

ON THE GALOIS MODULE STRUCTURE OF MINUS CLASS GROUPS

CORNELIUS GREITHER AND TAKENORI KATAOKA

ABSTRACT. The main object of this paper is the minus class groups associated to CM-fields as Galois modules. In a previous article of the authors, we introduced a notion of equivalence for modules and determined the equivalence classes of the minus class groups. In this paper, we show a concrete application of this result. We also study how large a proportion of equivalence classes can be realized as classes of minus class groups.

1. INTRODUCTION

In some sense this paper is a continuation of a paper of the authors [5]. The setting is given by a CM-field L which is an abelian extension of a totally real field K , the Galois group being called G . Let $\mathbb{Z}[G]^- := \mathbb{Z}[1/2][G]/(1+j)$ be the minus part of the group ring, where j denotes complex conjugation. For any $\mathbb{Z}[G]$ -module M , the minus part M^- is defined as $M^- := \mathbb{Z}[G]^- \otimes_{\mathbb{Z}[G]} M$. We consider the minus part $\text{Cl}_L^{T,-}$ of the T -modified class group Cl_L^T (the technicalities will be explained in §2.4).

The question is, as in previous work: How much can we say about the structure of $\text{Cl}_L^{T,-}$ as a module over $\mathbb{Z}[G]^-$, based on equivariant L -values and field-theoretic information (ramification and the like) attached to L/K ? The Fitting ideal of the Pontryagin dual $\text{Cl}_L^{T,-,\vee}$ had been determined, more and more generally and unconditionally, by the first author [4], Kurihara [10], and Dasgupta–Kakde [3]. Somewhat unexpectedly the Fitting ideal of the non-dualized module $\text{Cl}_L^{T,-}$ was determined later, in the paper [1] by Atsuta and the second author. In particular, as a consequence of lengthy computations, we obtained an inclusion relation

$$\text{Fitt}(\text{Cl}_L^{T,-}) \subset \text{Fitt}(\text{Cl}_L^{T,-,\vee}).$$

In [5], we introduced a new notion of equivalence for the category \mathcal{C} of finite $\mathbb{Z}[G]^-$ -modules, denoted simply by \sim . Moreover, we described the equivalence class of $\text{Cl}_L^{T,-}$ (see §2). A guiding principle in defining \sim is to regard G -cohomologically trivial modules as zero. From the view point of Fitting ideals, this implies that \sim ignores the contribution of invertible ideals. Therefore, the analytic factor coming from L -functions, which was present in the earlier descriptions of the Fitting ideal, is lost. Nevertheless, the notion \sim is useful enough. For instance, as a first application of the theory, we have reproved the aforementioned inclusion relation.

This paper deals with two problems concerning the structure of $\text{Cl}_L^{T,-}$ from the viewpoint of \sim . The first one is to obtain a more concrete application of the notion of \sim . The second

2020 *Mathematics Subject Classification.* 11R29 (Primary) 11R33 (Secondary).

Key words and phrases. Class groups, integral representations, lattices, syzygies.

is to obtain some idea how large a proportion of equivalence classes is realized via classes of class groups. It turns out that this proportion tends to be remarkably small. In §1.1 and §1.2 respectively, we will briefly explain these results.

1.1. A concrete application of the equivalence. It is our purpose here to show that our description of $\text{Cl}_L^{T,-}$ up to \sim can actually lead to concrete predictions concerning the structure of $\text{Cl}_L^{T,-}$. Of course our predictions will fall short of determining the isomorphism class a priori – that would be way too ambitious.

Let $p \geq 3$ be a prime number. We consider the case where L^+/K is a p -extension, where as usual L^+ denotes the maximal totally real subfield of L . In this case, L/K has a unique intermediate field F such that F/K is a quadratic extension. Then F must be a CM-field satisfying $F^+ = K$.

The following is the main result here. Let $\text{ord}_p(-)$ be the additive p -adic valuation normalized by $\text{ord}_p(p) = 1$. In Lemma 2.5, we will see that the T -modification is unnecessary because of the second assumption.

Theorem 1.1. *Suppose the following:*

- L^+/K is a cyclic p -extension of degree p^r for some $r \geq 1$.
- L has no non-trivial p -th roots of unity.
- There is a unique prime v of K that is ramified in L^+/K and split in L/L^+ .
- v is totally ramified in L^+/K .
- $\text{ord}_p(\# \text{Cl}_F^-) = 0$.

Then $\text{ord}_p(\# \text{Cl}_L^-)$ is in the set

$$\{r, 2r, 3r, \dots, pr\} \cup \{pr + 1, pr + 2, pr + 3, \dots\}.$$

In other words, $\text{ord}_p(\# \text{Cl}_L^-)$ is nonzero and either divisible by r or larger than pr .

The proof will be given in §3. In §3.3, we will also check these predictions on some explicit examples. The results indicate that the theorem may be sharp.

1.2. Realization problem. The second topic in this paper is the question: Which finite $\mathbb{Z}[G]^-$ -modules can be equivalent to a class group $\text{Cl}_L^{T,-}$ a priori?

To be more precise, let us fix an abstract finite abelian group Γ . For simplicity, we assume that the order of Γ is odd. Let \mathcal{C} be the category of finite $\mathbb{Z}'[\Gamma]$ -modules, where we put $\mathbb{Z}' = \mathbb{Z}[1/2]$. In this setting we have the notion of equivalence \sim on \mathcal{C} . Let \mathcal{C}/\sim be the set of equivalence classes. It is known that \mathcal{C}/\sim can be regarded as a commutative monoid with respect to direct sums.

Let us consider various abelian CM-extensions L/K such that $\text{Gal}(L^+/K) \simeq \Gamma$. Since the order of Γ is odd, as in §1.1, there is a unique intermediate CM-field F satisfying $F^+ = K$ and $\text{Gal}(L/F) \simeq \Gamma$. Then we have an identification

$$\mathbb{Z}[\text{Gal}(L/K)]^- \simeq \mathbb{Z}'[\Gamma]$$

induced by the inclusion $\Gamma \subset \text{Gal}(L/K)$. Therefore, we may talk about the class of the minus class group $\text{Cl}_L^{T,-}$ in \mathcal{C}/\sim .

We call an element of \mathcal{C}/\sim a *realizable* class if it is the class of $\text{Cl}_L^{T,-}$ for some extension L/K described above (both L and K vary). Let $\mathcal{Z}^{\text{real}} \subset \mathcal{C}/\sim$ be the subset of realizable classes. Now the question is to study the size of $\mathcal{Z}^{\text{real}}$.

Our main results involve another subset \mathcal{Z}^{adm} of \mathcal{C}/\sim , whose elements we call *admissible* classes. The definition of \mathcal{Z}^{adm} will be given in §2.6. Here we only mention that \mathcal{Z}^{adm} is defined in an algebraic way (independent from arithmetic) so that we have $\mathcal{Z}^{\text{real}} \subset \mathcal{Z}^{\text{adm}}$. Also, \mathcal{Z}^{adm} is by definition a submonoid, while it is not clear whether so is $\mathcal{Z}^{\text{real}}$ a priori.

Now the problem splits naturally into two sub-problems:

- (a) Do we have $\mathcal{Z}^{\text{real}} = \mathcal{Z}^{\text{adm}}$?
- (b) What is the monoid structure of \mathcal{Z}^{adm} ?

Note that (a) is an arithmetic problem; to prove $\mathcal{Z}^{\text{real}} = \mathcal{Z}^{\text{adm}}$, we have to construct suitable extensions L/K . On the other hand, (b) is an algebraic problem.

As for (a), we will give the following affirmative answer, which will be proved in §4:

Theorem 1.2. *For any finite abelian group Γ whose order is odd, we have $\mathcal{Z}^{\text{real}} = \mathcal{Z}^{\text{adm}}$.*

In particular, $\mathcal{Z}^{\text{real}}$ is a submonoid of \mathcal{C}/\sim . Note that we will moreover have a concrete condition on the base field K to realize each admissible class. In particular, if Γ is a cyclic group, every admissible class is realized by $K = \mathbb{Q}$ (see Remark 4.4).

As for (b), we need to introduce a finite set \mathcal{T} , which depends only on the group structure of Γ . When Γ is a p -group, the set \mathcal{T} is identified with the set of pairs (I, D) such that

- $I \subset D \subset \Gamma$ are subgroups,
- I is non-trivial, and
- D/I is cyclic.

The general definition will be given in Definition 5.1. The main result for (b) is the following:

Theorem 1.3. *The following hold:*

- (1) *Suppose Γ is cyclic or is a p -group for some prime number p . Then \mathcal{Z}^{adm} is a free monoid of rank $\#\mathcal{T}$.*
- (2) *Otherwise, \mathcal{Z}^{adm} is not a free monoid.*

Let us focus on p -groups. As an immediate corollary of Theorems 1.2 and 1.3, we obtain the following:

Corollary 1.4. *Suppose that Γ is a p -group for some prime number p . Then the subset $\mathcal{Z}^{\text{real}}$ of \mathcal{C}/\sim is a commutative monoid that is free of rank $\#\mathcal{T}$.*

Here is a brief discussion on the relative size of $\mathcal{Z}^{\text{real}}$ within \mathcal{C}/\sim when Γ is a non-trivial p -group for some prime number p . Note that the structure of \mathcal{C}/\sim is already discussed in [5].

- If Γ is of order p , then both $\mathcal{Z}^{\text{real}}$ and \mathcal{C}/\sim are free of rank one. Indeed, we may even prove $\mathcal{Z}^{\text{real}} = \mathcal{C}/\sim$, that is, all finite Γ -modules up to equivalence occur as minus class groups (see Theorem 4.1).

- If Γ is cyclic of order p^2 , in [5] we have shown that \mathcal{C}/\sim is not a free monoid and the rank of the abelian group associated to \mathcal{C}/\sim is $4p - 2$. This results from the Heller–Reiner classification on the Γ -lattices, given in [2]. On the other hand, it is easy to see that $\#\mathcal{T} = 3$. Therefore, $\mathcal{Z}^{\text{real}}$ is much smaller than \mathcal{C}/\sim just as 3 is smaller than $4p - 2$.
- For any other Γ , the classification of Γ -lattices is a deep result (see Heller and Reiner [7], [8]). In particular, it is known that the rank of the abelian group associated to \mathcal{C}/\sim is infinite. On the other hand, $\#\mathcal{T}$ is of course always finite. Therefore, $\mathcal{Z}^{\text{real}}$ is again much smaller than \mathcal{C}/\sim .

So only a small portion of equivalence classes are realized as minus class groups. It is interesting to observe that the situation around plus components is totally in contrast (see Remark 2.14).

1.3. Organization of this paper. We begin by reviewing results from [5] in §2. We obtain a description of the equivalence classes of minus class groups, and then introduce the notion of realizable and admissible classes.

In §3, we prove Theorem 1.1 and check numerical examples. In §4, we prove Theorem 1.2. In §§5–6, we prove Theorem 1.3.

2. REVIEW OF THE EQUIVALENCE RELATION

We begin with a review of the notion of equivalence introduced by the authors [5].

