm{Cl}_K^{T,\vee,-}$ and actually our result is more complicated. Our main tool is the technique of shifts of Fitting ideals, which was established by Kataoka [2020].

MSC2020: 11R29.
Keywords: class groups, Fitting ideals, CM-fields, equivariant Tamagawa number conjecture.

As an application of the description, we will obtain a necessary and sufficient condition for the Stickelberger element to be in the Fitting ideal of $\mathrm{Cl}_K^{T,-}$ (still assuming the eTNC). Note that the question for the dualized version $\mathrm{Cl}_K^{T,\vee,-}$ is called the strong Brumer–Stark conjecture and is answered affirmatively by Dasgupta and Kakde [2023] unconditionally.

Though we mainly assume the validity of the eTNC in this paper, we also obtain interesting unconditional results. For instance, in Theorem 1.6 we will show that the Fitting ideal of $\mathrm{Cl}_K^{T,-}$ is always contained in that of $\mathrm{Cl}_K^{T,\vee,-}$, and that the inclusion is often proper.

In the rest of this section, we give precise statements of the main results.

1A. ***Description of the Fitting ideal.*** Let K/k be a finite abelian CM-extension and put $G = \mathrm{Gal}(K/k)$. Let $S_\infty(k)$ be the set of archimedean places of k. Let $S_{\mathrm{ram}}(K/k)$ be the set of places of k which are ramified in K/k, including $S_\infty(k)$. For each finite prime $v \in S_{\mathrm{ram}}(K/k)$, let $I_v \subset G$ denote the inertia group of v in G and $\varphi_v \in G/I_v$ the arithmetic Frobenius of v. We then define elements g_v and h_v by

$$g_v = 1 - \varphi_v^{-1} + \#I_v \in \mathbb{Z}[G/I_v], \quad h_v = 1 - \frac{\nu_{I_v}}{\#I_v}\varphi_v^{-1} + \nu_{I_v} \in \mathbb{Q}[G],$$

where we put $\nu_{I_v} = \sum_{\tau \in I_v} \tau$. These elements are introduced in [Greither 2007, Lemmas 6.1 and 8.3] and [Kurihara 2021, Section 2.2, Equations (2.7) and (2.10)] (though in [Kurihara 2021] the same symbols g_v and h_v denote the involutions of ours). Note that $g_v = h_v$ if v is unramified in K/k. Moreover, we define a $\mathbb{Z}[G]$-module A_v by

$$A_v = \mathbb{Z}[G/I_v]/(g_v).$$

We write $\mathbb{Z}[G]^- = \mathbb{Z}[1/2][G]/(1+j)$, where j is the complex conjugation in G. For any $\mathbb{Z}[G]$-module M, we also define the minus component by $M^- = M \otimes_{\mathbb{Z}[G]} \mathbb{Z}[G]^-$. Note that we are implicitly inverting the action of 2. For any $x \in M$, we write x^- for the image of x under the natural map $M \to M^-$.

In general, for a set S of places of k, we write S_K for the set of places of K which lie above places in S. We take and fix a finite set T of finite primes of k satisfying the following:

- $T \cap S_{\mathrm{ram}}(K/k) = \varnothing$.
- $K_T^\times = \{x \in K^\times \mid \mathrm{ord}_w(x-1) > 0 \text{ for all primes } w \in T_K\}$ is torsion free. Here, ord_w denotes the normalized additive valuation.

Note that, if we fix an odd prime number p and are concerned with the p-components, the last condition can be weakened to that $K_T^\times$ is p-torsion-free. We consider the T-ray ideal class group of K defined by

$$\mathrm{Cl}_K^T = \mathrm{Cok}\left(K_T^\times \xrightarrow{\oplus \mathrm{ord}_w} \bigoplus_{w \notin T_K} \mathbb{Z}\right),$$

where w runs over the finite primes of K which are not in T_K.

For a character ψ of G, we write $L(s, \psi)$ for the primitive L-function for ψ. For any finite prime v of k, we put $N(v) = \#\mathbb{F}_v$, where $\mathbb{F}_v$ is the residue field of v. We then define the T-modified L-function by

$$L_T(s, \psi) = \left(\prod_{v \in T}(1 - \psi(\varphi_v)N(v)^{1-s})\right)L(s, \psi).$$

We define

$$\omega_T = \sum_{\psi} L_T(0, \psi)e_{\psi^{-1}} \in \mathbb{Q}[G], \tag{1-1}$$

where ψ runs over the characters of G and $e_\psi = \frac{1}{\#G}\sum_{\sigma \in G}\psi(\sigma)\sigma^{-1}$ is the idempotent of the ψ-component. We actually have $\omega_T \in \mathbb{Q}[G]$ instead of $\omega_T \in \mathbb{C}[G]$, thanks to the Siegel–Klingen theorem.

Now the first main theorem of this paper is the following, whose proof will be given in Section 3.

Theorem 1.1. *Assume that the eTNC for K/k holds. Then we have*

$$\mathrm{Fitt}_{\mathbb{Z}[G]^-}(\mathrm{Cl}_K^{T,-}) = \left(\prod_{v \in S_{\mathrm{ram}}(K/k) \setminus S_\infty(k)} h_v^- \, \mathrm{Fitt}^{[1]}_{\mathbb{Z}[G]^-}(A_v^-)\right)\omega_T^-,$$

where $\mathrm{Fitt}^{[1]}_{\mathbb{Z}[G]^-}$ *is the first shift of the Fitting ideal* (*see Definition 2.3*).

In the second main result below, we will obtain a concrete description of $h_v^- \, \mathrm{Fitt}^{[1]}_{\mathbb{Z}[G]^-}(A_v^-)$, which completes the description of the Fitting ideal of $\mathrm{Cl}_K^{T,-}$. We do not review the precise statement of the eTNC; see e.g., [Burns et al. 2016, Conjecture 3.6].

In order to compare with Theorem 1.1, we recall the result for the dualized version:

$$\mathrm{Fitt}_{\mathbb{Z}[G]^-}(\mathrm{Cl}_K^{T,\vee,-}) = \left(\prod_{v \in S_{\mathrm{ram}}(K/k) \setminus S_\infty(k)} \left(\nu_{I_v}, 1 - \frac{\nu_{I_v}}{\#I_v}\varphi_v^{-1}\right)^-\right)\omega_T^-. \tag{1-2}$$

As already mentioned, Kurihara [2021, Corollary 3.7] showed this formula under the validity of the eTNC, and recently Dasgupta and Kakde [2023, Theorem 1.4] removed the assumption. Here, for a general G-module M, we equip the Pontryagin dual $M^\vee$ with the G-action by $(\sigma f)(x) = f(\sigma x)$ for $\sigma \in G$, $f \in M^\vee$, and $x \in M$. This convention is the opposite of [Kurihara 2021] and [Dasgupta and Kakde 2023], so the right-hand side of the formula (1-2) differs from those by the involution.

We now briefly outline the proof of Theorem 1.1. An important ingredient is an exact sequence of $\mathbb{Z}[G]^-$-modules of the form

$$0 \to \mathfrak{A}^- \to W_{S_\infty}^- \to \mathrm{Cl}_K^{T,-} \to 0$$

as in Proposition 3.2, where $\mathfrak{A}^-$ is a projective module of finite rank $\#S'$. Here, S' is an auxiliary finite set of places of k. This sequence was constructed by Kurihara [2021], based on preceding work such as Ritter and Weiss [1996] and Greither [2007], and played a key role in proving (1-2) under the eTNC. Our novel idea is to construct an explicit injective homomorphism from $W_{S_\infty}^-$ to $(\mathbb{Z}[G]^-)^{\oplus \#S'}$ whose cokernel is isomorphic to the direct sum of A_v^- for $v \in S' \setminus S_\infty(k)$. Moreover, assuming the eTNC, we will compute the determinant of the composite map $\mathfrak{A}^- \hookrightarrow W_{S_\infty}^- \hookrightarrow (\mathbb{Z}[G]^-)^{\oplus \#S'}$. By using these observations, we obtain an exact sequence to which the theory of shifts of Fitting ideals can be applied, and then Theorem 1.1 follows.

1B. ***Computation of the shift of Fitting ideal.*** In order to make the formula of Theorem 1.1 more explicit, in Section 4, we will compute $\mathrm{Fitt}^{[1]}_{\mathbb{Z}[G]}(A_v)$. This will be accomplished by using a method similar to Greither and Kurihara [2015, Section 1.2], which was actually a motivation for introducing the shifts of Fitting ideals in [Kataoka 2020].

As the problem is purely algebraic, we deal with a general situation as follows (it should be clear from the notation how to apply the results below to the arithmetic situation; simply add subscripts v appropriately). Let G be a finite abelian group. Let I and D be subgroups of G such that $I \subset D \subset G$ and that the quotient D/I is a cyclic group. We choose a generator φ of D/I and put

$$g = 1 - \varphi^{-1} + \#I \in \mathbb{Z}[G/I], \quad h = 1 - \frac{\nu_I}{\#I}\varphi^{-1} + \nu_I \in \mathbb{Q}[G],$$

which are not a zero divisor. We define a finite $\mathbb{Z}[G]$-module A by

$$A = \mathbb{Z}[G/I]/(g).$$

In order to state the result, we introduce some notations. We choose a decomposition

$$I = I_1 \times \cdots \times I_s \tag{1-3}$$

as an abelian group such that I_l is a cyclic group for each $1 \leq l \leq s$. Here, we do not assume any minimality on this decomposition, so we allow even the extreme case where I_l is trivial for some l.

For each $1 \leq l \leq s$, we put $\nu_l = \nu_{I_l} = \sum_{\sigma \in I_l} \sigma \in \mathbb{Z}[G]$. We also put $\mathcal{I}_D = \mathrm{Ker}(\mathbb{Z}[G] \to \mathbb{Z}[G/D])$.

Definition 1.2. For $0 \leq i \leq s$, we define Z_i as the ideal of $\mathbb{Z}[G]$ generated by $\nu_{l_1} \cdots \nu_{l_{s-i}}$ where $(l_1, \dots, l_{s-i})$ runs over all tuples of integers satisfying $1 \leq l_1 < \cdots < l_{s-i} \leq s$, that is,

$$Z_i = (\nu_{l_1} \cdots \nu_{l_{s-i}} \mid 1 \leq l_1 < \cdots < l_{s-i} \leq s).$$

We clearly have $Z_0 = (\nu_I) \subset Z_1 \subset \cdots \subset Z_s = (1)$. We then define an ideal $\mathcal{J}$ of $\mathbb{Z}[G]$ by

$$\mathcal{J} = \sum_{i=1}^{s} Z_i \mathcal{I}_D^{i-1}.$$

Note that the definition of Z_i does depend on the choice of the decomposition (1-3). On the other hand, it can be shown directly that the ideal $\mathcal{J}$ is independent from the choice. We omit the direct proof because, at any rate, the independency can be deduced from the discussion in Section 4.