In §§2.1–2.3, we recall the equivalence relation \sim , the re-interpretation of \sim in terms of lattices, and the notion of shift. The theory of shifts is basically known from work of the second author [9], but we add a new aspect, linking it with Heller’s loop operator for lattices.

After fixing the arithmetic setup in §2.4, we obtain the description of the equivalence class of minus class groups in §2.5. In §2.6, we introduce the notion of realizable classes and admissible classes.

2.1. The equivalence relation. Let R be a commutative ring that is Gorenstein of Krull dimension one. Typical examples include finite group rings such as $\mathbb{Z}[G]^-$ and $\mathbb{Z}'[\Gamma]$, where

- G is a finite abelian group and $(-)^-$ is considered with respect to a fixed element $j \in G$ whose exact order is 2.
- Γ is a finite abelian group.

Note that in [5] we established the general theory for Gorenstein rings of finite Krull dimension, but in this paper we only need dimension one cases.

Let \mathcal{C} be the category of finitely generated torsion R -modules. Let us write \mathcal{P} for the subcategory of \mathcal{C} that consists of modules whose projective dimensions over R are at most one. Note that when $R = \mathbb{Z}[G]^-$ or $R = \mathbb{Z}'[\Gamma]$ as above, \mathcal{C} consists of all finite R -modules and \mathcal{P} consists of all finite R -modules that are G -c.t. or Γ -c.t., respectively (“c.t.” is an abbreviation of “cohomologically trivial”).

Definition 2.1. We define a relation \sim on \mathcal{C} as follows:

- (a) A *sandwich* is a module M in \mathcal{C} with a three-step filtration by submodules $0 \subset M' \subset M'' \subset M$ satisfying the following conditions:
- The top quotient M/M'' and the bottom quotient $M'/0 = M'$ are both in \mathcal{P} .
 - The middle filtration quotient M''/M' is in \mathcal{C} .
- The middle filtration quotient M''/M' is called the *filling* of the sandwich.
- (b) Two modules X and Y in \mathcal{C} are *equivalent* ($X \sim Y$), if X is the filling of some sandwich M , Y is the filling of some other sandwich N , and M and N are isomorphic as R -modules. The isomorphism between M and N is not assumed to respect the filtrations.

For basic properties of this notion and in particular the nontrivial fact that this is an equivalence relation we refer to [5, Remark 2.4, Propositions 2.5–2.6]. For now let us just remark that one easily shows: $M \sim 0$ is equivalent to $M \in \mathcal{P}$. Indeed, the definition of \sim arose from the idea of forcing that property.

The set of equivalence classes \mathcal{C}/\sim is equipped with a commutative monoid structure with respect to direct sums. In the following, \mathcal{C}/\sim will always be studied as a commutative monoid. For each module M in \mathcal{C} , we write $[M]$ for the equivalence class of M in \mathcal{C}/\sim .

2.2. The equivalence classes via lattices. In [5, §4], we established an interpretation of the equivalence relation \sim via lattices. Let us briefly review the results here.

Let Lat^{pe} denote the commutative monoid of R -lattices up to projective equivalence. Here, an R -lattice (which we sometimes simply call a lattice) is by definition a finitely generated torsion-free R -module. Two R -lattices are projectively equivalent if they become isomorphic after adding finitely generated projective R -modules. We write

$$\mathcal{L} \sim_{\text{pe}} \mathcal{L}'$$

if \mathcal{L} and \mathcal{L}' are projectively equivalent lattices. The monoid structure of Lat^{pe} is defined by direct sums.

Definition 2.2. We define an injective monoid homomorphism

$$\Phi : \mathcal{C}/\sim \hookrightarrow \text{Lat}^{\text{pe}}$$

as follows: To each $X \in \mathcal{C}$, choose an epimorphism $F \rightarrow X$ from a finitely generated projective R -module F to X and define a lattice \mathcal{L}_X as its kernel. Though \mathcal{L}_X depends on the choice of the epimorphism, it is proved in [5, Theorem 4.2] that this induces a well-defined map Φ that sends the class of X to the class of \mathcal{L}_X , and that moreover Φ is injective. The image of Φ is also discussed in [5, Lemma 4.3].

2.3. The shift operator. There are shift operators ω^n on the monoid \mathcal{C}/\sim , see [5, Definition 3.4] and following discussion. ($\omega^n(X)$ in this paper means $X[n]$ in [5].) Let us briefly define them.

Definition 2.3. For any $X \in \mathcal{C}$, taking a short exact sequence

$$0 \rightarrow Y \rightarrow P \rightarrow X \rightarrow 0,$$

where $P \in \mathcal{P}$, we define $\omega^1(X) \sim Y$. This ω^1 is indeed well-defined and an automorphism. We then define the general ω^n inductively by $\omega^{n+1} = \omega^1 \circ \omega^n$ for any integer n .

On the lattice side, we have the Heller operator Ω , which is an automorphism of Lat^{pe} . It works as follows: given a lattice \mathcal{L} , take an exact sequence $0 \rightarrow \mathcal{M} \rightarrow F \rightarrow \mathcal{L} \rightarrow 0$, again with F finitely generated projective over R . Then Ω sends the class of \mathcal{L} to the class of \mathcal{M} .

We can link our shift operator ω^1 and the Heller operator Ω . The relation is as simple as possible.

Lemma 2.4. *There is a commutative square as follows:*

$$\begin{array}{ccc} \mathcal{C}/\sim & \xrightarrow[\simeq]{\omega^1} & \mathcal{C}/\sim \\ \downarrow \Phi & & \downarrow \Phi \\ \text{Lat}^{\text{pe}} & \xrightarrow[\simeq]{\Omega} & \text{Lat}^{\text{pe}}. \end{array}$$

Proof. Take $X \in \mathcal{C}$ and an exact sequence $0 \rightarrow Y \rightarrow P \rightarrow X \rightarrow 0$ with $P \in \mathcal{P}$, so $Y \sim \omega^1(X)$. Take compatible projective resolutions so as to obtain a diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathcal{L}' & \longrightarrow & \mathcal{L} & \longrightarrow & \mathcal{L}'' \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & F' & \longrightarrow & F & \longrightarrow & F'' \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & Y & \longrightarrow & P & \longrightarrow & X \longrightarrow 0, \end{array}$$

in which the modules F', F, F'' are finitely generated projective and the upper (lower) vertical arrows are injections (surjections respectively). Then \mathcal{L}' represents $\Phi(Y)$ and \mathcal{L}'' represents $\Phi(X)$. Moreover, \mathcal{L} is projective over R since $P \in \mathcal{P}$ and F is projective. Therefore we also have that \mathcal{L}' represents $\Omega(\mathcal{L}'')$. These observations imply that both $\Phi(\omega^1(X))$ and $\Omega(\Phi(X))$ are represented by \mathcal{L}' , so the lemma follows. \square

2.4. The arithmetic setup. We review the setting, which will be in force throughout the paper. Assume that L is a CM-field which is an abelian extension of a totally real field K . Write G for $\text{Gal}(L/K)$. Note that G must have even order; it contains a privileged element j of order 2 given by complex conjugation.

We also have to discuss T -modification, in order to make the results from [1] applicable. Let T be any finite set of prime ideals of K not containing any ramified prime. Let T_L denote the set of primes of L that lie above primes in T .

An ideal J of L is called T -principal, if it admits a generator $x \in L_T^\times$, where the latter group is defined as

$$L_T^\times = \{x \in L^\times \mid \text{ord}_{\mathfrak{P}}(x - 1) > 0, \forall \mathfrak{P} \in T_L\}.$$

The T -modified class group Cl_L^T is then defined as the group of all fractional ideals of L having support disjoint from T , modulo the subgroup of T -principal ideals. This is a slight enlargement of the usual class group Cl_L . More precisely, there is a canonical surjection $\text{Cl}_L^T \rightarrow \text{Cl}_L$, and its kernel is an epimorphic image of $\bigoplus_{\mathfrak{P} \in T_L} \kappa(\mathfrak{P})^\times$, where $\kappa(\mathfrak{P})$ denotes the residue field at \mathfrak{P} .

The requirement for T in [1] and many other papers is the following: In addition to the conditions already stated, T must be such that L_T^\times is \mathbb{Z} -torsion-free. In other words, we must have $\mu(L) \cap L_T^\times = \{1\}$, where $\mu(L)$ denotes the group of roots of unity in L . Trivially this implies that T cannot be empty. However, the following lemma implies that in certain cases this modification does not matter. Let ${}_p\text{Cl}_L$ and ${}_p\text{Cl}_L^T$ be the p -Sylow subgroups of Cl_L and Cl_L^T , respectively.

Lemma 2.5. *If L has no non-trivial p -th roots of unity, there is a legitimate choice of T such that ${}_p\text{Cl}_L^T \simeq {}_p\text{Cl}_L$.*

Proof. Let f be the order of $\mu(L)$, which is prime to p by the assumption. By Tchebotarev's density theorem, one can find a prime \mathfrak{P} of L such that the order of $\kappa(\mathfrak{P})^\times$ is divisible by f but not by p . Set $T = \{\mathfrak{p}\}$ with $\mathfrak{p} = \mathfrak{P} \cap K$. Then we have $\mu(L) \cap L_T^\times = \{1\}$ since $f \mid \#(\kappa(\mathfrak{P})^\times)$. On the other hand, the order of $\kappa(\mathfrak{P})^\times$ is prime to p , so in the p -part there is no difference between Cl_L^T and Cl_L . \square

2.5. The equivalence classes of class groups. When one takes [1] and [5] together, one sees that using the notions of equivalence and of shifting one can say a lot on $\text{Cl}_L^{T,-}$.

We need a little more notation. Let v run through the finite primes of K ramifying in L . For each such v , let $I_v \subset G$ be the inertia group and $\varphi_v \in G/I_v$ the Frobenius at v . Define

$$g_v = 1 - \varphi_v^{-1} + \#I_v \in \mathbb{Z}[G/I_v]; \quad A_v = \mathbb{Z}[G/I_v]/(g_v),$$

where $\#I_v$ denotes the order of I_v .

We will work over the ring $\mathbb{Z}[G]^-$ and define \mathcal{C} and \mathcal{P} accordingly. Then [1, Proposition 3.6] shows the existence of a short exact sequence of $\mathbb{Z}[G]^-$ -modules

$$0 \rightarrow \text{Cl}_L^{T,-} \rightarrow P \rightarrow \bigoplus_v A_v^- \rightarrow 0,$$

where P is a G -c.t. module (i.e., in \mathcal{P}). Given the good behaviour of shift under equivalence, this gives the following basic result:

Theorem 2.6. *With all the notation introduced so far, we have*

$$\text{Cl}_L^{T,-} \sim \bigoplus_v \omega^1(A_v^-),$$

where v runs over the finite primes of K that are ramified in L .

Note that the right hand side does not depend on the set T , and that the variance under T is hidden in the equivariant L -value, which is not a part of the statement here. Nevertheless, to keep things technically correct, one has to leave T in at least formally.