Example 1.3. When $s = 1$, we have

$$\mathcal{J} = (1).$$

When $s = 2$, we have

$$\mathcal{J} = (\nu_1, \nu_2) + \mathcal{I}_D.$$

When $s = 3$, we have

$$\mathcal{J} = (\nu_1\nu_2, \nu_2\nu_3, \nu_3\nu_1) + (\nu_1, \nu_2, \nu_3)\mathcal{I}_D + \mathcal{I}_D^2.$$

In this setting, we can describe $\operatorname{Fitt}^{[1]}_{\mathbb{Z}[G]}(A)$ as follows. It is convenient to state the result after multiplying by h.

Theorem 1.4. *We have*

$$h \operatorname{Fitt}^{[1]}_{\mathbb{Z}[G]}(A) = \left(\nu_I, \left(1 - \frac{\nu_I}{\#I}\varphi^{-1}\right)\mathcal{J}\right)$$

as fractional ideals of $\mathbb{Z}[G]$.

1C. ***Stickelberger element and Fitting ideal.*** As an application of Theorems 1.1 and 1.4, we shall discuss the problem whether or not the Stickelberger element lies in the Fitting ideal of $\mathrm{Cl}_K^{T,-}$.

We return to the setup in Section 1A. Let p be a fixed odd prime number and we shall work over $\mathbb{Z}_p$. Let G' denote the maximal subgroup of G of order prime to p. We put $k_p = K^{G'}$, which is the maximal p-extension of k contained in K. For each character χ of G', we regard $\mathcal{O}_\chi = \mathbb{Z}_p[\mathrm{Im}(\chi)]$ as a $\mathbb{Z}_p[G']$-module via χ, and put $\mathbb{Z}_p[G]^\chi = \mathbb{Z}_p[G] \otimes_{\mathbb{Z}_p[G']} \mathcal{O}_\chi$. For a $\mathbb{Z}_p[G]$-module M, we put $M^\chi = M \otimes_{\mathbb{Z}_p[G]} \mathbb{Z}_p[G]^\chi$, which is a $\mathbb{Z}_p[G]^\chi$-module. For an element $x \in M$, we write x^χ for the image of x by the natural map $M \to M^\chi$. We note that $\mathbb{Z}_p[G]$ is isomorphic to the direct product of $\mathbb{Z}_p[G]^\chi$ if χ runs over the equivalence classes of characters of G'.

From now on, we fix an odd character χ of G'. We define $K_\chi = K^{\mathrm{Ker}(\chi)}$. Then K_χ is a CM-field, $K_\chi \supset k_p$, and K_χ / k_p is a cyclic extension of order prime to p.

We put $S_\chi = S_{\mathrm{ram}}(K_\chi/k)$ and consider the χ-component of the Stickelberger element defined by

$$\theta^\chi_{K/k,T} = \sum_{\psi|_{G'}=\chi} L_{S_\chi,T}(0, \psi) e_{\psi^{-1}} \in \mathbb{Z}_p[G]^\chi, \tag{1-4}$$

where ψ runs over characters of G whose restriction to G' coincides with χ and we write

$$L_{S_\chi,T}(s, \psi) = \left(\prod_{v \in S_\chi \setminus S_\infty(k)} (1 - \psi(\varphi_v))\right)\left(\prod_{v\in T}(1 - \psi(\varphi_v)N(v)^{1-s})\right)L(s, \psi).$$

Note that, comparing (1-1) and (1-4), we have

$$\theta^\chi_{K/k,T} = \left(\prod_{v \in S_\chi \setminus S_\infty(k)} \left(1 - \frac{\nu_{I_v}}{\#I_v}\varphi_v^{-1}\right)^\chi\right)\omega_T^\chi. \tag{1-5}$$

Concerning the dualized version, by the work of Dasgupta and Kakde [2023, Theorem 1.3], we always have

$$\theta^\chi_{K/k,T} \in \operatorname{Fitt}_{\mathbb{Z}_p[G]^\chi}((\mathrm{Cl}_K^T \otimes \mathbb{Z}_p)^{\vee,\chi}).$$

This is called the strong Brumer–Stark conjecture. More precisely, the displayed claim is a bit stronger than [Dasgupta and Kakde 2023, Theorem 1.3] as we took S_χ instead of $S_{\mathrm{ram}}(K/k)$ in the definition of the Stickelberger element, but in any case it is an immediate consequence of the formula (1-2).

On the other hand, the corresponding claim without dual is known to be false in general; see [Greither and Kurihara 2008]. However, we had only partial results and an exact condition was unknown. The following theorem is strong as it gives a *necessary and sufficient* condition.

Theorem 1.5. *Assume that the eTNC for K/k holds* (*indeed*, *the p-part of the eTNC suffices*). *Then*, *for each odd character χ of G'*, *the following are equivalent*:

(i) *We have $\theta^{\chi}_{K/k,T} \in \mathrm{Fitt}_{\mathbb{Z}_p[G]^{\chi}}((\mathrm{Cl}^T_K \otimes \mathbb{Z}_p)^{\chi})$.*

(ii) *We have either $\theta^{\chi}_{K/k,T} = 0$ or*, *for any $v \in S_{\chi} \setminus S_{\infty}(k)$*, *one of the following holds.*

   (a) *v does not split completely in K_{χ}/k_p.*

   (b) *The inertia group I_v is cyclic.*

This theorem will be proved in Section 5 as an application of Theorems 1.1 and 1.4. Note that there is an elementary equivalent condition for $\theta^{\chi}_{K/k,T} = 0$ as in Lemma 5.3.

Theorem 1.5 indicates that the failure of the inertia groups to be cyclic is an obstruction for studying the Fitting ideal of the class group *without dual*. The same phenomenon will appear again in Theorem 1.6 below. We should say that this kind of phenomenon had been observed in preceding work, such as [Greither and Kurihara 2008]. Nickel [2011, Section 4] studied much the same subject when all the p-adic primes are tamely ramified. In that case, the inertia groups are indeed cyclic, so a main result [Nickel 2011, Section 4.2, Theorem 5] is now a part of Theorem 1.5.

It is also remarkable that the obstruction does not occur in the absolutely abelian case (i.e., when $k = \mathbb{Q}$), since in that case the inertia groups are automatically cyclic, apart from the 2-parts. This seems to fit the fact that Kurihara [2003a] and Kurihara and Miura [2011] succeeded in studying the class groups without dual in the absolutely abelian case.

Let us outline the proof of Theorem 1.5. We assume that χ is a faithful character of G' (i.e., $K_{\chi} = K$); actually we can deduce the general case from this case. Since ω^{χ}_T is a not a zero divisor of $\mathbb{Z}_p[G]^{\chi}$, by Theorem 1.1 and (1-5), we have $\theta^{\chi}_{K/k,T} \in \mathrm{Fitt}_{\mathbb{Z}_p[G]^{\chi}}((\mathrm{Cl}^T_K \otimes \mathbb{Z}_p)^{\chi})$ if and only if

$$\prod_v \left(1 - \frac{\nu_{I_v}}{\# I_v}\varphi_v^{-1}\right)^{\chi} \subset \prod_v (h_v \, \mathrm{Fitt}^{[1]}_{\mathbb{Z}_p[G]}(A_v \otimes \mathbb{Z}_p))^{\chi} \tag{1-6}$$

holds as fractional ideals of $\mathbb{Z}_p[G]^{\chi}$, where on both sides v runs over the elements of $S_{\mathrm{ram}}(K/k) \setminus S_{\infty}(k)$.

Obviously we may assume that $\theta^{\chi}_{K/k,T} \neq 0$. The proof of (ii) ⇒ (i) is the easier part. We will show that, under the assumption (ii), the inclusion of (1-6) holds even for every v before taking the product. On the other hand, the opposite direction (i) ⇒ (ii) is the harder part. That is because, roughly speaking, we have to work over the ring $\mathbb{Z}_p[G]^{\chi}$, whose ring theoretic properties are not very nice. A key idea to overcome this issue is to reduce to a computation in a discrete valuation ring. More concretely, we make use of a character ψ of G which satisfies $\psi|_{G'} = \chi$ and a certain additional condition, whose existence is verified by Lemma 5.3, and then we consider the $\mathbb{Z}_p[G]^{\chi}$-algebra $\mathcal{O}_{\psi} = \mathbb{Z}_p[\mathrm{Im}(\psi)]$. By investigating the ideals in (1-6) after base change from $\mathbb{Z}_p[G]^{\chi}$ to $\mathcal{O}_{\psi}$, we will show (i) ⇒ (ii).

1D. ***Unconditional consequences.*** Even if we do not assume the validity of the eTNC, our argument shows the following.

Theorem 1.6. *We have an inclusion*

$$\mathrm{Fitt}_{\mathbb{Z}[G]^-}(\mathrm{Cl}_K^{T,-}) \subset \mathrm{Fitt}_{\mathbb{Z}[G]^-}(\mathrm{Cl}_K^{T,\vee,-}).$$

Moreover, the inclusion is an equality if I_v is cyclic for every $v \in S_{\mathrm{ram}}(K/k) \setminus S_\infty(k)$.

This theorem follows immediately from Corollaries 3.7 and 4.2. Furthermore, by similar arguments as the proof of Theorem 1.5, we can observe that the inclusion is often proper.

As already remarked, Dasgupta and Kakde [2023] proved the formula (1-2) *unconditionally*. Therefore, if I_v is cyclic for every $v \in S_{\mathrm{ram}}(K/k) \setminus S_\infty(k)$, we can also deduce from Theorem 1.6 that $\mathrm{Fitt}_{\mathbb{Z}[G]^-}(\mathrm{Cl}_K^{T,-})$ also coincides with that ideal, and this removes the assumption on the eTNC in Theorem 1.1. However, in Theorem 1.1 we still need to assume the eTNC when I_v is not cyclic for some v.

2. Definition of Fitting ideals and their shifts

In this section, we fix our notations concerning Fitting ideals.

2A. ***Fitting ideals.*** Let R be a noetherian ring.

Definition 2.1 [Northcott 1976]. We define the Fitting ideals as follows:

(i) Let A be a matrix over R with m rows and n columns. For each integer $0 \le i \le n$, we define $\mathrm{Fitt}_{i,R}(A)$ as the ideal of R generated by the $(n-i) \times (n-i)$ minors of A. For each integer $i > n$, we also define $\mathrm{Fitt}_{i,R}(A) = (1)$.

(ii) Let X be a finitely generated R-module. We choose a finite presentation A of X with m rows and n columns, that is, an exact sequence

$$R^m \xrightarrow{\times A} R^n \to X \to 0.$$

Here and henceforth, as a convention, we deal with row vectors, so we multiply matrices from the right. Then, for each $i \ge 0$, we define the i-th Fitting ideal of X by

$$\mathrm{Fitt}_{i,R}(X) = \mathrm{Fitt}_{i,R}(A).$$

It is known that this ideal does not depend on the choice of A. When $i = 0$, we also write $\mathrm{Fitt}_R(X) = \mathrm{Fitt}_{0,R}(X)$ and call it the initial Fitting ideal.

We will later make use of the following elementary lemma. We omit the proof; see [Kurihara 2003b, Lemma 3.3].

Lemma 2.2. *Let X be a finitely generated R-module and I be an ideal of R. If X is generated by n elements over R, then we have*

$$\mathrm{Fitt}_{0,R}(X/IX) = \sum_{i=0}^{n} I^i \,\mathrm{Fitt}_{i,R}(X).$$

2B. ***Shifts of Fitting ideals.*** In this subsection, we review the definition of shifts of Fitting ideals introduced by Kataoka [2020].

Although we can deal with a more general situation, for simplicity we consider the following. Let Λ be a Dedekind domain (e.g., $\Lambda = \mathbb{Z}$, $\mathbb{Z}\left[\frac{1}{2}\right]$, or $\mathbb{Z}_p$). Let Δ be a finite abelian group and consider the ring $R = \Lambda[\Delta]$.

We define $\mathcal{C}$ as the category of R-modules of finite length. We also define a subcategory $\mathcal{P}$ of $\mathcal{C}$ by

$$\mathcal{P} = \{P \in \mathcal{C} \mid \mathrm{pd}_R(P) \le 1\},$$

where pd_R denotes the projective dimension over R. Note that any module M in $\mathcal{C}$ satisfies $\mathrm{pd}_\Lambda(M) \le 1$.

Definition 2.3. Let X be an R-module in $\mathcal{C}$ and $d \ge 0$ an integer. We take an exact sequence

$$0 \to Y \to P_1 \to \cdots \to P_d \to X \to 0$$

in $\mathcal{C}$ with $P_1, \dots, P_d \in \mathcal{P}$. Then we define

$$\mathrm{Fitt}_R^{[d]}(X) = \left(\prod_{i=1}^{d} \mathrm{Fitt}_R(P_i)^{(-1)^i} \right) \mathrm{Fitt}_R(Y).$$

The well-definedness (i.e., the independence from the choice of the d-step resolution) is proved in [Kataoka 2020, Theorem 2.6 and Proposition 2.7].

We also introduce a variant for the case where d is negative.

Definition 2.4. Let X be an R-module in $\mathcal{C}$ and $d \le 0$ an integer. We take an exact sequence

$$0 \to X \to P_{-d} \to \cdots \to P_1 \to Y \to 0$$

in $\mathcal{C}$ with $P_1, \dots, P_{-d} \in \mathcal{P}$. Then we define

$$\mathrm{Fitt}_R^{\langle d \rangle}(X) = \left(\prod_{i=1}^{-d} \mathrm{Fitt}_R(P_i)^{(-1)^i} \right) \mathrm{Fitt}_R(Y).$$

The well-definedness is proved in [Kataoka 2020, Theorem 3.19 and Propositions 2.7 and 3.17].

3. Fitting ideals of ideal class groups

In this section, we prove Theorem 1.1, which describes the Fitting ideal of $\mathrm{Cl}_K^{T,-}$ using shifts of Fitting ideals. We keep the notation in Section 1A.

3A. ***Brief review of work of Kurihara.*** We first review necessary ingredients from [Kurihara 2021], which in turn relies on preceding work, in particular [Ritter and Weiss 1996] and [Greither 2007].

For each place w of K, let D_w and I_w denote the decomposition subgroup and the inertia subgroup of w in G, respectively. These subgroups depend only on the place of k which lies below w.

Let us introduce local modules W_v. For any finite group H, we define ΔH as the augmentation ideal in $\mathbb{Z}[H]$.

Definition 3.1. For each finite prime w of K, we define a $\mathbb{Z}[D_w]$-module W_{K_w} by

$$W_{K_w} = \{(x, y) \in \Delta D_w \oplus \mathbb{Z}[D_w/I_w] \mid \bar{x} = (1 - \varphi_v^{-1})y\},$$

where $\bar{x}$ denotes the image of x in $\mathbb{Z}[D_w/I_w]$. For each finite prime v of k, we define the $\mathbb{Z}[G]$-module W_v by taking the direct sum as

$$W_v = \bigoplus_{w \mid v} W_{K_w},$$

where w runs over the finite primes of K which lie above v. Alternatively, W_v can be regarded as the induced module of W_{K_w} from D_w to G, as long as we choose a place w of K above v.

We take an auxiliary finite set S' of places of k satisfying the following conditions:

- $S' \supset S_{\mathrm{ram}}(K/k)$.
- $S' \cap T = \varnothing$.
- $\mathrm{Cl}^T_{K,S'} = 0$, where $\mathrm{Cl}^T_{K,S'} = \mathrm{Cok}(K_T^\times \xrightarrow{\oplus \mathrm{ord}_w} \bigoplus_{w \notin S'_K \cup T_K} \mathbb{Z})$.
- G is generated by the decomposition groups D_v of v for all $v \in S'$.

We define a $\mathbb{Z}[G]$-module W_{S_∞} by

$$W_{S_\infty} = \bigoplus_{w \in S_\infty(K)} \Delta D_w \oplus \bigoplus_{v \in S' \setminus S_\infty(k)} W_v.$$

By using local and global class field theory, Kurihara constructed an exact sequence of the following form.

Proposition 3.2 [Kurihara 2021, Section 2.2, sequence (2.5)]. *We have an exact sequence*

$$0 \to \mathfrak{A}^- \to W_{S_\infty}^- \to \mathrm{Cl}_K^{T,-} \to 0,$$

where $\mathfrak{A}^-$ is a projective $\mathbb{Z}[G]^-$-module of rank $\#S'$.

Remark 3.3. Kurihara [2021] took the linear dual of this sequence, and the resulting sequence played an important role to study $\mathrm{Cl}_K^{T,\vee,-}$. In this paper, we do not take the linear dual but instead study the sequence itself for the proof of Theorem 1.1.

3B. ***Definition of f_v.*** Our key ingredient for the proof of Theorem 1.1 is the following homomorphism f_v.

Definition 3.4. For a finite prime w of K, we define a $\mathbb{Z}[D_w]$-homomorphism

$$f_w : W_{K_w} \to \mathbb{Z}[D_w]$$

by $f_w(x, y) = x + \nu_{I_w}(y)$ (recall the definition of W_{K_w} in Definition 3.1). For a finite prime v of k, we then define a $\mathbb{Z}[G]$-homomorphism $f_v : W_v \to \mathbb{Z}[G]$ by

$$f_v : W_v = \bigoplus_{w \mid v} W_{K_w} \xrightarrow{\oplus f_w} \bigoplus_{w \mid v} \mathbb{Z}[D_w] \simeq \mathbb{Z}[G],$$

where the last isomorphism depends on a choice of w.

In Section 1A we introduced a finite $\mathbb{Z}[G]$-module $A_v = \mathbb{Z}[G/I_v]/(g_v)$ with $g_v = 1 - \varphi_v^{-1} + \# I_v$. It is actually motivated by the following.

Lemma 3.5. *For any finite prime v of k, the map f_v is injective and*

$$\operatorname{Cok} f_v \simeq A_v.$$

Proof. It is enough to show that f_w is injective and $\operatorname{Cok} f_w \simeq \mathbb{Z}[D_w/I_w]/(g_v)$ for any finite prime w of K. Put $J_w = \operatorname{Ker}(\mathbb{Z}[D_w] \to \mathbb{Z}[D_w/I_w])$. We define a homomorphism $\alpha_w : J_w \to W_{K_w}$ by $\alpha_w(x) = (x, 0)$. Let us consider the following commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & J_w \arrow[r, "\alpha_w"] \arrow[d, equal] & W_{K_w} \arrow[r] \arrow[d, "f_w"] & \operatorname{Cok}\alpha_w \arrow[r] \arrow[d, "f'_w"] & 0 \\
0 \arrow[r] & J_w \arrow[r] & \mathbb{Z}[D_w] \arrow[r] & \mathbb{Z}[D_w/I_w] \arrow[r] & 0
\end{tikzcd}$$

where the lower sequence is the trivial one, the commutativity of the left square is easy, and the right vertical arrow is the induced one. By the definition of W_{K_w}, we have

$$\operatorname{Cok}\alpha_w = \{(\bar{x}, y) \in \Delta(D_w/I_w) \times \mathbb{Z}[D_w/I_w] \mid \bar{x} = (1 - \varphi_v^{-1})y\}.$$

Since D_w/I_w is a cyclic group generated by φ_v^{-1}, the $\mathbb{Z}[D_w/I_w]$-module $\operatorname{Cok}\alpha_w$ is free of rank 1 with a basis $(1 - \varphi_v^{-1}, 1)$. Moreover, f'_w sends this basis to $g_v = 1 - \varphi_v^{-1} + \# I_v$. Therefore, f'_w is injective with cokernel isomorphic to $\mathbb{Z}[D_w/I_w]/(g_v)$. Then by the diagram f_w also satisfies the desired properties. □

For any $v \in S' \setminus S_\infty(k)$, we consider the homomorphism $f_v^- : W_v^- \to \mathbb{Z}[G]^-$ which is the minus component of f_v. For any $v \in S_\infty(k)$, we have $(\oplus_{w \mid v} \Delta D_w)^- \simeq \mathbb{Z}[G]^-$ by choosing w, so we fix this isomorphism and write f_v^- for it. Using these f_v^-, we consider the following commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & \mathfrak{A}^- \arrow[r] \arrow[d, equal] & W_{S_\infty}^- \arrow[r] \arrow[d, "\oplus_{v \in S'} f_v^-"] & \mathrm{Cl}_K^{T,-} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathfrak{A}^- \arrow[r, "\psi"] & \bigoplus_{v \in S'} \mathbb{Z}[G]^- \arrow[r] & \operatorname{Cok}\psi \arrow[r] & 0,
\end{tikzcd}$$

where the upper sequence is that in Proposition 3.2 and the map ψ is defined by the commutativity. By Lemma 3.5 and the snake lemma, we get the following proposition.