Lemma 2.7. *If v is ramified or inert in L/L^+ , then A_v^- is in \mathcal{P} .*

Proof. It is enough to show that $\mathbb{Z}_p \otimes A_v^- = \mathbb{Z}_p[G/I_v]^-/(g_v)$ is G -c.t. for any odd prime p . First suppose that v is ramified in L/L^+ , that is, $j \in I_v$. Then j acts as $+1$ on $\mathbb{Z}_p[G/I_v]$, so the minus part $\mathbb{Z}_p[G/I_v]^-$ is already trivial. Second suppose that $p \nmid \#I_v$. In this case, $\mathbb{Z}_p[G/I_v]$ is G -c.t., so its quotient $\mathbb{Z}_p[G/I_v]^-/(g_v)$ is also G -c.t.

Finally, suppose v is inert in L/L^+ and $p \mid \#I_v$. In this case, the restriction of j to G/I_v is a power of the Frobenius φ_v , that is, there is a positive integer m such that $j = \varphi_v^m$. Then

$$(1 + \#I_v)^m - (\varphi_v^{-1})^m = (1 + \#I_v)^m - j$$

is a multiple of g_v in $\mathbb{Z}[G/I_v]$. Since $p \mid \#I_v$ and $j = -1$ in the minus component, the displayed element is a p -adic unit in $\mathbb{Z}_p[G/I_v]^-$. Therefore, g_v is also a unit in $\mathbb{Z}_p[G/I_v]^-$, so we obtain $\mathbb{Z}_p[G/I_v]^-/(g_v) = 0$. \square

Definition 2.8. We define $S(L/K)$ as the set of finite primes of K that are ramified in L^+/K and split in L/L^+ .

Now Lemma 2.7 implies that Theorem 2.6 can be rephrased as follows:

Corollary 2.9. *We have*

$$\mathrm{Cl}_L^{T,-} \sim \bigoplus_{v \in S(L/K)} \omega^1(A_v^-).$$

2.6. Realizable classes and admissible classes. Let us fix a finite abelian group Γ whose order is odd. We study the category \mathcal{C} over $\mathbb{Z}'[\Gamma]$. As explained in the introduction, we define the set of realizable classes as follows:

Definition 2.10. We say that an element of \mathcal{C}/\sim is realizable if it is the class of $\mathrm{Cl}_L^{T,-}$ for some extension L/K such that $\mathrm{Gal}(L^+/K) \simeq \Gamma$, where we identify $\mathbb{Z}[\mathrm{Gal}(L/K)]^-$ with $\mathbb{Z}'[\Gamma]$. The set of realizable classes is denoted by $\mathcal{Z}^{\mathrm{real}} \subset \mathcal{C}/\sim$.

Next we define the submonoid of admissible classes. The motivation for the definition will be clear in Corollary 2.12.

Let us employ a useful term from group theory. Given a prime number p , a finite group is called *p-elementary* if it is the product of a p -group and a cyclic group. A finite group is called *elementary* if it is p -elementary for some prime number p .

Definition 2.11. (1) Associated to Γ , we define $\tilde{\mathcal{S}}$ as the set of pairs (I, φ) , where

- $I \subset \Gamma$ is a subgroup,
- I is non-trivial,
- I is an elementary group, and
- $\varphi \in \Gamma/I$ is an element.

(2) For each $(I, \varphi) \in \tilde{\mathcal{S}}$, we define a finite $\mathbb{Z}'[\Gamma]$ -module $A_{I,\varphi}$ by

$$A_{I,\varphi} := \mathbb{Z}'[\Gamma/I]/(1 - \varphi^{-1} + \#I).$$

(3) We define a submonoid $\mathcal{Z}^{\mathrm{adm}} \subset \mathcal{C}/\sim$ of admissible classes by

$$\mathcal{Z}^{\mathrm{adm}} = \langle [\omega^1(A_{I,\varphi})] \mid (I, \varphi) \in \tilde{\mathcal{S}} \rangle,$$

which is generated by $[\omega^1(A_{I,\varphi})]$ for various $(I, \varphi) \in \tilde{\mathcal{S}}$.

Corollary 2.12. *Let L/K be an extension such that $\mathrm{Gal}(L^+/K) \simeq \Gamma$. We identify $\mathbb{Z}'[\Gamma]$ and $\mathbb{Z}[\mathrm{Gal}(L/K)]^-$. Then we have*

$$\mathrm{Cl}_L^{T,-} \sim \bigoplus_{v \in S(L/K)} \omega^1(A_{I_v, \varphi_v}).$$

In particular, we have $\mathcal{Z}^{\text{real}} \subset \mathcal{Z}^{\text{adm}}$.

Proof. By local class field theory, for each prime $v \in S(L/K)$, the inertia group I_v is p -elementary for the prime number p lying below v . Therefore, we have $(I_v, \varphi_v) \in \tilde{\mathcal{S}}$ and also $A_v^- \simeq A_{I_v, \varphi_v}$. The corollary follows immediately from Corollary 2.9. \square

Now Theorems 1.2 and 1.3 are formulated, except for the general definition of \mathcal{T} .

Remark 2.13. The following observation will be used to prove Theorem 1.3. For any integer n , the monoid \mathcal{Z}^{adm} is isomorphic to the submonoid generated by $[\omega^n(A_{I, \varphi})]$ for various $(I, \varphi) \in \tilde{\mathcal{S}}$. This is because the shift automorphisms ω^{n-1} respect the monoid structure of \mathcal{C}/\sim .

Remark 2.14. The authors are grateful to Manabu Ozaki, who provided them with the following information.

Let p be an odd prime number. Let Γ be any finite p -group. Then, for any finite $\mathbb{Z}_p[\Gamma]$ -module M , there is a finite abelian extension L^+/K of totally real fields such that $\text{Gal}(L^+/K) \simeq \Gamma$ and $\mathbb{Z}_p \otimes_{\mathbb{Z}} \text{Cl}_{L^+}$ is isomorphic to M as Γ -modules.

This claim can be shown as follows. For the given Γ -module M , we consider the semi-direct product of $M \rtimes \Gamma$. It is a p -group, so we may apply the main theorem of Hajir–Maire–Ramakrishna [6]. As a consequence, there exists a totally real field K such that the Galois group of the maximal unramified (not necessarily abelian) p -extension over K is isomorphic to $M \rtimes \Gamma$. Then defining L^+ as the intermediate field corresponding to M , the requirement is satisfied.

3. CONCRETE APPLICATIONS

In this section, we prove Theorem 1.1. For this, in §3.1, we compute the lattice associated to the class group explicitly when the Galois group is cyclic. The general case is doable in principle, but it seems to be complicated. Then the proof of Theorem 1.1 will be given in §3.2. In §3.3, we will also observe numerical examples, which suggest that our theoretical result may be sharp. A direct generalization of Theorem 1.1 will be also provided.

3.1. Computation of the lattice. First we compute the lattice $\Phi(\omega^1(A_{I, \varphi}))$.

Theorem 3.1. *Let Γ be a cyclic group of odd order. Let $(I, \varphi) \in \tilde{\mathcal{S}}$, which simply means that $I \subset \Gamma$ is a subgroup and $\varphi \in \Gamma/I$ is an element. Take a lift $\tilde{\varphi} \in \Gamma$ of φ . We consider the module $A_{I, \varphi} = \mathbb{Z}'[\Gamma/I]/(1 - \varphi^{-1} + \#I)$ over $\mathbb{Z}'[\Gamma]$. Then we have*

$$\Phi(\omega^1(A_{I, \varphi})) \sim_{\text{pe}} (N_I, 1 - \tilde{\varphi}^{-1} + \#I),$$

where we define the norm element $N_I = \sum_{\sigma \in I} \sigma \in \mathbb{Z}[I]$ and the right hand side is the ideal of $\mathbb{Z}'[\Gamma]$ generated by the two elements inside the brackets.

Proof. By Lemma 2.4, we have $\Phi(\omega^1(A_{I, \varphi})) \sim_{\text{pe}} \Omega(\Phi(A_{I, \varphi}))$. Let τ be a generator of I . Put $\tilde{g} = 1 - \tilde{\varphi}^{-1} + \#I$. Then we have $\Phi(A_{I, \varphi}) \sim_{\text{pe}} (\tau - 1, \tilde{g})$, so we have to compute

$$\Phi(\omega^1(A_{I, \varphi})) \sim_{\text{pe}} \Omega((\tau - 1, \tilde{g})).$$

Put $R = \mathbb{Z}'[\Gamma]$. Let $\rho : R^2 \rightarrow (\tau - 1, \tilde{g})$ be the surjective homomorphism that sends the first basis element to $\tau - 1$ and the second to \tilde{g} . Then by definition $\Omega((\tau - 1, \tilde{g}))$ is projectively equivalent to $\text{Ker}(\rho)$.

We claim that $\text{Ker}(\rho)$ is generated by $(N_I, 0)$ and $(\tilde{g}, 1 - \tau)$. Indeed, $(N_I, 0), (\tilde{g}, 1 - \tau) \in \text{Ker}(\rho)$ is clear. Suppose that $(a, b) \in \text{Ker}(\rho)$, that is, $a(\tau - 1) = -b\tilde{g}$. Since \tilde{g} is a non-zero-divisor, b is annihilated by N_I , and so we can write $b = b_0(1 - \tau)$ for some $b_0 \in R$. Then $(a, b) - b_0(\tilde{g}, 1 - \tau)$ is another element in $\text{Ker}(\rho)$ whose second component is zero. The fact that $(a - b_0\tilde{g}, 0) \in \text{Ker}(\rho)$ easily gives that $a - b_0\tilde{g} \in (N_I)$. This shows the claim.

It is now easily checked that the first projection $R^2 \rightarrow R$ gives an isomorphism between $\text{Ker}(\rho)$ and (N_I, \tilde{g}) . This completes the proof. \square

By Corollary 2.12 and Theorem 3.1, we obtain the following:

Theorem 3.2. *In the situation of Corollary 2.12, if Γ is cyclic, then we have*

$$\Phi(\text{Cl}_L^{T,-}) \sim_{\text{pe}} \bigoplus_{v \in S(L/K)} (N_{I_v}, 1 - \widetilde{\varphi}_v^{-1} + \#I_v),$$

where $\widetilde{\varphi}_v$ is a lift of φ_v .

3.2. Proof of Theorem 1.1. Now we begin the proof of Theorem 1.1. As in §1.1, we consider the case where L^+/K is a cyclic p -extension, where p is an odd prime number. Let F be the unique quadratic extension of K in L . Let us write $R = \mathbb{Z}_p[G]^- \simeq \mathbb{Z}_p[\Gamma]$ and ${}_p\text{Cl}_L^- = \mathbb{Z}_p \otimes_{\mathbb{Z}} \text{Cl}_L^-$.

We begin with the following, which implies that ${}_p\text{Cl}_L^-$ is a cyclic R -module in the situation of Theorem 1.1.

Proposition 3.3. *Suppose that L^+/K is a cyclic p -extension and ${}_p\text{Cl}_F^- = 0$. Then the R -module ${}_p\text{Cl}_L^-$ is generated by $\#S(L/K)$ elements and annihilated by N_Γ .*

Proof. The last statement that N_Γ annihilates ${}_p\text{Cl}_L^-$ is a direct consequence of the assumption ${}_p\text{Cl}_F^- = 0$.

For the first statement we use genus theory. By Nakayama's lemma, it is enough to show that the Galois coinvariant module $({}_p\text{Cl}_L^-)_\Gamma$ is generated by $\#S(L/K)$ elements as a \mathbb{Z}_p -module. Let H be the extension of L that is a subfield of the Hilbert class field of L and the Artin map gives an isomorphism $\text{Gal}(H/L) \simeq {}_p\text{Cl}_L^-$. Then by Galois theory we find an intermediate field H' of H/L such that

$$\text{Gal}(H'/L) \simeq ({}_p\text{Cl}_L^-)_\Gamma.$$

Since Γ is cyclic, it is known that $\text{Gal}(H'/F)$ is the abelianization of $\text{Gal}(H/F)$, that is, H' is the maximal abelian extension of F in H .

Since H'/K is Galois, the Galois group $\text{Gal}(F/K)$ acts on $\text{Gal}(H'/F)$, so we have a decomposition

$$\text{Gal}(H'/F) = \text{Gal}(H'/F)^+ \times \text{Gal}(H'/F)^-$$

with respect to the action of the complex conjugation. By the construction, we have $\text{Gal}(H'/F)^+ \simeq \text{Gal}(L/F) \simeq \Gamma$ and $\text{Gal}(H'/F)^- \simeq \text{Gal}(H'/L) \simeq ({}_p\text{Cl}_L^-)_\Gamma$.

For any finite prime v of K , we define a subgroup $I_v \subset \text{Gal}(H'/F)$ as $I_v = \sum_{w|v} I_w$, where w denotes the (either one or two) primes of F lying above v and $I_w \subset \text{Gal}(H'/F)$ denotes the inertia group of w in H'/F . Then I_v is stable under the action of $\text{Gal}(F/K)$, so we also have a decomposition $I_v = I_v^+ \times I_v^-$. Note that I_v^+ is identified with the inertia group of v in $\text{Gal}(L^+/K) \simeq \Gamma$.

Since we assume ${}_p\text{Cl}_F^- = 0$, the group $\text{Gal}(H'/F)^-$ is generated by I_v^- for all finite primes v of K . Therefore, the proposition follows if we show that $I_v^- = 0$ unless $v \in S(L/K)$ and, moreover, I_v^- is cyclic when $v \in S(L/K)$. Since H'/L is unramified, for each prime w of F , the inertia group I_w in $\text{Gal}(H'/F)$ is isomorphic to the inertia group of w in $\text{Gal}(L/F) \simeq \Gamma$. This already shows $I_v^- = 0$ unless $v \in S(L/K)$; if v does not split in F/K , then $I_v = I_w \simeq I_v^+$, where w is the unique prime of F lying above v . If $v \in S(L/K)$, there are two primes w, w' of F lying above v . Both I_w and $I_{w'}$ are cyclic since Γ is cyclic, and moreover both are isomorphic to I_v^+ . Combining this with $I_v = I_w + I_{w'}$, we conclude that I_v^- is cyclic, as claimed. \square

From now on, let us assume the hypotheses of Theorem 1.1. By Proposition 3.3, we can write ${}_p\text{Cl}_L^- = R/J$ for a suitable ideal J . By Theorem 3.2, taking Lemma 2.5 into account, J is projectively equivalent, and even isomorphic, to (N_Γ, p^r) . Note that this lattice is non-free, so the case $r = 1$ follows at once. By Proposition 3.3, J must contain N_Γ .

Therefore, Theorem 1.1 follows from the following algebraic proposition:

Proposition 3.4. *Suppose that Γ is a cyclic group of order p^r with a prime $p \geq 3$ and $r \geq 2$. Let J be an ideal of $R = \mathbb{Z}_p[\Gamma]$ such that $(N_\Gamma) \subset J \subset R$ and $J \simeq (N_\Gamma, p^r)$. Then $\text{ord}_p(\#(R/J))$ is in $\{r, 2r, \dots, pr\} \cup \{pr+1, pr+2, \dots\}$.*

Proof. By the assumption, there is an element $w \in \mathbb{Q}_p[G]^\times$ such that $J = w(N_\Gamma, p^r)$. Then we have

$$(N_\Gamma) \subset w(N_\Gamma, p^r) \subset R.$$

Claim 3.5. *We have $w \in \frac{1}{p^r}R$ and $\text{aug}(w) \in \mathbb{Z}_p^\times$, where aug denotes the augmentation.*

Proof. The claim $w \in \frac{1}{p^r}R$ is clear. We have $wN_\Gamma = \text{aug}(w)N_\Gamma$, so $\text{aug}(w) \in \mathbb{Z}_p$ also follows. It remains to show $\text{aug}(w) \in \mathbb{Z}_p^\times$ by using $N_\Gamma \in w(N_\Gamma, p^r)$.

We have

$$w(N_\Gamma, p^r) = w(N_\Gamma, N_\Gamma - p^r) = (\text{aug}(w)N_\Gamma, w(N_\Gamma - p^r)),$$

so there are $x \in \mathbb{Z}_p$ and $y \in R$ such that

$$N_\Gamma = x \text{aug}(w)N_\Gamma + yw(N_\Gamma - p^r).$$

Since $N_\Gamma(N_\Gamma - p^r) = 0$, we have $y(N_\Gamma - p^r) = 0$, so this is simplified to

$$N_\Gamma = x \text{aug}(w)N_\Gamma.$$

This says $x \text{aug}(w) = 1$, so the claim follows. \square

Now we have

$$J = w(N_\Gamma, p^r) = (N_\Gamma, p^r w).$$

So

$$R/J \simeq \overline{R}/(\overline{p^r w}),$$

where we put $\overline{R} = R/(N_\Gamma)$.

We fix a generator σ of Γ . We also fix a compatible system (ζ_{p^i}) of p -power roots of unity, that is, ζ_{p^i} is a generator of the group μ_{p^i} of p^i -th roots of unity and we have $(\zeta_{p^i})^p = \zeta_{p^{i-1}}$. For each $1 \leq i \leq r$, let $\chi_i : \Gamma \rightarrow \mathbb{Z}_p[\mu_{p^i}]^\times$ be the character such that $\chi_i(\sigma) = \zeta_{p^i}$. We also write χ_i to mean the induced algebra homomorphism $R \rightarrow \mathbb{Z}_p[\mu_{p^i}]$. Then $(\chi_i)_{1 \leq i \leq r}$ gives an injective homomorphism

$$\overline{R} \hookrightarrow \prod_{i=1}^r \mathbb{Z}_p[\mu_{p^i}].$$

The cokernel is finite. Then by a standard argument, we obtain

$$\#(\overline{R}/(\overline{p^r w})) = \# \left(\prod_{i=1}^r \mathbb{Z}_p[\mu_{p^i}] / (\chi_i(p^r w)) \right).$$

It follows that

$$\begin{aligned} \text{ord}_p(\#(\overline{R}/(\overline{p^r w}))) &= \sum_{i=1}^r \text{ord}_p(\#\mathbb{Z}_p[\mu_{p^i}] / (\chi_i(p^r w))) \\ &= \sum_{i=1}^r \text{ord}_{\mathbb{Q}_p(\mu_{p^i})}(\chi_i(p^r w)), \end{aligned}$$

where $\text{ord}_{\mathbb{Q}_p(\mu_{p^i})}$ denotes the additive valuation on $\mathbb{Q}_p(\mu_{p^i})$, normalized so that we have $\text{ord}_{\mathbb{Q}_p(\mu_{p^i})}(\zeta_{p^i} - 1) = 1$.

Here is a quick summary: Put $c_i := \text{ord}_{\mathbb{Q}_p(\mu_{p^i})}(\chi_i(p^r w))$. Then we have

$$\text{ord}_p(\#(R/J)) = \sum_{i=1}^r c_i.$$

We have to investigate c_i . By Claim 3.5, we have $p^r w \in R$, so there exists an element $u \in R$ such that

$$p^r w - \text{aug}(p^r w) = (\sigma - 1)u.$$

Then we have

$$p^r w = (\sigma - 1)u + p^r \text{aug}(w)$$

and Claim 3.5 implies $\text{aug}(w) \in \mathbb{Z}_p^\times$.

Put $a_i := \text{ord}_{\mathbb{Q}_p(\mu_{p^i})}(\chi_i(u))$.

Claim 3.6. *If one of a_1, \dots, a_r is less than $p - 1$, then we have $a_1 = \dots = a_r$.*

Proof. For $2 \leq i \leq r$, since $\chi_i(\sigma)^p = \chi_{i-1}(\sigma)$, we have $\chi_i(u)^p \equiv \chi_{i-1}(u)$ modulo (p) . Therefore, one of the following holds:

- $\text{ord}_p(\chi_i(u)^p) = \text{ord}_p(\chi_{i-1}(u))$, that is, $a_i = a_{i-1}$.
- $\text{ord}_p(\chi_i(u)^p) \geq 1$ and $\text{ord}_p(\chi_{i-1}(u)) \geq 1$, that is, $a_i \geq p^{i-2}(p-1)$ and $a_{i-1} \geq p^{i-2}(p-1)$.

This observation implies the claim (the latter option cannot occur for any i by induction). \square

Now let us complete the proof of the proposition. We put

$$b_i := \text{ord}_{\mathbb{Q}_p(\mu_{p^i})}(\chi_i((\sigma - 1)u)) = 1 + a_i.$$

Case 1. Suppose one of a_1, \dots, a_r is less than $p - 1$. Then Claim 3.6 implies

$$a_1 = \dots = a_r \in \{0, 1, \dots, p - 2\},$$

so

$$b_1 = \dots = b_r \in \{1, 2, \dots, p - 1\}.$$

Then, since

$$\text{ord}_{\mathbb{Q}_p(\mu_{p^i})}(p^r \text{aug}(w)) = rp^{i-1}(p - 1) \geq r(p - 1) > p - 1 \geq b_i,$$

we obtain $c_i = b_i$ for $1 \leq i \leq r$. Therefore,

$$\sum_{i=1}^r c_i = rb_1 \in \{r, 2r, \dots, (p - 1)r\}.$$

Case 2. Suppose all of a_1, \dots, a_r are $\geq p - 1$. Then all of b_1, \dots, b_r are $\geq p$. As in Case 1, we have

$$\text{ord}_{\mathbb{Q}_p(\mu_{p^i})}(p^r \text{aug}(w)) \geq p,$$

so we deduce that all of c_1, \dots, c_r are $\geq p$. Therefore, we have

$$\sum_{i=1}^r c_i \geq pr.$$

This completes the proof of Proposition 3.4. □

This also finishes the proof of Theorem 1.1.

3.3. Numerical examples. For numerical examples we are forced to choose $K = \mathbb{Q}$, $p = 3$, and $r = 2$. We take the imaginary quadratic field F as one of

$$\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-5}), \mathbb{Q}(\sqrt{-6}).$$

(Note that $\mathbb{Q}(\sqrt{-3})$ is not allowed.) The class numbers of these are 1, 1, 2, 2 respectively, so they are prime to 3.