Proposition 3.6. *We have an exact sequence*

$$0 \to \mathrm{Cl}_K^{T,-} \to \operatorname{Cok}\psi \to \bigoplus_{v\in S'\setminus S_\infty(k)} A_v^- \to 0.$$

Moreover, the $\mathbb{Z}[G]^-$*-module* $\operatorname{Cok}\psi$ *is finite with* $\mathrm{pd}_{\mathbb{Z}[G]^-}(\operatorname{Cok}\psi) \le 1$.

Then we can describe the Fitting ideals of $\mathrm{Cl}_K^{T,-}$ and of $\mathrm{Cl}_K^{T,\vee,-}$ as follows.

Corollary 3.7. *We have*

$$\mathrm{Fitt}_{\mathbb{Z}[G]^-}(\mathrm{Cl}_K^{T,-}) = \mathrm{Fitt}_{\mathbb{Z}[G]^-}(\operatorname{Cok}\psi) \prod_{v\in S'\setminus S_\infty(k)} \mathrm{Fitt}^{[1]}_{\mathbb{Z}[G]^-}(A_v^-)$$

and

$$\mathrm{Fitt}_{\mathbb{Z}[G]^-}(\mathrm{Cl}_K^{T,\vee,-}) = \mathrm{Fitt}_{\mathbb{Z}[G]^-}(\operatorname{Cok}\psi) \prod_{v\in S'\setminus S_\infty(k)} \mathrm{Fitt}^{\langle -1\rangle}_{\mathbb{Z}[G]^-}(A_v^-).$$

Proof. The first formula follows directly from Proposition 3.6 and Definition 2.3. For the second formula, by [Kataoka 2020, Proposition 4.7], we have

$$\mathrm{Fitt}_{\mathbb{Z}[G]^-}(\mathrm{Cl}_K^{T,\vee,-}) = \mathrm{Fitt}^{\langle -2\rangle}_{\mathbb{Z}[G]^-}(\mathrm{Cl}_K^{T,-}).$$

By Proposition 3.6 and Definition 2.4, we also have

$$\mathrm{Fitt}^{\langle -2\rangle}_{\mathbb{Z}[G]^-}(\mathrm{Cl}_K^{T,-}) = \mathrm{Fitt}_{\mathbb{Z}[G]^-}(\operatorname{Cok}\psi) \prod_{v\in S'\setminus S_\infty(k)} \mathrm{Fitt}^{\langle -1\rangle}_{\mathbb{Z}[G]^-}(A_v^-).$$

This completes the proof. □

3C. *Fitting ideal of* Cok ψ.

Recall the definitions of ω_T and of h_v in Section 1A.

Theorem 3.8. *Assume that the eTNC for K/k holds. Then we have*

$$\mathrm{Fitt}_{\mathbb{Z}[G]^-}(\operatorname{Cok}\psi) = \biggl(\biggl(\prod_{v\in S'\setminus S_\infty(k)} h_v^-\biggr)\omega_T^-\biggr).$$

Proof. For each $v \in S'\setminus S_\infty(k)$, we define a basis e_v of $\mathrm{Hom}_{\mathbb{Q}[G]}(W_v\otimes\mathbb{Q}, \mathbb{Q}[G])$ as in [Kurihara 2021, Section 2.2, Equation (2.9)] (we do not recall the precise definition here). Then we can see that its dual basis e'_v of $W_v\otimes\mathbb{Q}$ is given by

$$e'_v = \frac{1}{1-\widetilde{\varphi_v}^{-1}+N_{I_v}}(1-\widetilde{\varphi_v}^{-1}, 1),$$

where $\widetilde{\varphi_v}$ is a lift of φ_v. Then, by the definition of f_v, this element satisfies $f_v(e'_v)=1$, where by abuse of notation f_v denotes the homomorphism $W_v\otimes\mathbb{Q}\to\mathbb{Q}[G]$ induced by $f_v : W_v \to \mathbb{Z}[G]$. For $v \in S_\infty(k)$, as a basis over $\mathbb{Z}[G]^-$, we take the element $e_v'^{,-}$ of $\bigl(\bigoplus_{w\mid v}\Delta D_w\bigr)^-$ which is characterized by $f_v^-(e_v'^{,-})=1$.

Let us consider the isomorphism $\Psi : \mathfrak{A}^- \otimes \mathbb{Q} \to W^-_{S_\infty} \otimes \mathbb{Q}$ induced by the sequence in Proposition 3.2. Then, under the eTNC, Kurihara [2021, Theorem 3.6] proved that $\mathfrak{A}^-$ is a free $\mathbb{Z}[G]^-$-module (a priori we only know $\mathfrak{A}^-$ is projective) and

$$\det(\Psi) = \biggl(\prod_{v \in S' \setminus S_\infty(k)} h_v^- \biggr) \omega_T^-$$

with respect to a certain basis of $\mathfrak{A}^-$ as a $\mathbb{Z}[G]^-$-module and the basis $(e_v'^{,-})_{v \in S'}$ of $W^-_{S_\infty}$. Actually this is an easy reformulation of the result of Kurihara, which concerns the determinant of the linear dual of Ψ.

Therefore, the determinant of the composite map ψ of Ψ and $\bigoplus_{v \in S'} f_v^-$, with respect to the basis of $\mathfrak{A}^-$ and the standard basis of $(\mathbb{Z}[G]^-)^{\oplus \# S'}$, also coincides with $\bigl(\prod_{v \in S' \setminus S_\infty(k)} h_v^-\bigr)\omega_T^-$. This shows the theorem. □

We are now ready to prove Theorem 1.1.

Proof of Theorem 1.1. By Corollary 3.7 and Theorem 3.8, we have

$$\mathrm{Fitt}_{\mathbb{Z}[G]^-}(\mathrm{Cl}_K^{T,-}) = \biggl(\prod_{v \in S' \setminus S_\infty(k)} h_v^- \, \mathrm{Fitt}^{[1]}_{\mathbb{Z}[G]^-}(A_v^-) \biggr) \omega_T^-.$$

For $v \in S' \setminus S_{\mathrm{ram}}(K/k)$, we have $A_v = \mathbb{Z}[G]/(h_v)$, so

$$\mathrm{Fitt}^{[1]}_{\mathbb{Z}[G]^-}(A_v^-) = (h_v^-)^{-1}.$$

Then Theorem 1.1 follows. □

Remark 3.9. Similarly, under the validity of the eTNC, Corollary 3.7 and Theorem 3.8 also imply a formula

$$\mathrm{Fitt}_{\mathbb{Z}[G]^-}(\mathrm{Cl}_K^{T,\vee,-}) = \biggl(\prod_{v \in S_{\mathrm{ram}}(K/k) \setminus S_\infty(k)} h_v^- \, \mathrm{Fitt}^{\langle -1 \rangle}_{\mathbb{Z}[G]^-}(A_v^-) \biggr) \omega_T^-.$$

Combining this with Proposition 4.1 below, we can recover the formula (1-2). This argument may be regarded as a reinterpretation of the work [Kurihara 2021] by using the shifts of Fitting ideals.

4. Computation of shifts of Fitting ideals

In this section, we prove Theorem 1.4 on the description of $\mathrm{Fitt}^{[1]}_{\mathbb{Z}[G]}(A)$. We keep the notations as in Section 1B.

4A. *Computation of* $\mathrm{Fitt}^{\langle -1 \rangle}_{\mathbb{Z}[G]}(A)$.

Before $\mathrm{Fitt}^{[1]}_{\mathbb{Z}[G]}(A)$, we determine $\mathrm{Fitt}^{\langle -1 \rangle}_{\mathbb{Z}[G]}(A)$, which is actually much easier.

We choose a lift $\widetilde{\varphi} \in D$ of φ and put

$$\tilde{g} = 1 - \widetilde{\varphi}^{-1} + \# I \in \mathbb{Z}[G],$$

which is again a not a zero divisor. Obviously, g is then the natural image of $\tilde{g}$ to $\mathbb{Z}[G/I]$.

Proposition 4.1. *We have*

$$\mathrm{Fitt}^{\langle -1\rangle}_{\mathbb{Z}[G]}(A) = (1, \nu_I g^{-1}).$$

Therefore, *we also have*

$$h\,\mathrm{Fitt}^{\langle -1\rangle}_{\mathbb{Z}[G]}(A) = \left(\nu_I, 1 - \frac{\nu_I}{\#I}\varphi^{-1}\right).$$

Proof. We have an exact sequence

$$0 \to \mathbb{Z}[G/I] \xrightarrow{\nu_I} \mathbb{Z}[G] \to \mathbb{Z}[G]/(\nu_I) \to 0.$$

Since multiplication by $\tilde{g}$ is injective on each of these modules, applying the snake lemma, we obtain an exact sequence

$$0 \to A \to \mathbb{Z}[G]/(\tilde{g}) \to \mathbb{Z}[G]/(\tilde{g}, \nu_I) \to 0.$$

By Definition 2.4, we then have

$$\mathrm{Fitt}^{\langle -1\rangle}_{\mathbb{Z}[G]}(A) = (\tilde{g})^{-1}(\tilde{g}, \nu_I) = (1, \nu_I g^{-1}).$$

This proves the former formula of the proposition.

Since we have $\nu_I g = \nu_I h$, the former formula implies $h\,\mathrm{Fitt}^{\langle -1\rangle}_{\mathbb{Z}[G]}(A) = (\nu_I, h)$. Then the latter formula follows from $h \equiv 1 - \frac{\nu_I}{\#I}\varphi^{-1} \pmod{(\nu_I)}$. □

Before proving Theorem 1.4, we show a corollary.

Corollary 4.2. *We have an inclusion*

$$\mathrm{Fitt}^{[1]}_{\mathbb{Z}[G]}(A) \subset \mathrm{Fitt}^{\langle -1\rangle}_{\mathbb{Z}[G]}(A).$$

Moreover, *if I is a cyclic group*, *the inclusion is an equality.*

Proof. By Definition 1.2, the ideal $\mathcal{J}$ is contained in $\mathbb{Z}[G]$ and we have $\mathcal{J} = \mathbb{Z}[G]$ if I is cyclic. Hence this corollary immediately follows from Theorem 1.4 and Proposition 4.1. □

4B. *Computation of* $\mathrm{Fitt}^{[1]}_{\mathbb{Z}[G]}(A)$.

This subsection is devoted to the proof of Theorem 1.4.

We fix the decomposition (1-3) of I. For each $1 \le l \le s$, we choose a generator σ_l of I_l and put $\tau_l = \sigma_l - 1 \in \mathbb{Z}[G]$. Note that we then have $\nu_l = 1 + \sigma_l + \sigma_l^2 + \cdots + \sigma_l^{\#I_l - 1}$ and $\tau_l \nu_l = 0$. As in Section 4A, we put $\tilde{g} = 1 - \widetilde{\varphi}^{-1} + \#I$ after choosing $\widetilde{\varphi}$.

We recall $\mathcal{I}_D = \mathrm{Ker}(\mathbb{Z}[G] \to \mathbb{Z}[G/D])$ and also put $\mathcal{I}_I = \mathrm{Ker}(\mathbb{Z}[G] \to \mathbb{Z}[G/I])$. Then we have $\mathcal{I}_I = (\tau_1, \dots, \tau_s)$ and $\mathcal{I}_D = (\mathcal{I}_I, 1 - \widetilde{\varphi}^{-1})$.

We begin with a proposition.

Proposition 4.3. *We have*

$$\mathrm{Fitt}^{[1]}_{\mathbb{Z}[G]}(A) = \sum_{i=0}^{s} \tilde{g}^{i-1}\,\mathrm{Fitt}_{i,\mathbb{Z}[G]}(\mathcal{I}_I).$$

Proof. We have the tautological exact sequence

$$0 \to \mathcal{I}_I \to \mathbb{Z}[G] \to \mathbb{Z}[G/I] \to 0.$$

Since multiplication by $\tilde{g}$ is injective on each of these modules, by applying snake lemma, we obtain an exact sequence

$$0 \to \mathcal{I}_I/\tilde{g}\mathcal{I}_I \to \mathbb{Z}[G]/(\tilde{g}) \to A \to 0.$$

Then Definition 2.3 implies

$$\mathrm{Fitt}^{[1]}_{\mathbb{Z}[G]}(A) = \tilde{g}^{-1}\,\mathrm{Fitt}_{\mathbb{Z}[G]}(\mathcal{I}_I/\tilde{g}\mathcal{I}_I).$$

Since $\mathcal{I}_I$ is generated by the s elements $\tau_1, \dots, \tau_s$, we have

$$\mathrm{Fitt}_{\mathbb{Z}[G]}(\mathcal{I}_I/\tilde{g}\mathcal{I}_I) = \sum_{i=0}^{s} \tilde{g}^i\,\mathrm{Fitt}_{i,\mathbb{Z}[G]}(\mathcal{I}_I)$$

by Lemma 2.2. Thus we obtain the proposition. □

Our next task is to determine $\mathrm{Fitt}_{i,\mathbb{Z}[G]}(\mathcal{I}_I)$ for $0 \leq i \leq s$. The result will be Proposition 4.9 below. For that purpose, we construct a concrete free resolution of $\mathbb{Z}$ over $\mathbb{Z}[I]$, using an idea of Greither and Kurihara [2015, Section 1.2]; one may also refer to [Kataoka 2020, Section 4.3]. We will have to deal with a large matrix denoted by $M_s(\nu_1, \dots, \nu_s, \tau_1, \dots, \tau_s)$, but it is not surprising; in a relevant study Greither, Kurihara and Tokio [Greither et al. 2020] dealt with an even more complicated matrix.

For each $1 \leq l \leq s$, we have a homological complex

$$C^l : \cdots \xrightarrow{\tau_l} \mathbb{Z}[I_l] \xrightarrow{\nu_l} \mathbb{Z}[I_l] \xrightarrow{\tau_l} \mathbb{Z}[I_l] \to 0$$

over $\mathbb{Z}[I_l]$, concentrated at degrees ≥ 0. Let C^l_n be the degree n component of C^l, so $C^l_n = \mathbb{Z}[I_l]$ if $n \geq 0$ and $C^l_n = 0$ otherwise. Then the homology groups are $H_n(C^l) = 0$ for $n \neq 0$ and $H_0(C^l) \simeq \mathbb{Z}$.

We define a complex C over $\mathbb{Z}[I]$ by

$$C = \bigotimes_{l=1}^{s} C^l,$$

which is the tensor product of complexes over $\mathbb{Z}$ (we do not specify the sign convention as it does not matter to us; we define it appropriately so that the descriptions of d_1 and d_2 below are valid). Explicitly, the degree n component C_n of C is defined as

$$C_n = \bigoplus_{n_1+\cdots+n_s=n} C^1_{n_1} \otimes \cdots \otimes C^s_{n_s}.$$

Clearly the tensor product is zero unless $n_1, \dots, n_s \geq 0$, and in that case

$$C^1_{n_1} \otimes \cdots \otimes C^s_{n_s} = \mathbb{Z}[I_1] \otimes \cdots \otimes \mathbb{Z}[I_s] \simeq \mathbb{Z}[I].$$

It is convenient to write $x_1^{n_1} \cdots x_s^{n_s}$ for the basis of $C^1_{n_1} \otimes \cdots \otimes C^s_{n_s}$ for each $n_1, \dots, n_s \geq 0$, following [Greither and Kurihara 2015]. Then, for each $n \geq 0$, the module C_n is a free module on the set of monomials of $x_1, \dots, x_s$ of degree n.

A basic property of tensor products of complexes implies that $H_n(C) = 0$ for $n \neq 0$ and $H_0(C) \simeq \mathbb{Z}$. Therefore, C is a free resolution of $\mathbb{Z}$ over $\mathbb{Z}[I]$.

It will be necessary to investigate some components of C of low degrees. Note that C_0 is free of rank one with a basis $1 (= x_1^0 \cdots x_s^0)$, C_1 is a free module on the set

$$S_1 = \{x_1, \dots, x_s\},$$

and C_2 is a free module on the set $S_2 \cup S_2'$ where

$$S_2 = \{x_1^2, \dots, x_s^2\}, \quad S_2' = \{x_l x_{l'} \mid 1 \leq l < l' \leq s\}.$$

Moreover, the differential $d_n : C_n \to C_{n-1}$ for $n = 1, 2$ are described as follows. We have

$$d_1(x_l) = \tau_l \cdot 1$$

for each $1 \leq l \leq s$,

$$d_2(x_l^2) = \nu_l x_l$$

for each $1 \leq l \leq s$, and

$$d_2(x_l x_{l'}) = \tau_l x_{l'} - \tau_{l'} x_l$$

for each $1 \leq l < l' \leq s$.

Let M denote the presentation matrix of d_2. For clarity, we define M formally as follows.

Definition 4.4. We define a matrix

$$M = M_s(\nu_1, \dots, \nu_s, \tau_1, \dots, \tau_s)$$

with the columns (resp. the rows) indexed by S_1 (resp. $S_2 \cup S_2'$), by

$$\begin{cases} \text{the } (x_l^2, x_l) \text{ component is } \nu_l & \text{for } 1 \leq l \leq s, \\ \text{the } (x_l x_{l'}, x_l) \text{ component is } -\tau_{l'} & \text{for } 1 \leq l < l' \leq s, \\ \text{the } (x_l x_{l'}, x_{l'}) \text{ component is } \tau_l & \text{for } 1 \leq l < l' \leq s, \\ \text{and the other components are zero.} \end{cases}$$

Here, we do not specify the orders of the sets S_1 and $S_2 \cup S_2'$. The ambiguity does not matter for our purpose.

For later use, we also define a matrix

$$N_s(\tau_1, \dots, \tau_s)$$

as the submatrix of M with the rows in S_2 removed. More precisely, we define the matrix $N_s(\tau_1, \dots, \tau_s)$ with the columns (resp. rows) indexed by S_1 (resp. S_2'), by

$$\begin{cases} \text{the } (x_l x_{l'}, x_l) \text{ component is } -\tau_{l'} & \text{for } 1 \leq l < l' \leq s, \\ \text{the } (x_l x_{l'}, x_{l'}) \text{ component is } \tau_l & \text{for } 1 \leq l < l' \leq s, \\ \text{and the other components are zero.} \end{cases}$$

Therefore, by choosing appropriate orders of rows and columns, we have:

$$M_s(\nu_1, \dots, \nu_s, \tau_1, \dots, \tau_s) = \begin{pmatrix} \nu_1 & & \\ & \ddots & \\ & & \nu_s \\ & N_s(\tau_1, \dots, \tau_s) & \end{pmatrix}$$

Example 4.5. When $s = 3$, we have:

$$M = \begin{pmatrix} \nu_1 & & \\ & \nu_2 & \\ & & \nu_3 \\ & -\tau_3 & \tau_2 \\ -\tau_3 & & \tau_1 \\ -\tau_2 & \tau_1 & \end{pmatrix}$$

Here, we use the order x_2x_3, x_1x_3, x_1x_2 for the set S_2'.

Proposition 4.6. *The matrix $M_s(\nu_1, \dots, \nu_s, \tau_1, \dots, \tau_s)$, over $\mathbb{Z}[G]$, is a presentation matrix of the module $\mathcal{I}_I$.*

Proof. By the construction, M is a presentation matrix of $\mathrm{Ker}(\mathbb{Z}[I] \to \mathbb{Z})$ over $\mathbb{Z}[I]$. Since $\mathbb{Z}[G]$ is flat over $\mathbb{Z}[I]$, we obtain the proposition by base change. □

Proposition 4.7. *For each $0 \leq i \leq s$, we have*

$$\mathrm{Fitt}_{i,\mathbb{Z}[G]}(M) = \sum_{j=0}^{s-i} \sum_{\substack{\boldsymbol{a} \subset \{1,2,\dots,s\} \\ \#\boldsymbol{a} = j}} \nu_{a_1} \cdots \nu_{a_j} \, \mathrm{Fitt}_{i,\mathbb{Z}[G]}(N_{s-j}(\tau_{a_{j+1}}, \dots, \tau_{a_s})).$$

Here, for each j, in the second summation $\boldsymbol{a}$ runs over subsets of $\{1, 2, \dots, s\}$ of j elements, and for each $\boldsymbol{a}$ we define $a_1, \dots, a_s$ by requiring

$$\boldsymbol{a} = \{a_1, \dots, a_j\}, \quad \{a_1, \dots, a_s\} = \{1, 2, \dots, s\}, \quad a_1 < \cdots < a_j, \quad a_{j+1} < \cdots < a_s.$$

The matrix $N_{s-j}(\tau_{a_{j+1}}, \dots, \tau_{a_s})$ is defined as in Definition 4.4 for $s - j$ and $\tau_{a_{j+1}}, \dots, \tau_{a_s}$ instead of s and $\tau_1, \dots, \tau_s$.