Also, we take L^+ as the unique subfield of $\mathbb{Q}(\mu_q)$ of degree 9 for some prime q that is congruent to 1 modulo 9. The prime q must split in F/\mathbb{Q} , which can be rephrased as a certain congruence condition of q (e.g., when $F = \mathbb{Q}(\sqrt{-1})$, then q is congruent to 1 modulo 4). We consider the primes q in the range $q < 3600$.

Our fields L will be the compositum of L^+ and F . The numerical result is that the 3-valuation of the class number of Cl_L^- takes values

$$2, 4, 6, 7, 8, 9, 10, 11.$$

This does not violate the prediction, of course, and also suggests that our prediction is sharp.

Remark 3.7. We even did more: even if we remove the condition that $S(L/K)$ consists of a single element (but all $v \in S(L/K)$ are totally ramified in L^+/K), a similar reasoning shows that $\text{ord}_p(\# \text{Cl}_L^-)$ is in the set

$$\{rn, r(n+1), \dots, r(n+p-1)\} \cup \{r(n+p-1)+1, r(n+p-1)+2, \dots\},$$

where we put $n = \#S(L/K)$. When $n = 1$, this recovers Theorem 1.1. We can of course check this generalized prediction for numerical examples. For instance, for $p = 3$, $r = 2$, and $n = 2$, the possibilities are 4, 6, 8, 9, 10, \dots . This theoretical result can be shown by suitably modifying Proposition 3.4; the details are omitted.

4. THE REALIZABILITY PROBLEM

In this section, we prove Theorem 1.2. Before that, in §4.1, we will illustrate the problem in the simplest non-trivial case, i.e., when Γ is the cyclic group whose order is an odd prime number p . The proof of Theorem 1.2 will be given in §4.2.

4.1. First case study. Let us show the following, which was stated in the introduction:

Theorem 4.1. *Let Γ be a cyclic group whose order is an odd prime number p and we work with the coefficient ring $\mathbb{Z}'[\Gamma]$. Then we have*

$$\mathcal{Z}^{\text{real}} = \mathcal{Z}^{\text{adm}} = \mathcal{C}/\sim,$$

that is, every equivalence class of finite Γ -modules are realized as the class of $\text{Cl}_L^{T,-}$ for some extension L/K with $\text{Gal}(L^+/K) \simeq \Gamma$. Moreover, we may restrict the base field K to be \mathbb{Q} .

Proof. Since Γ is a p -group, the monoid \mathcal{C}/\sim for $\mathbb{Z}'[\Gamma]$ can be identified with that for $\mathbb{Z}_p[\Gamma]$ (see Proposition 5.6). Therefore, we may work over $\mathbb{Z}_p[\Gamma]$ instead. By the interpretation via lattices as in §2.2, it is enough to examine

$$\Phi(\mathcal{Z}^{\text{real}}) = \Phi(\mathcal{C}/\sim)$$

considered in Lat^{pe} .

In [5, §5.1], we showed that \mathcal{C}/\sim is a free monoid of rank one. This corresponds to the well-known classification of $\mathbb{Z}_p[\Gamma]$ -lattices that every lattice with constant rank is up to a free summand a direct sum of copies of \mathcal{M} , where \mathcal{M} is the maximal order in $\mathbb{Q}_p[\Gamma]$. Therefore, the basis of $\Phi(\mathcal{C}/\sim)$ is the class of \mathcal{M} .

On the other hand, by Theorem 3.2, $\Phi(\mathcal{Z}^{\text{real}})$ consists of the classes of

$$\bigoplus_{v \in S(L/K)} (N_\Gamma, p),$$

where L/K varies. Here we used the observation that, for any $v \in S(L/K)$, we have $I_v = \Gamma$ and φ_v is trivial since Γ is a simple group. It is easy to see that $(N_\Gamma, p) = (N_\Gamma, p - N_\Gamma)$ is isomorphic to \mathcal{M} .

As a result, the theorem follows if we show that for any given integer $n \geq 0$, there is an abelian CM extension L/\mathbb{Q} with $\text{Gal}(L^+/\mathbb{Q}) \simeq \Gamma$ such that $\#S(L/\mathbb{Q}) = n$. This is a fairly easy exercise. When $n \geq 1$, take prime numbers q_1, \dots, q_n that are congruent to 1 modulo p , and take L^+ as a cyclic extension of \mathbb{Q} of order p in $\mathbb{Q}(\mu_{q_1}, \dots, \mu_{q_n})$ in which all q_1, \dots, q_n

are ramified. By taking an imaginary quadratic field F in which q_1, \dots, q_n are split, we find a desired field as $L = FL^+$. When $n = 0$, we only have to take F so that the primes are not split. \square

4.2. Proof of Theorem 1.2. Now we come back to general Γ . By the description in Corollary 2.12, we obtain Theorem 1.2 from the following:

Theorem 4.2. *Let Γ be an abstract finite abelian group whose order is odd. Suppose that we are given a family $(I_1, \varphi_1), \dots, (I_n, \varphi_n) \in \tilde{\mathcal{S}}$. Then there exist a totally real field K , a finite abelian CM-extension L/K , and a group isomorphism $\text{Gal}(L^+/K) \simeq \Gamma$ satisfying the following: We have $\#S(L/K) = n$ and we can label $S(L/K) = \{v_1, \dots, v_n\}$ so that the inertia group I_{v_i} corresponds to I_i and the Frobenius φ_{v_i} in Γ/I_{v_i} corresponds to φ_i .*

To prove this, we make use of the following, which results from global class field theory:

Theorem 4.3 (Grunwald–Wang theorem [11, (9.2.8)]). *Let K be a number field, G a finite abelian group, and S a finite set of primes of K . Suppose that for every $v \in S$ we are given a finite abelian extension L_v/K_v and an embedding $\text{Gal}(L_v/K_v) \hookrightarrow G$. Suppose that we are not in the special case (in the sense of [11, (9.1.5), (9.1.7)]). Then there exist a finite abelian extension L/K and an isomorphism $\text{Gal}(L/K) \simeq G$ that realizes the designated local extensions for $v \in S$.*

Proof of Theorem 4.2. Step 1. First, we construct a totally real field K and distinct primes v_i of K ($1 \leq i \leq n$). The required condition is mild: it is enough to choose them so that there is a surjective homomorphism

$$\mathcal{O}_{K_{v_i}}^\times \twoheadrightarrow I_i$$

for each $1 \leq i \leq n$, where $\mathcal{O}_{K_{v_i}}^\times$ denotes the local unit group. This is possible since, by the definition of $\tilde{\mathcal{S}}$, for each $1 \leq i \leq n$, there is a prime number p_i such that I_i is p_i -elementary. We may take v_i as a p_i -adic prime.

Step 2. We construct a finite abelian extension $L_{v_i}^+/K_{v_i}$ for each $1 \leq i \leq n$. Let $\tilde{\varphi}_i \in \Gamma$ be a lift of $\varphi_i \in \Gamma/I_i$ and let $D_i \subset \Gamma$ be the subgroup generated by I_i and $\tilde{\varphi}_i$. Let us choose a uniformizer of K_{v_i} , which gives an isomorphism $K_{v_i}^\times \simeq \mathcal{O}_{K_{v_i}}^\times \times \mathbb{Z}$. Then, combining the surjective homomorphism $\mathcal{O}_{K_{v_i}}^\times \twoheadrightarrow I_i$ in Step 1 with the map $\mathbb{Z} \rightarrow D_i$ that sends 1 to $\tilde{\varphi}_i$, we obtain a surjective homomorphism $K_{v_i}^\times \twoheadrightarrow D_i$. We define a finite abelian extension $L_{v_i}^+/K_{v_i}$ as the one corresponding to this $K_{v_i}^\times \twoheadrightarrow D_i$ via local class field theory. Then by construction, we have an isomorphism $\text{Gal}(L_{v_i}^+/K_{v_i}) \simeq D_i$ such that the inertia group corresponds to I_i and the Frobenius corresponds to φ_i .

Step 3. Now we apply the Grunwald–Wang theorem to construct a finite abelian extension L^+/K . We take $S = \{v_1, \dots, v_n\}$ and the local extension for each v_i is $L_{v_i}^+/K_{v_i}$ as in Step 2. Because the exponent of Γ is odd (so not divisible by 4), we are not in “the special case.” Therefore, by the Grunwald–Wang theorem, we can construct an abelian extension L^+/K and an isomorphism $\text{Gal}(L^+/K) \simeq \Gamma$ such that the localizations at v_1, \dots, v_n are as designated. Note that this L^+ is certainly totally real since the order of Γ is odd.

Step 4. We construct a quadratic CM-extension F/K so that the composite field $L = FL^+$ is an extension of K with the desired properties.

Let $S_{\text{ram}}(L^+/K)$ be the set of finite primes of K that are ramified in L^+ . We shall construct F satisfying the following:

- Each v_i is split in F/K for $1 \leq i \leq n$.
- Each $v \in S_{\text{ram}}(L^+/K) \setminus \{v_1, \dots, v_n\}$ does not split in F/K .

We can find such an F by again using the Grunwald–Wang theorem. The global Galois group is the cyclic group of order two, so we are not in “the special case.” The local extensions for $S_{\text{ram}}(L^+/K)$ are as described above. The local extensions for archimedean places are all \mathbb{C}/\mathbb{R} , so that F is a CM extension of K .

Here is a sketch of an alternative construction of F/K . Since it should be a Kummer extension, it is enough to find an element of K^\times whose square root generates F . The element should satisfy suitable congruent conditions at primes in $S_{\text{ram}}(L^+/K)$, 2-adic primes, and archimedean places. Then the existence follows from the approximation theorem.

Now, by the construction of F , if we set $L = FL^+$, we clearly have $S(L/K) = \{v_1, \dots, v_n\}$. The inertia group and the Frobenius at each v_i are (I_i, φ_i) as required, because of the construction of L^+ in Steps 2–3 (F does not affect them since v_i is split in F/K). This completes the proof of Theorem 4.2. \square

Remark 4.4. In the proof of Theorem 4.2, Step 1 tells us a recipe for the construction of the base field K . If Γ is cyclic, then each I_i is also cyclic, so we may take $K = \mathbb{Q}$, thanks to the theorem on arithmetic progressions (cf. Theorem 4.1). On the other hand, if Γ is not cyclic, we cannot take a uniform K that satisfies Theorem 4.2 for all families $\{(I_i, \varphi_i)\}_i$.

5. REPHRASING THE PROBLEM ON \mathcal{Z}^{adm}

In this section, we show Theorem 5.3, which describes the structure of \mathcal{Z}^{adm} . It will be a key step to prove Theorem 1.3.