Proof. By the definition of higher Fitting ideals, $\mathrm{Fitt}_{i,\mathbb{Z}[G]}(M)$ is generated by $\det(H)$ for square submatrices H of M of size $s - i$. Such a matrix H is in one-to-one correspondence with choices of a subset

$A_H^{\text{column}} \subset S_1 = \{x_1, \dots, x_s\}$ with $\# A_H^{\text{column}} = s - i$ and a subset $A_H^{\text{row}} \subset S_2 \cup S_2' = \{x_1^2, \dots, x_s^2, x_1x_2, \dots, x_{s-1}x_s\}$ with $\# A_H^{\text{row}} = s - i$. We only have to deal with H satisfying $\det(H) \neq 0$.

For each H, we define j and $\boldsymbol{a}$ by

$$j = \#(A_H^{\text{row}} \cap S_2)$$

(so clearly $0 \leq j \leq s - i$) and

$$A_H^{\text{row}} \cap S_2 = \{x_{a_1}^2, \dots, x_{a_j}^2\}.$$

Recall that the x_l^2 row in the matrix M contains a unique nonzero component ν_l in the x_l column. Therefore, the assumption $\det(H) \neq 0$ forces $x_{a_1}, \dots, x_{a_j} \in A_H^{\text{column}}$ and

$$\det(H) = \pm \nu_{a_1} \cdots \nu_{a_j} \det(H'),$$

where H' is the square submatrix of H of size $(s - i) - j$, with rows in $A_{H'}^{\text{row}} = A_H^{\text{row}} \setminus \{x_{a_1}^2, \dots, x_{a_j}^2\} = A_H^{\text{row}} \cap S_2'$ and columns in $A_{H'}^{\text{column}} = A_H^{\text{column}} \setminus \{x_{a_1}, \dots, x_{a_j}\}$.

Let $N_{\boldsymbol{a}}$ denote the submatrix of $N_s(\tau_1, \dots, \tau_s)$ obtained by removing the $x_{a_1}, \dots, x_{a_j}$ columns. Then it is clear that the $\det(H')$ (for fixed j and $\boldsymbol{a}$) as above generate $\mathrm{Fitt}_{i,\mathbb{Z}[G]}(N_{\boldsymbol{a}})$. The argument so far implies

$$\mathrm{Fitt}_{i,\mathbb{Z}[G]}(M) = \sum_{j=0}^{s-i} \sum_{\substack{\boldsymbol{a} \subset \{1,2,\dots,s\} \\ \#\boldsymbol{a} = j}} \nu_{a_1} \cdots \nu_{a_j} \, \mathrm{Fitt}_{i,\mathbb{Z}[G]}(N_{\boldsymbol{a}}).$$

By the formula $\tau_l \nu_l = 0$, we may remove the components $\pm\tau_{a_1}, \dots, \pm\tau_{a_j}$ from the matrix $N_{\boldsymbol{a}}$ in the right hand side. It is easy to check that the resulting matrix is nothing but $N_{s-j}(\tau_{a_{j+1}}, \dots, \tau_{a_s})$ (with several zero rows added). This completes the proof. □

Proposition 4.8. *For $s \geq 0$ and $i \geq 0$, we have*

$$\mathrm{Fitt}_{i,\mathbb{Z}[G]}(N_s(\tau_1, \dots, \tau_s)) = \begin{cases} (1) & (i \geq s), \\ 0 & (s \geq 1, i = 0), \\ (\tau_1, \dots, \tau_s)^{s-i} & (1 \leq i < s). \end{cases}$$

Proof. Since $N_s(\tau_1, \dots, \tau_s)$ has s columns, the case for $i \geq s$ is clear.

We show the vanishing when $s \geq 1$ and $i = 0$. Let $R = \mathbb{Z}[T_1, \dots, T_s]$ be the polynomial ring over $\mathbb{Z}$. Then we have a ring homomorphism $f : R \to \mathbb{Z}[G]$ defined by sending T_l to τ_l. We define a matrix $N_s(T_1, \dots, T_s)$ over R in the same way as in Definition 4.4, with $\tau_\bullet$ replaced by $T_\bullet$. Then, by the base change via f, we have

$$\mathrm{Fitt}_{\mathbb{Z}[G]}(N_s(\tau_1, \dots, \tau_s)) = f(\mathrm{Fitt}_R(N_s(T_1, \dots, T_s)))\mathbb{Z}[G].$$

Hence the left hand side would vanish if we show that $\mathrm{Fitt}_R(N_s(T_1, \dots, T_s)) = 0$.

For each $1 \leq l \leq s$, we consider the complex

$$\widetilde{C}^l : 0 \to \mathbb{Z}[T_l] \xrightarrow{T_l} \mathbb{Z}[T_l] \to 0,$$

over $\mathbb{Z}[T_l]$, which satisfies $H_n(\widetilde{C}^l) = 0$ for $n \neq 0$ and $H_0(\widetilde{C}^l) \simeq \mathbb{Z}$. Similarly as previous, by taking the tensor product of the complexes $\widetilde{C}^l$ over $\mathbb{Z}$, we obtain an exact sequence

$$\cdots \to \widetilde{C}_2 \xrightarrow{N_s(T_1,\ldots,T_s)} \to \widetilde{C}_1 \xrightarrow{\begin{pmatrix} T_1 \\ \vdots \\ T_s \end{pmatrix}} \to \widetilde{C}_0 \to \mathbb{Z} \to 0$$

over R. (Alternatively, this exact sequence is obtained from the Koszul complex for the regular sequence $T_1, \ldots, T_s$.) This implies that $\mathrm{Fitt}_R(N_s(T_1, \ldots, T_s))$ is the Fitting ideal of the augmentation ideal of R. Since $s \geq 1$, the augmentation ideal of R is generically of rank one, so we obtain $\mathrm{Fitt}_R(N_s(T_1, \ldots, T_s)) = 0$, as desired.

Finally we show the case where $1 \leq i < s$. Since the components of the matrix $N_s(\tau_1, \ldots, \tau_s)$ are either 0 or one of $\tau_1, \ldots, \tau_s$, the inclusion $\subset$ is clear. In order to show the other inclusion, we use the induction on s.

For a while we fix an arbitrary $1 \leq l \leq s$. Then, by permuting the rows and columns, the matrix $N_s(\tau_1, \ldots, \tau_s)$ can be transformed into:

$$\begin{pmatrix} N_{s-1}(\tau_1, \ldots, \check{\tau}_l, \ldots, \tau_s) & & & & & \\ -\tau_l & & & & & \tau_1 \\ & -\tau_l & & & & \vdots \\ & & \ddots & & & \check{\tau}_l \\ & & & -\tau_l & & \vdots \\ & & & & -\tau_l & \tau_s \end{pmatrix}$$

(The symbol $(\check{-})$ means omitting that term.) Here, the x_l column is placed in the right-most, and the $x_1x_l, \ldots, x_{l-1}x_l, x_lx_{l+1}, \ldots, x_lx_s$ rows are placed in the lower. We also reversed the signs of some rows for readability as that does not matter at all.

This expression implies

$$\mathrm{Fitt}_{i,\mathbb{Z}[G]}(N_s(\tau_1, \ldots, \tau_s)) \supset (\tau_1, \ldots, \check{\tau}_l, \ldots, \tau_s)\, \mathrm{Fitt}_{i,\mathbb{Z}[G]}(N_{s-1}(\tau_1, \ldots, \check{\tau}_l, \ldots, \tau_s)).$$

By the induction hypothesis (note that $1 \leq i \leq s-1$), we have

$$\mathrm{Fitt}_{i,\mathbb{Z}[G]}(N_s(\tau_1, \ldots, \tau_s)) \supset (\tau_1, \ldots, \check{\tau}_l, \ldots, \tau_s)(\tau_1, \ldots, \check{\tau}_l, \ldots, \tau_s)^{s-1-i} = (\tau_1, \ldots, \check{\tau}_l, \ldots, \tau_s)^{s-i}.$$

Now we vary l and then obtain

$$\mathrm{Fitt}_{i,\mathbb{Z}[G]}(N_s(\tau_1, \ldots, \tau_s)) \supset \sum_{l=1}^{s} (\tau_1, \ldots, \check{\tau}_l, \ldots, \tau_s)^{s-i} = (\tau_1, \ldots, \tau_s)^{s-i},$$

where the last equality follows from $s - i < s$. This completes the proof of the proposition. □

Now we incorporate Propositions 4.6, 4.7 and 4.8 to prove the following.

Proposition 4.9. *For $0 \le i \le s$, we define an ideal J_i of $\mathbb{Z}[G]$ by*

$$J_i = \begin{cases} (\nu_1 \cdots \nu_s) = (\nu_I) & (i = 0), \\ \sum_{j=0}^{s-i} Z_{i+j}\mathcal{I}_I^j = Z_i + Z_{i+1}\mathcal{I}_I + \cdots + Z_s\mathcal{I}_I^{s-i} & (1 \le i \le s). \end{cases}$$

Then we have

$$\mathrm{Fitt}_{i,\mathbb{Z}[G]}(\mathcal{I}_I) = J_i.$$

Proof. By Propositions 4.6 and 4.7, we have

$$\begin{aligned} \mathrm{Fitt}_{i,\mathbb{Z}[G]}(\mathcal{I}_I) &= \mathrm{Fitt}_{i,\mathbb{Z}[G]}(M) \\ &= \sum_{j=0}^{s-i} \sum_{\substack{\boldsymbol{a} \subset \{1,2,\dots,s\} \\ \#\boldsymbol{a}=j}} \nu_{a_1} \cdots \nu_{a_j} \, \mathrm{Fitt}_{i,\mathbb{Z}[G]}(N_{s-j}(\tau_{a_{j+1}}, \dots, \tau_{a_s})). \end{aligned}$$

When $i = 0$, Proposition 4.8 implies

$$\mathrm{Fitt}_{0,\mathbb{Z}[G]}(N_{s-j}(\tau_{a_{j+1}}, \dots, \tau_{a_s})) = \begin{cases} (1) & (j = s), \\ 0 & (0 \le j < s). \end{cases}$$

Clearly, $j = s$ forces $\boldsymbol{a} = \{1, 2, \dots, s\}$, so we obtain

$$\mathrm{Fitt}_{0,\mathbb{Z}[G]}(\mathcal{I}_I) = (\nu_1 \cdots \nu_s) = J_0.$$

When $1 \le i \le s$, since $1 \le i \le s - j$ by the choice of j, Proposition 4.8 implies

$$\mathrm{Fitt}_{i,\mathbb{Z}[G]}(N_{s-j}(\tau_{a_{j+1}}, \dots, \tau_{a_s})) = (\tau_{a_{j+1}}, \dots, \tau_{a_s})^{s-i-j}.$$

Then we obtain

$$\mathrm{Fitt}_{i,\mathbb{Z}[G]}(\mathcal{I}_I) = \sum_{j=0}^{s-i} \sum_{\substack{\boldsymbol{a} \subset \{1,2,\dots,s\} \\ \#\boldsymbol{a}=j}} \nu_{a_1} \cdots \nu_{a_j} (\tau_{a_{j+1}}, \dots, \tau_{a_s})^{s-i-j}.$$

Using the relation $\nu_l \tau_l = 0$, for each $0 \le j \le s - i$, we have

$$\sum_{\substack{\boldsymbol{a} \subset \{1,2,\dots,s\} \\ \#\boldsymbol{a}=j}} \nu_{a_1} \cdots \nu_{a_j} (\tau_{a_{j+1}}, \dots, \tau_{a_s})^{s-i-j} = \sum_{\substack{\boldsymbol{a} \subset \{1,2,\dots,s\} \\ \#\boldsymbol{a}=j}} \nu_{a_1} \cdots \nu_{a_j} \mathcal{I}_I^{s-i-j} = Z_{s-j}\mathcal{I}_I^{s-i-j}.$$

These formulas imply $\mathrm{Fitt}_{i,\mathbb{Z}[G]}(\mathcal{I}_I) = J_i$. □

We are ready to prove Theorem 1.4.

Proof of Theorem 1.4. By Propositions 4.3 and 4.9, we have

$$\mathrm{Fitt}^{[1]}_{\mathbb{Z}[G]}(A) = \sum_{i=0}^{s} \tilde{g}^{i-1} J_i.$$

Then, noting $J_0 = (\nu_I)$, we can deduce

$$h\,\mathrm{Fitt}^{[1]}_{\mathbb{Z}[G]}(A) = \left(\nu_I, \left(1 - \frac{\nu_I}{\#I}\varphi^{-1}\right)\sum_{i=1}^{s}\tilde{g}^{i-1}J_i\right)$$

in the same way as in the proof of Proposition 4.1. Then it is enough to show

$$\mathcal{J} = \sum_{i=1}^{s}\tilde{g}^{i-1}J_i. \tag{4-1}$$

We claim that

$$(\mathcal{I}_I, \#I)J_{i+1} \subset J_i \tag{4-2}$$

holds for $1 \le i \le s-1$. We first see

$$\mathcal{I}_I J_{i+1} = \mathcal{I}_I \sum_{j=0}^{s-i-1} Z_{i+1+j}\mathcal{I}_I^j = \sum_{j=1}^{s-i} Z_{i+j}\mathcal{I}_I^j \subset J_i.$$

We also have $\nu_I J_{i+1} \subset (\nu_I) \subset J_0 \subset J_i$. Since $(\mathcal{I}_I, \#I) = (\mathcal{I}_I, \nu_I)$ as an ideal, these show the claim (4-2).

Using (4-2), we next show

$$\sum_{i=1}^{s}\tilde{g}^{i-1}J_i = \sum_{i=1}^{s}(1-\widetilde{\varphi}^{-1})^{i-1}J_i. \tag{4-3}$$

More generally we actually show

$$\sum_{i=1}^{s'}\tilde{g}^{i-1}J_i = \sum_{i=1}^{s'}(1-\widetilde{\varphi}^{-1})^{i-1}J_i$$

by induction on s', for each $0 \le s' \le s$. The case $s' = 0$ is trivial. For $1 \le s' \le s$, we have

$$\begin{aligned}\sum_{i=1}^{s'}\tilde{g}^{i-1}J_i &= \tilde{g}^{s'-1}J_{s'} + \sum_{i=1}^{s'-1}\tilde{g}^{i-1}J_i \\ &= \left(\sum_{i=1}^{s'}(1-\widetilde{\varphi}^{-1})^{i-1}(\#I)^{s'-i}\right)J_{s'} + \sum_{i=1}^{s'-1}(1-\widetilde{\varphi}^{-1})^{i-1}J_i.\end{aligned}$$

Here, the second equality follows from the induction hypothesis and expanding the power $\tilde{g}^{s'-1}$. By (4-2), for $1 \le i \le s'-1$, we have $(\#I)^{s'-i}J_{s'} \subset J_i$. Therefore, we obtain

$$\begin{aligned}\sum_{i=1}^{s'}\tilde{g}^{i-1}J_i &= (1-\widetilde{\varphi}^{-1})^{s'-1}J_{s'} + \sum_{i=1}^{s'-1}(1-\widetilde{\varphi}^{-1})^{i-1}J_i \\ &= \sum_{i=1}^{s'}(1-\widetilde{\varphi}^{-1})^{i-1}J_i.\end{aligned}$$

This completes the proof of (4-3).

The right hand side of (4-3) can be computed as

$$\begin{aligned}\sum_{i=1}^{s}(1-\widetilde{\varphi}^{-1})^{i-1}J_i &= \sum_{i=1}^{s}\sum_{j=0}^{s-i} Z_{i+j}\mathcal{I}_I^j(1-\widetilde{\varphi}^{-1})^{i-1}\\ &= \sum_{k=1}^{s}\sum_{j=0}^{k} Z_k\mathcal{I}_I^j(1-\widetilde{\varphi}^{-1})^{k-j-1}\\ &= \sum_{k=1}^{s} Z_k\mathcal{I}_D^{k-1} = \mathcal{J}.\end{aligned}$$

Here, the first equality follows from the definition of J_i, the second by putting $i+j=k$, the third by $\mathcal{I}_D = (\mathcal{I}_I, 1-\widetilde{\varphi}^{-1})$, and the final by the definition of $\mathcal{J}$. Then, combining this with (4-3), we obtain the formula (4-1). This completes the proof of Theorem 1.4. □

5. Stickelberger element and Fitting ideal

In this section, we prove Theorem 1.5. As explained after the statement, we need to compare the ideals in the both sides of (1-6) for each v before taking the product. That task will be done in Section 5A, and after that we complete the proof of Theorem 1.5 in Section 5B.

In this section we fix an odd prime number p and always work over $\mathbb{Z}_p$.

5A. ***Comparison of ideals.*** In this subsection, we again consider the general algebraic situation as in Section 1B. Our task in this subsection is to compare the two fractional ideals

$$\mathcal{A} = h\,\mathrm{Fitt}^{[1]}_{\mathbb{Z}_p[G]}(A\otimes\mathbb{Z}_p), \quad \mathcal{B} = \left(1-\frac{\nu_I}{\#I}\varphi^{-1}\right)$$

of $\mathbb{Z}_p[G]$. In Lemma 5.1 (resp. Lemma 5.2) below, we deal with the case where D *is not* (resp. *is*) a p-group. We will make use of the concrete description of $\mathcal{A}$ in Theorem 1.4. As we always work over $\mathbb{Z}_p$ instead of $\mathbb{Z}$, by abuse of notation, in this subsection we simply write $\mathcal{I}_I$, $\mathcal{I}_D$, Z_i, and $\mathcal{J}$ for the extensions of those ideals from $\mathbb{Z}[G]$ to $\mathbb{Z}_p[G]$. We have no afraid of confusion due to this.

Let G' denote the maximal subgroup of G whose order is prime to p.

Lemma 5.1. *Let χ be a faithful character of G' (note that this requires that G' be cyclic). Suppose that D is not a p-group. Then we have*

$$\mathcal{A}^{\chi} = \mathcal{B}^{\chi}$$

as fractional ideals of $\mathbb{Z}_p[G]^{\chi}$.

Proof. We write $D' = D\cap G'$ and $I' = I\cap G'$. We first note that $\mathcal{I}_D^{\chi} = (1)$. This is because χ is nontrivial on D' by the assumptions. Then we have $\mathcal{J}^{\chi} = (1)$ by Definition 1.2, so Theorem 1.4 implies

$$\mathcal{A}^{\chi} = \left(\nu_I, \left(1-\frac{\nu_I}{\#I}\varphi^{-1}\right)\right)^{\chi}.$$

We have to show

$$\nu_I^\chi \in \left(1 - \frac{\nu_I}{\#I}\varphi^{-1}\right)^\chi.$$

When I' is nontrivial, then $\nu_I^\chi = 0$ as χ is nontrivial on I', so this is obvious. Let us suppose that I' is trivial. Since $\nu_I^2 = (\#I)\nu_I$, we have

$$\nu_I\left(1 - \frac{\nu_I}{\#I}\varphi^{-1}\right) = \nu_I(1 - \varphi^{-1}).$$

The element $(1 - \widetilde{\varphi}^{-1})^\chi$ of $\mathbb{Z}_p[G]^\chi$ is a unit since $\mathcal{I}_D = (\mathcal{I}_I, 1 - \widetilde{\varphi}^{-1})$, $\mathcal{I}_D^\chi = (1)$, and $\mathcal{I}_I^\chi \subsetneqq (1)$. This completes the proof. □

Lemma 5.2. *Suppose that I is nontrivial and that D is a p-group. Let $s = \mathrm{rank}_p(I)$ be the p-rank of I, that is, the number of minimal generators of I (note that $s \geq 1$):*

(1) *We have*

$$\mathcal{A} \supset \mathcal{I}_D^{s-1}\mathcal{B}$$

as fractional ideals of $\mathbb{Z}_p[G]$.