5.1. The key theorem. Let Γ be a finite abelian group. In what follows we do not assume that the order of Γ is odd and work over $\mathbb{Z}[\Gamma]$ instead of $\mathbb{Z}'[\Gamma]$, which simply widens the scope of the argument. Let \mathcal{C}/\sim be the monoid associated to the ring $\mathbb{Z}[\Gamma]$. As in Definition 2.11, we re-define

$$A_{I,\varphi} := \mathbb{Z}[\Gamma/I]/(1 - \varphi^{-1} + \#I)$$

(so the former one is recovered by the base-change to \mathbb{Z}' from \mathbb{Z}), and then define the submonoid $\mathcal{Z}^{\text{adm}} \subset \mathcal{C}/\sim$ in the same way. We will study the structure of \mathcal{Z}^{adm} .

Definition 5.1. We define various sets as follows:

- (1) Let \mathcal{S} be the set of pairs (I, D) , where
 - $I \subset D \subset \Gamma$ are subgroups,
 - I is non-trivial,
 - I is an elementary group, and
 - D/I is cyclic.
- (2) For each prime p , we write Γ_p for the maximal p -quotient of Γ . Let \mathcal{S}_p be the set of pairs (I_p^*, D_p^*) such that $I_p^* \subset D_p^* \subset \Gamma_p$ are subgroups satisfying
 - I_p^* is non-trivial and

– D_p^*/I_p^* is cyclic.

In other words, \mathcal{S}_p is defined just as \mathcal{S} , for Γ_p instead of Γ . Note that $\mathcal{S}_p = \emptyset$ unless $p \mid \#\Gamma$.

- (3) Let \mathcal{T} be the set of tuples (p, H, I_p^*, D_p^*) such that
- p is a prime number (necessarily a prime divisor of $\#\Gamma$),
 - $H \subset \Gamma$ is a subgroup such that Γ/H is cyclic of order prime to p , and
 - $(I_p^*, D_p^*) \in \mathcal{S}_p$.

Definition 5.2. We define a monoid homomorphism

$$\beta : \mathbb{N}^{\mathcal{S}} \rightarrow \mathbb{N}^{\mathcal{T}}$$

by

$$\beta((I, D)) = \sum_{\substack{D \subset H \\ I_p = I_p^* \\ D_p = D_p^*}} (p, H, I_p^*, D_p^*)$$

for each $(I, D) \in \mathcal{S}$, where the sum runs over $(p, H, I_p^*, D_p^*) \in \mathcal{T}$ satisfying $D \subset H$, $I_p = I_p^*$, and $D_p = D_p^*$.

Now we can state the key theorem, whose proof will be given in the rest of this section.

Theorem 5.3. *The monoid \mathcal{Z}^{adm} is isomorphic to the image of $\beta : \mathbb{N}^{\mathcal{S}} \rightarrow \mathbb{N}^{\mathcal{T}}$.*

The image of β will be studied in §6, which results in Theorem 1.3. For now, let us consider the case where Γ is a p -group.

Corollary 5.4. *Suppose Γ is a p -group for some prime number p . Then \mathcal{Z}^{adm} is a free monoid of rank $\#\mathcal{S} = \#\mathcal{T}$.*

Proof. By identifying $\Gamma = \Gamma_p$, we have $\mathcal{S} = \mathcal{S}_p$. Moreover, we have $\mathcal{S} = \mathcal{T}$ by identifying (I, D) with (p, Γ, I, D) . The map β is then the identity map. As a consequence, we obtain the corollary. \square

Example 5.5. Suppose that Γ is cyclic of order p^r . Then the choice of I and D is

$$I = p^i \Gamma, \quad D = p^j \Gamma$$

with $0 \leq i \leq r-1$ and $0 \leq j \leq i$. Therefore, we have

$$\#\mathcal{S} = \sum_{i=0}^{r-1} (i+1) = \frac{1}{2}r(r+1).$$

5.2. Reduction to consideration over local rings. For each prime p , the ring $\mathbb{Z}_p[\Gamma]$ is decomposed as a product of local rings

$$\mathbb{Z}_p[\Gamma] \simeq \prod_{\chi} \mathcal{O}_{\chi}[\Gamma_p],$$

where χ runs over a set of representatives of the characters of Γ of order prime to p , modulo \mathbb{Q}_p -conjugacy. Here, recall that Γ_p denotes the maximal p -quotient of Γ . We will also write

I_p and D_p for the maximal p -quotient of I and D , respectively. Let $\mathcal{C}_{p,\chi}$ be the category of finite $\mathcal{O}_\chi[\Gamma_p]$ -modules.

For each (p, χ) , as we reviewed in §2.2, we have a monoid injective homomorphism

$$\Phi : (\mathcal{C}_{p,\chi})/\sim \hookrightarrow \text{Lat}_{\mathcal{O}_\chi[\Gamma_p]}^{\text{pe}}.$$

Moreover, [5, Theorem 5.2] implies that $\text{Lat}_{\mathcal{O}_\chi[\Gamma_p]}^{\text{pe}}$ is free on the set of indecomposable $\mathcal{O}_\chi[\Gamma_p]$ -lattices that are not projective (i.e., free). Note that this is true since $\mathcal{O}_\chi[\Gamma_p]$ is a henselian local ring, so the theorem of Krull–Remak–Schmidt–Azumaya holds.

Proposition 5.6. *The natural monoid homomorphism*

$$\mathcal{C}/\sim \rightarrow \bigoplus_{p,\chi} (\mathcal{C}_{p,\chi})/\sim$$

is an isomorphism.

Proof. For each $X \in \mathcal{C}$, since X is finite, $\mathbb{Z}_p \otimes_{\mathbb{Z}} X$ is identified with the p -Sylow subgroup of X and we have

$$X \simeq \bigoplus_p (\mathbb{Z}_p \otimes_{\mathbb{Z}} X).$$

Moreover, any $\mathbb{Z}_p[\Gamma]$ -module Y is a direct sum of its χ -components $Y_\chi := \mathcal{O}_\chi[\Gamma_p] \otimes_{\mathbb{Z}_p[\Gamma]} Y$. In addition, X is Γ -c.t. if and only if so are all its components. These observations imply the proposition. \square

For a prime number p , let us put

$${}_p A_{I,\varphi} = \mathbb{Z}_p \otimes_{\mathbb{Z}} A_{I,\varphi} = \mathbb{Z}_p[\Gamma/I]/(1 - \varphi^{-1} + \#I).$$

Now we are forced to study the relation among $({}_p A_{I,\varphi})_\chi$ (or equivalently among the associated lattices) for various $(I, \varphi) \in \tilde{\mathcal{S}}$.

5.3. Reduction to two propositions. For $(I, \varphi) \in \tilde{\mathcal{S}}$, define $D \subset \Gamma$ to be the subgroup generated by I and a lift of φ ; consequently, φ generates D/I . The proof of the following two propositions will be given later.

Proposition 5.7. *Let p be a prime number and χ a character of Γ whose order is prime to p . The following are equivalent:*

- (i) *We have $({}_p A_{I,\varphi})_\chi \sim 0$.*
- (ii) *I_p is trivial or χ is non-trivial on D .*

For $(I, \varphi) \in \tilde{\mathcal{S}}$, let us define $\mathcal{L}_{I,\varphi} \in \text{Lat}_{\mathbb{Z}[\Gamma]}^{\text{pe}}$ as the lattice associated to $\omega^{-1}(A_{I,\varphi}) \in \mathcal{C}/\sim$. The reason why we consider ω^{-1} (instead of ω^1) will be explained later.

Proposition 5.8. *Let (I, φ) and (I', φ') be two elements of $\tilde{\mathcal{S}}$. Let p be a prime number and χ a character of Γ whose order is prime to p . Suppose that $({}_p A_{I,\varphi})_\chi \not\sim 0$ and $({}_p A_{I',\varphi'})_\chi \not\sim 0$. Then the following are equivalent:*

- (i) $({}_p \mathcal{L}_{I,\varphi})_\chi \sim_{\text{pe}} ({}_p \mathcal{L}_{I',\varphi'})_\chi$.
- (ii) $({}_p \mathcal{L}_{I,\varphi})_\chi$ and $({}_p \mathcal{L}_{I',\varphi'})_\chi$ have a common (nonzero) direct summand in $\text{Lat}_{\mathcal{O}_\chi[\Gamma_p]}^{\text{pe}}$.

(iii) We have $I_p = I'_p$ and $D_p = D'_p$.

Let us prove Theorem 5.3, assuming these propositions.

Recall that \mathcal{Z}^{adm} is defined as the image of the homomorphism

$$\mathbb{N}^{\tilde{\mathcal{S}}} \rightarrow \mathcal{C}/\sim$$

that sends (I, φ) to $[\omega^1(A_{I, \varphi})]$. As noted in Remark 2.13, we may consider $\omega^{-1}(A_{I, \varphi})$ instead.

First, for each (p, χ) , let us consider the image of $\mathbb{N}^{\tilde{\mathcal{S}}} \rightarrow \text{Lat}_{\mathcal{O}_\chi[\Gamma_p]}^{\text{pe}}$ given by $(I, \varphi) \mapsto ({}_p\mathcal{L}_{I, \varphi})_\chi$. Thanks to Proposition 5.7 and Proposition 5.8 (i) \Leftrightarrow (ii), the image is a free monoid and its basis is the set

$$\{({}_p\mathcal{L}_{I, \varphi})_\chi \in \text{Lat}_{\mathcal{O}_\chi[\Gamma_p]}^{\text{pe}} \mid (I, \varphi) \in \tilde{\mathcal{S}}, I_p \text{ is non-trivial and } \chi \text{ is trivial on } D\}.$$

Here, projectively equivalent lattices are counted as the same. Moreover, by Proposition 5.8 (ii) \Leftrightarrow (iii), this set is in one-to-one correspondence with the set \mathcal{S}_p by $({}_p\mathcal{L}_{I, \varphi})_\chi \leftrightarrow (I_p, D_p)$. Consequently, we have a commutative diagram

$$\begin{array}{ccc} \mathbb{N}^{\tilde{\mathcal{S}}} & \xrightarrow{\quad} & \text{Lat}_{\mathcal{O}_\chi[\Gamma_p]}^{\text{pe}} \\ & \searrow \beta_{p, \chi} & \uparrow \\ & & \mathbb{N}^{\mathcal{S}_p}, \end{array}$$

where the map $\beta_{p, \chi}$ sends $(I, \varphi) \in \tilde{\mathcal{S}}$ to

$$\begin{cases} (I_p, D_p) \in \mathcal{S}_p & \text{(if } I_p \text{ is non-trivial and } \chi \text{ is trivial on } D) \\ 0 & \text{(otherwise).} \end{cases}$$

Now we vary p, χ . By the description of $\beta_{p, \chi}$, we obtain the following commutative diagram

$$\begin{array}{ccccc} \mathbb{N}^{\tilde{\mathcal{S}}} & \xrightarrow{(\beta_{p, \chi})} & \bigoplus_{(p, \chi)} \mathbb{N}^{\mathcal{S}_p} & \hookrightarrow & \bigoplus_{(p, \chi)} \text{Lat}_{\mathcal{O}_\chi[\Gamma_p]}^{\text{pe}} \\ \downarrow & & \uparrow & & \\ \mathbb{N}^{\mathcal{S}} & \xrightarrow{(\beta_{p, H})} & \bigoplus_{(p, H)} \mathbb{N}^{\mathcal{S}_p} & & \end{array}$$

The surjective homomorphism $\mathbb{N}^{\tilde{\mathcal{S}}} \rightarrow \mathbb{N}^{\mathcal{S}}$ is induced by the surjective map $\tilde{\mathcal{S}} \rightarrow \mathcal{S}$ that sends (I, φ) to (I, D) as before. The injective homomorphism $\bigoplus_{(p, H)} \mathbb{N}^{\mathcal{S}_p} \rightarrow \bigoplus_{(p, \chi)} \mathbb{N}^{\mathcal{S}_p}$ is the diagonal one that sends H -component to χ -components with $\text{Ker}(\chi) = H$. Finally, the map $\beta_{p, H} : \mathbb{N}^{\mathcal{S}} \rightarrow \bigoplus_{(p, H)} \mathbb{N}^{\mathcal{S}_p}$ sends (I, D) to

$$\begin{cases} (I_p, D_p) \in \mathcal{S}_p & \text{(if } I_p \text{ is non-trivial and } D \subset H) \\ 0 & \text{(otherwise).} \end{cases}$$

Then, identifying $\bigoplus_{(p, H)} \mathbb{N}^{\mathcal{S}_p}$ with $\mathbb{N}^{\mathcal{T}}$, we may identify the map $(\beta_{p, H})$ as β . Thus, we obtain Theorem 5.3, assuming Propositions 5.7 and 5.8.

5.4. Tate cohomology groups. In this subsection, we deduce Proposition 5.7 and a part of Proposition 5.8. As observed in [5, Lemma 6.1], the definition of \sim implies that equivalent modules in \mathcal{C} have isomorphic Tate cohomology groups. So our idea is to compute Tate cohomology groups for various subgroups H of Γ (now we consider an arbitrary subgroup H in contrast with Definition 5.1).

Lemma 5.9. *For any subgroup $H \subset \Gamma$, both $\hat{H}^0(H, A_{I,\varphi})$ and $\hat{H}^{-1}(H, A_{I,\varphi})$ are isomorphic to $\mathbb{Z}[\Gamma/(D+H)]/(\#(I \cap H))$ as $\mathbb{Z}[\Gamma/H]$ -modules.*

Proof. First let us show that

$$\hat{H}^i(H, \mathbb{Z}[\Gamma/I]) \simeq \begin{cases} \mathbb{Z}[\Gamma/(I+H)]/(\#(I \cap H)) & (i = 0) \\ 0 & (i = -1, 1). \end{cases}$$

For this, we observe that, for any $i \in \mathbb{Z}$,

$$\begin{aligned} \hat{H}^i(H, \mathbb{Z}[\Gamma/I]) &\simeq \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[I+H]} \hat{H}^i(H, \mathbb{Z}[(I+H)/I]) \\ &\simeq \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[I+H]} \hat{H}^i(H, \mathbb{Z}[H/(I \cap H)]) \\ &\simeq \mathbb{Z}[\Gamma] \otimes_{\mathbb{Z}[I+H]} \hat{H}^i(I \cap H, \mathbb{Z}) \end{aligned}$$

by using Shapiro's lemma. When $i = 1$, the claim follows from

$$H^1(I \cap H, \mathbb{Z}) = \text{Hom}(I \cap H, \mathbb{Z}) = 0.$$

To show the claim for $i = -1, 0$, we only have to observe that $H_0(I \cap H, \mathbb{Z}) = \mathbb{Z}$, $H^0(I \cap H, \mathbb{Z}) = \mathbb{Z}$, and the multiplication by $N_{I \cap H}$ coincides with the multiplication by $\#(I \cap H)$ on \mathbb{Z} .

By the definition of $A_{i,\varphi}$, we have an exact sequence

$$0 \rightarrow \mathbb{Z}[\Gamma/I] \xrightarrow{1-\varphi^{-1}+\#I} \mathbb{Z}[\Gamma/I] \rightarrow A_{I,\varphi} \rightarrow 0.$$

Then the lemma follows from the resulting long exact sequence. Here, we need to use that $\hat{H}^i(H, \mathbb{Z}[\Gamma/I])$ is annihilated by $\#I$. \square

Proof of Proposition 5.7. Suppose (ii) is false, i.e., I_p is non-trivial and χ is trivial on D . Then

$$\hat{H}^0(I, ({}_pA_{I,\varphi})_\chi) \simeq \mathbb{Z}_p[\Gamma/D]_\chi/(\#I_p)$$

is nonzero, so (i) is false.

Now suppose (ii) is true. If I_p is trivial, then $\mathbb{Z}_p[\Gamma/I]$ is Γ -c.t., so ${}_pA_{I,\varphi}$ is also Γ -c.t. If I_p is non-trivial and χ is non-trivial on D , then $({}_pA_{I,\varphi})_\chi = 0$. Therefore, (i) is true. \square

Proof of Proposition 5.8 (i) \Rightarrow (ii) and (i) \Rightarrow (iii). (i) \Rightarrow (ii) is clear. To show (i) \Rightarrow (iii), it is enough to show that the module structure of

$$\hat{H}^0(H, ({}_pA_{I,\varphi})_\chi) \simeq \mathbb{Z}_p[\Gamma/(D+H)]_\chi/(\#(I \cap H))$$

allows to recover the groups I_p and D_p . Here, I_p is non-trivial and χ is trivial on D .

For each p -subgroup H of Γ , the order $\#(I \cap H)$ is determined by the minimum positive integer that annihilates $\hat{H}^0(H, ({}_pA_{I,\varphi})_\chi)$. By varying H , we thus determine the subgroup I_p of Γ_p .

Then, by taking the p -Sylow subgroup of I as H , we know the module $\mathbb{Z}_p[\Gamma/D]_\chi/(\#I_p)$. Since I_p is non-trivial, this determines D_p . This is what we wanted. \square

We will prove (ii) \Rightarrow (i) and (iii) \Rightarrow (i) in the subsequent subsections.

5.5. The lattice associated to $\omega^{-1}(A_{I,\varphi})$. To do this, we obtain a concrete description of $\mathcal{L}_{I,\varphi}$, which was defined as the lattice associated to $\omega^{-1}(A_{I,\varphi})$. It is a key idea here that $\omega^{-1}(A_{I,\varphi})$ is much easier than $\omega^1(A_{I,\varphi})$, which we described in §3.1 only when the group is cyclic. We write $\nu_I = \sum_{\sigma \in I} \sigma \in \mathbb{Z}[I]$ for the norm element.

Proposition 5.10. *We have*

$$\mathcal{L}_{I,\varphi} \sim_{\text{pe}} \left(\nu_I, 1 - \frac{\nu_I}{\#I} \varphi^{-1} \right).$$

Proof. We use the computation in [1, §4A], which was used to determine $\text{Fitt}^{[-1]}(A_{I,\varphi})$. Let us mention here that the idea here comes from the fact that $\text{Fitt}^{[-1]}(A_{I,\varphi})$ is easier than $\text{Fitt}^{[1]}(A_{I,\varphi})$, which corresponds to $\text{Cl}_L^{T,-,\vee}$ versus $\text{Cl}_L^{T,-}$.

We have an exact sequence

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

Let $\tilde{\varphi} \in D$ be a lift of $\varphi \in D/I$. Put $\tilde{g} = 1 - \tilde{\varphi}^{-1} + \#I \in \mathbb{Z}[\Gamma]$, which is of course a lift of $g = 1 - \varphi^{-1} + \#I$. By the snake lemma, we obtain an exact sequence

$$0 \rightarrow A_{I,\varphi} \rightarrow \mathbb{Z}[\Gamma]/(\tilde{g}) \rightarrow \mathbb{Z}[\Gamma]/(\tilde{g}, \nu_I) \rightarrow 0.$$

This implies

$$\omega^{-1}(A_{I,\varphi}) \sim \mathbb{Z}[\Gamma]/(\tilde{g}, \nu_I).$$

Therefore, by the construction of Φ , we see that $\Phi(\omega^{-1}(A_{I,\varphi}))$ is the class of the lattice

$$(\tilde{g}, \nu_I) \subset \mathbb{Z}[\Gamma].$$

Let us modify this lattice by multiplying some non-zero-divisors of $\mathbb{Q}[\Gamma]$. First we have

$$\tilde{g}^{-1}(\tilde{g}, \nu_I) = (1, \nu_I g^{-1}).$$

Put $h := 1 - \frac{\nu_I}{\#I} \varphi^{-1} + \nu_I$. Then $\nu_I g = \nu_I h$, so

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

This completes the proof. \square

From now on, when we write $\mathcal{L}_{I,\varphi}$, it always means the representative described in this proposition. For each odd prime number p and a character χ of Γ of order prime to p , we have

$$({}_p \mathcal{L}_{I,\varphi})_\chi = \left(\nu_{I_p}, 1 - \frac{\nu_{I_p}}{\#I_p} \bar{\varphi}^{-1} \right)$$

as lattices of $\mathcal{O}_\chi[G_p]$, where $\bar{\varphi} \in G_p$ denotes the image of φ .

Proof of Proposition 5.8 (iii) \Rightarrow (i). It is enough to show that (iii) implies that $({}_p\mathcal{L}_{I,\varphi})_\chi$ and $({}_p\mathcal{L}_{I',\varphi'})_\chi$ are isomorphic. Since $\overline{\varphi}$ and $\overline{\varphi'}$ generate the same subgroup of G_p/I_p , the elements $(1 - \overline{\varphi}^{-1})$ and $(1 - \overline{\varphi'}^{-1})$ generate the same ideal of $\mathbb{Z}_p[G_p/I_p]$. It follows that there is a unit $u \in \mathbb{Z}_p[G_p/I_p]^\times$ such that

$$u(1 - \overline{\varphi}^{-1}) = (1 - \overline{\varphi'}^{-1}).$$

To ease the notation, let us put $e = \frac{\nu_{I_p}}{\#I_p}$. Then we have $(eu + (1 - e))({}_p\mathcal{L}_{I,\varphi})_\chi = ({}_p\mathcal{L}_{I',\varphi'})_\chi$. Indeed,

$$\begin{aligned} (eu + (1 - e))({}_p\mathcal{L}_{I,\varphi})_\chi &= \left((eu + (1 - e))\nu_{I_p}, (eu + (1 - e))(1 - e\overline{\varphi}^{-1}) \right) \\ &= \left(eu\nu_{I_p}, eu(1 - \overline{\varphi}^{-1}) + (1 - e) \right) \\ &= \left(\nu_{I_p}, 1 - e\overline{\varphi'}^{-1} \right) \\ &= ({}_p\mathcal{L}_{I',\varphi'})_\chi. \end{aligned}$$

Thus we have proved Proposition 5.8 (iii) \Rightarrow (i). \square

Remark 5.11. In fact, we have a more natural proof of Proposition 5.8 (i) \Leftrightarrow (iii). Let us sketch it. By Proposition 5.12 below, the lattice ${}_p\mathcal{L}_{I,\varphi}$ is an extension of $\mathbb{Z}_p[\Gamma]/(\nu_I)$ by $\mathbb{Z}_p[\Gamma/I]$. It is possible to directly compute its extension class; we have an isomorphism

$$\text{Ext}_{\mathbb{Z}_p[\Gamma]}^1(\mathbb{Z}_p[\Gamma]/(\nu_I), \mathbb{Z}_p[\Gamma/I]) \simeq \mathbb{Z}_p[\Gamma/I]/(\#I)$$

and the extension class corresponds to the class of $\varphi^{-1} - 1$. Therefore, condition (iii) in Proposition 5.8 claims that the extension classes are the same up to a unit, which indicates that the lattices are isomorphic.