(2) *Let ψ be a character of G such that $\psi|_{G'}$ is faithful on G' and that ψ is nontrivial on D. Then we have*

$$\psi(\mathcal{A}) = \psi(\mathcal{I}_D)^{s-1}\psi(\mathcal{B})$$

as ideals of $\mathcal{O}_\psi$.

Proof. We may take a decomposition (1-3) of I so that s coincides with the p-rank of I as the lemma, and then I_l is nontrivial for each $1 \leq l \leq s$:

(1) By Definition 1.2, we have $\mathcal{I}_D^{s-1} \subset \mathcal{J}$ (by the $i = s$ term as $Z_s = (1)$). Then Theorem 1.4 shows the claim (1).

(2) We first show $\psi(\mathcal{J}) = \psi(\mathcal{I}_D)^{s-1}$. By the claim (1) above, the inclusion $\psi(\mathcal{J}) \supset \psi(\mathcal{I}_D)^{s-1}$ holds. For each $1 \leq l \leq s$, we observe $(\psi(\nu_l)) \subset (p)$ since $\psi(\nu_l)$ is either 0 or $\#I_l$. Moreover, we have $(p) \subset \psi(\mathcal{I}_D)$ since ψ is nontrivial on D and we have $(p) \subset (1-\zeta)$ if ζ is any nontrivial root of unity. These observations imply $\psi(Z_i) \subset \psi(\mathcal{I}_D)^{s-i}$ for $1 \leq i \leq s$. By the definition of $\mathcal{J}$, we then have $\psi(\mathcal{J}) \subset \psi(\mathcal{I}_D)^{s-1}$ as claimed.

By Theorem 1.4 and the above claim, we have

$$\psi(\mathcal{A}) = (\psi(\nu_I), \psi(\mathcal{B})\psi(\mathcal{I}_D)^{s-1}).$$

We have to show $\psi(\nu_I) \in \psi(\mathcal{B})\psi(\mathcal{I}_D)^{s-1}$. This is obvious if ψ is nontrivial on I. If ψ is trivial on I, we have

$$\psi(\nu_I) = \#I \in (p^s) \subset \psi(\mathcal{B})\psi(\mathcal{I}_D)^{s-1},$$

where the last inclusion follows from $\psi(\mathcal{B}) = \psi(\mathcal{I}_D) = (1 - \psi(\varphi)^{-1}) \supset (p)$. This completes the proof of (2). □

5B. ***Proof of Theorem 1.5.*** Now we consider the setup in Section 1C. In particular, we fix an odd prime number p and an odd character χ of G'. Recall the χ-component of the Stickelberger element $\theta^{\chi}_{K/k,T}$ defined as (1-4)

Lemma 5.3. *We have $\theta^{\chi}_{K/k,T} \neq 0$ if and only if there exists a character ψ of G such that $\psi|_{G'} = \chi$ and that ψ is nontrivial on D_v for any $v \in S_\chi \setminus S_\infty(k)$.*

Proof. By (1-5) and the fact that ω^{χ}_{T} is a not a zero divisor, we have $\theta^{\chi}_{K/k,T} \neq 0$ if and only if there exists a character ψ of G such that $\psi|_{G'} = \chi$ and, for every $v \in S_\chi \setminus S_\infty(k)$, we have $\psi(1 - (\nu_{I_v}/\#I_v)\varphi_v^{-1}) \neq 0$. The last condition is equivalent to that ψ is nontrivial on D_v. This proves the lemma. □

We begin the proof of Theorem 1.5.

Proof of Theorem 1.5. As already remarked in the outline of the proof after Theorem 1.5, we may and do assume that χ is a faithful character of G'. This is because we have $(\mathrm{Cl}^T_K \otimes \mathbb{Z}_p) \otimes_{\mathbb{Z}_p[G]} \mathbb{Z}_p[\mathrm{Gal}(K_\chi/k)] \simeq \mathrm{Cl}^T_{K_\chi} \otimes \mathbb{Z}_p$ as the degree of K/K_χ is prime to p. Moreover, to simplify the notation, we write $S = S_\chi = S_{\mathrm{ram}}(K/k)$ and $S_{\mathrm{fin}} = S \setminus S_\infty(k)$. Recall that, by Theorem 1.1, the condition (i) is equivalent to (1-6). As in Section 5A, for each $v \in S_{\mathrm{fin}}$, we consider the fractional ideals of $\mathbb{Z}_p[G]$

$$\mathcal{A}_v = h_v \,\mathrm{Fitt}^{[1]}_{\mathbb{Z}_p[G]}(A_v \otimes \mathbb{Z}_p), \quad \mathcal{B}_v = \left(1 - \frac{\nu_{I_v}}{\#I_v}\varphi_v^{-1}\right).$$

We first suppose (ii) and aim at showing (i). The case where $\theta^{\chi}_{K/k,T} = 0$ is trivial, so we assume that, for any $v \in S_{\mathrm{fin}}$, either (a) or (b) holds. Then we obtain $\mathcal{B}^{\chi}_v \subset \mathcal{A}^{\chi}_v$ for any $v \in S_{\mathrm{fin}}$, by applying Lemma 5.1 (resp. Lemma 5.2(1)) if (a) (resp. (b)) holds. Thus (1-6) holds.

We now prove that (i) implies (ii). Suppose that both (i) and the negation of (ii) hold. Since $\theta^{\chi}_{K/k,T} \neq 0$, we may take a character ψ as in Lemma 5.3. By applying ψ to (1-6), we obtain

$$\prod_{v \in S_{\mathrm{fin}}} \psi(\mathcal{B}_v) \subset \prod_{v \in S_{\mathrm{fin}}} \psi(\mathcal{A}_v).$$

On the other hand, by Lemmas 5.1 and 5.2(2), for each $v \in S_{\mathrm{fin}}$, we have $\psi(\mathcal{A}_v) \subset \psi(\mathcal{B}_v)$. Moreover, the inclusion is proper if and only if both the conditions (a) and (b) in (ii) are false. Therefore, by the hypothesis that (ii) fails, we obtain

$$\prod_{v \in S_{\mathrm{fin}}} \psi(\mathcal{A}_v) \subsetneqq \prod_{v \in S_{\mathrm{fin}}} \psi(\mathcal{B}_v).$$

Thus we get a contradiction. This completes the proof of Theorem 1.5. □

Acknowledgments

Both of the authors are sincerely grateful to Masato Kurihara for his continuous support during the research. They also thank Cornelius Greither for extremely encouraging comments. Kataoka is supported by JSPS KAKENHI Grant Number 19J00763.

References

[Burns et al. 2016] D. Burns, M. Kurihara, and T. Sano, "On zeta elements for $\mathbb{G}_m$", *Doc. Math.* **21** (2016), 555–626. MR Zbl

[Dasgupta and Kakde 2023] S. Dasgupta and M. Kakde, "On the Brumer–Stark conjecture", *Ann. of Math.* (2) **197**:1 (2023), 289–388. MR Zbl

[Greither 2007] C. Greither, "Determining Fitting ideals of minus class groups via the equivariant Tamagawa number conjecture", *Compos. Math.* **143**:6 (2007), 1399–1426. MR Zbl

[Greither and Kurihara 2008] C. Greither and M. Kurihara, "Stickelberger elements, Fitting ideals of class groups of CM-fields, and dualisation", *Math. Z.* **260**:4 (2008), 905–930. MR Zbl

[Greither and Kurihara 2015] C. Greither and M. Kurihara, "Tate sequences and Fitting ideals of Iwasawa modules", *Algebra i Analiz* **27**:6 (2015), 117–149. In Russian; translated in *St. Petersburg Math. J.* **27**:6 (2016), 941–965. MR Zbl

[Greither et al. 2020] C. Greither, M. Kurihara, and H. Tokio, "The second syzygy of the trivial G-module, and an equivariant main conjecture", pp. 317–349 in *Development of Iwasawa theory—the centennial of K. Iwasawa's birth*, edited by M. Kurihara et al., Adv. Stud. Pure Math. **86**, Math. Soc., Tokyo, 2020. MR Zbl

[Kataoka 2020] T. Kataoka, "Fitting invariants in equivariant Iwasawa theory", pp. 413–465 in *Development of Iwasawa theory—the centennial of K. Iwasawa's birth*, edited by M. Kurihara et al., Adv. Stud. Pure Math. **86**, Math. Soc., Tokyo, 2020. MR Zbl

[Kurihara 2003a] M. Kurihara, "Iwasawa theory and Fitting ideals", *J. Reine Angew. Math.* **561** (2003), 39–86. MR Zbl

[Kurihara 2003b] M. Kurihara, "On the structure of ideal class groups of CM-fields", *Doc. Math.* **Extra Vol.** (2003), 539–563. MR Zbl

[Kurihara 2021] M. Kurihara, "Notes on the dual of the ideal class groups of CM-fields", *J. Théor. Nombres Bordeaux* **33**:3, part 2 (2021), 971–996. MR

[Kurihara and Miura 2011] M. Kurihara and T. Miura, "Stickelberger ideals and Fitting ideals of class groups for abelian number fields", *Math. Ann.* **350**:3 (2011), 549–575. MR Zbl

[Nickel 2011] A. Nickel, "On the equivariant Tamagawa number conjecture in tame CM-extensions", *Math. Z.* **268**:1-2 (2011), 1–35. MR Zbl

[Northcott 1976] D. G. Northcott, *Finite free resolutions*, Cambridge Tracts in Mathematics **71**, Cambridge University Press, 1976. MR Zbl

[Ritter and Weiss 1996] J. Ritter and A. Weiss, "A Tate sequence for global units", *Compositio Math.* **102**:2 (1996), 147–178. MR Zbl

Communicated by Samit Dasgupta
Received 2021-12-13 Revised 2022-12-25 Accepted 2023-02-13

mahiro.atsuta@gm.tsuda.ac.jp *Institute for Mathematics and Computer Science, Tsuda University, Tokyo, Japan*

tkataoka@rs.tus.ac.jp *Department of Mathematics, Faculty of Science Division II, Tokyo University of Science, Tokyo, Japan*

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2023 is US $485/year for the electronic version, and $705/year (+$65, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY
mathematical sciences publishers
nonprofit scientific publishing
http://msp.org/

Algebra & Number Theory

Volume 17 No. 11 2023