5.6. Direct summands of $({}_p\mathcal{L}_{I,\varphi})_\chi$. Let us study the lattice $\mathcal{L}_{I,\varphi}$ described in Proposition 5.10, as a preparation for the missing equivalence of the proof of Proposition 5.8.

Proposition 5.12. *We have an exact sequence*

$$0 \rightarrow \mathbb{Z}[\Gamma/I] \xrightarrow{\nu_I} \mathcal{L}_{I,\varphi} \rightarrow \mathbb{Z}[\Gamma]/(\nu_I) \rightarrow 0.$$

Proof. Consider the natural exact sequence

$$0 \rightarrow \mathbb{Q}[\Gamma/I] \xrightarrow{\nu_I} \mathbb{Q}[\Gamma] \xrightarrow{\pi} \mathbb{Q}[\Gamma]/\nu_I\mathbb{Q}[\Gamma] \rightarrow 0.$$

Let us show that this induces the claimed exact sequence, by observing the image and the preimage of $\mathcal{L}_{I,\varphi}$.

Since $\pi(\nu_I) = 0$ and $\pi(1 - \frac{\nu_I}{\#I}\varphi^{-1}) = 1$, we see that $\pi(\mathcal{L}_{I,\varphi})$ is generated by 1 over $\mathbb{Z}[\Gamma]$. The natural homomorphism $\mathbb{Z}[\Gamma]/(\nu_I) \rightarrow \mathbb{Q}[\Gamma]/\nu_I\mathbb{Q}[\Gamma]$ is injective and its image is generated by 1 over $\mathbb{Z}[\Gamma]$. Therefore, the image of $\mathcal{L}_{I,\varphi}$ is $\mathbb{Z}[\Gamma]/(\nu_I)$, as claimed.

To determine the preimage, let $a \in \mathbb{Q}[\Gamma/I]$ be any element such that $\nu_I a \in \mathcal{L}_{I,\varphi}$. We want to show $a \in \mathbb{Z}[\Gamma/I]$. Let us take elements $b \in \mathbb{Z}[\Gamma/I]$ and $c \in \mathbb{Z}[\Gamma]$ such that $\nu_I a = \nu_I b + (1 - \frac{\nu_I}{\#I}\varphi^{-1})c$. Then $\nu_I(a - b) = (1 - \frac{\nu_I}{\#I}\varphi^{-1})c$. In particular, this equation implies $c \in \nu_I\mathbb{Q}[\Gamma]$, so

$$c \in \mathbb{Z}[\Gamma] \cap \nu_I\mathbb{Q}[\Gamma] = \nu_I\mathbb{Z}[\Gamma] = (\nu_I).$$

Then

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

This implies $\nu_I a \in (\nu_I)$, so $a \in \mathbb{Z}[\Gamma/I]$, as claimed. This completes the proof. \square

Proposition 5.13. *Let p be a prime number and χ a character of Γ of order prime to p . Then either $({}_p\mathcal{L}_{I,\varphi})_\chi$ is indecomposable over $\mathcal{O}_\chi[G_p]$, or the sequence*

$$0 \rightarrow \mathbb{Z}_p[G/I]_\chi \rightarrow ({}_p\mathcal{L}_{I,\varphi})_\chi \rightarrow (\mathbb{Z}_p[G]/(\nu_I))_\chi \rightarrow 0,$$

which is obtained by Proposition 5.12, splits.

Proof. Note that both $\mathbb{Z}_p[G/I]_\chi$ and $(\mathbb{Z}_p[G]/(\nu_I))_\chi$ are indecomposable unless zero, since they are cyclic modules over a local ring.

Suppose that there is a decomposition $({}_p\mathcal{L}_{I,\varphi})_\chi = M_1 \oplus M_2$ with nonzero M_1 and M_2 . Since $(\mathbb{Z}_p[G]/(\nu_I))_\chi$ is a cyclic module, by Nakayama's lemma, we may assume that the map $M_1 \rightarrow (\mathbb{Z}_p[G]/(\nu_I))_\chi$ is surjective.

We claim that the map $M_2 \rightarrow (\mathbb{Z}_p[G]/(\nu_I))_\chi$ is zero. For this, we may work after base-change from \mathbb{Z}_p to \mathbb{Q}_p so that everything is semi-simple. Then M_1 and M_2 have no common irreducible components as $M_1 \oplus M_2$ is (generically) free of rank one. Since there is a surjective map from M_1 to $(\mathbb{Z}_p[G]/(\nu_I))_\chi$, we see that $(\mathbb{Z}_p[G]/(\nu_I))_\chi$ and M_2 have no common irreducible components. This shows the claim.

Now by the displayed exact sequence, $\mathbb{Z}_p[G/I]_\chi$ is isomorphic to $\text{Ker}(M_1 \rightarrow (\mathbb{Z}_p[G]/(\nu_I))_\chi) \oplus M_2$. Therefore, $M_1 \rightarrow (\mathbb{Z}_p[G]/(\nu_I))_\chi$ is isomorphic, so the sequence splits. \square

Proof of Proposition 5.8 (ii) \Rightarrow (i). Suppose that $({}_p\mathcal{L}_{I,\varphi})_\chi$ and $({}_p\mathcal{L}_{I',\varphi'})_\chi$ have a common direct summand. We want to show that then these two lattices are indeed isomorphic. If one of them is indecomposable, then the claim is clear (notice that the \mathcal{O}_χ -ranks of $({}_p\mathcal{L}_{I,\varphi})_\chi$ and $({}_p\mathcal{L}_{I',\varphi'})_\chi$ are the same). Suppose that both are decomposable. By Proposition 5.13, we have

$$({}_p\mathcal{L}_{I,\varphi})_\chi \simeq \mathbb{Z}_p[G/I]_\chi \oplus (\mathbb{Z}_p[G]/(\nu_I))_\chi$$

and similarly for $({}_p\mathcal{L}_{I',\varphi'})_\chi$. The assumption implies that one of the following holds:

$$\begin{cases} \mathbb{Z}_p[G/I]_\chi \simeq \mathbb{Z}_p[G/I']_\chi \\ \mathbb{Z}_p[G/I]_\chi \simeq (\mathbb{Z}_p[G]/(\nu_{I'}))_\chi \\ (\mathbb{Z}_p[G]/(\nu_I))_\chi \simeq \mathbb{Z}_p[G/I']_\chi \\ (\mathbb{Z}_p[G]/(\nu_I))_\chi \simeq (\mathbb{Z}_p[G]/(\nu_{I'}))_\chi \end{cases}$$

Neither the second nor the third isomorphism can hold, because one side contains the trivial character component and the other does not. Therefore, the first or the fourth occurs, which implies $I_p = I'_p$ and the desired isomorphism of lattices follows. This completes the proof. \square

6. THE STRUCTURE OF \mathcal{Z}^{adm}

In this section, we prove Theorem 1.3 by using Theorem 5.3. Let Γ be a finite abelian group. The case where Γ is a p -group was done in Corollary 5.4. The case where Γ is cyclic will be done in §6.2, and the other cases will be in §6.3.

6.1. Useful observations. To study the image of β , the following is useful.

Lemma 6.1. *Let $(I, D) \in \mathcal{S}$ and we suppose D is cyclic. Then we have*

$$\beta((I, D)) = \sum_{p \mid \#I} \beta((I_{(p)}, D)),$$

where $I_{(p)}$ denotes the p -Sylow subgroup of I . Here we have $(I_{(p)}, D) \in \mathcal{S}$ thanks to the assumption that D is cyclic.

Proof. This can be checked directly from the definition of β . □

Corollary 6.2. *Define a subset $\mathcal{S}' \subset \mathcal{S}$ by*

$$\mathcal{S}' = \{(I, D) \in \mathcal{S} \mid \text{either } D \text{ is non-cyclic or } \#I \text{ is a prime-power}\}.$$

Then we have $\beta(\mathbb{N}^{\mathcal{S}'}) = \beta(\mathbb{N}^{\mathcal{S}})$.

Proof. For each $(I, D) \in \mathcal{S} \setminus \mathcal{S}'$, we have that D is cyclic (and $\#I$ is not a prime-power, but formally this property is unnecessary for now). For each $p \mid \#I$, defining $I_{(p)}$ as in Lemma 6.1, we have $(I_{(p)}, D) \in \mathcal{S}'$ since $\#I_{(p)}$ is a prime-power. Then Lemma 6.1 implies that $\beta((I, D)) \in \beta(\mathbb{N}^{\mathcal{S}'})$. □

According to this corollary, we only have to study the image of the homomorphism

$$\beta' = \beta|_{\mathbb{N}^{\mathcal{S}'}} : \mathbb{N}^{\mathcal{S}'} \rightarrow \mathbb{N}^{\mathcal{T}}.$$

Let us compare the cardinalities of \mathcal{S}' and \mathcal{T} .

Proposition 6.3. *We have $\#\mathcal{S}' \geq \#\mathcal{T}$ and the equality holds if and only if Γ is cyclic or $\#\Gamma$ is a prime-power.*

Proof. We define

$$\begin{aligned} \mathcal{S}'' &= \{(I, D) \in \mathcal{S} \mid \#I \text{ is a prime-power}\} \\ &= \coprod_{p \mid \#\Gamma} \{(I, D) \in \mathcal{S} \mid \#I \text{ is a } p\text{-power}\}. \end{aligned}$$

Then it is clear that $\mathcal{S}' \supset \mathcal{S}''$. Moreover, it is easy to see that $\#\mathcal{S}'' = \#\mathcal{T}$. Therefore, we have $\#\mathcal{S}' \geq \#\mathcal{T}$. The equality is equivalent to $\mathcal{S}'' = \mathcal{S}'$. The equality fails if and only if there is (I, D) such that D is non-cyclic and $\#I$ is non-prime-power. Such a pair (I, D) exists if and only if Γ is non-cyclic and $\#\Gamma$ is non-prime-power. □

Remark 6.4. The authors conjecture that the homomorphism $\beta'' = \beta|_{\mathbb{N}^{\mathcal{S}''}} : \mathbb{N}^{\mathcal{S}''} \rightarrow \mathbb{N}^{\mathcal{T}}$ is injective. This is true when Γ is cyclic or $\#\Gamma$ is a prime-power, i.e., when $\mathcal{S}' = \mathcal{S}''$ (see Corollary 5.4 and Proposition 6.5). However, we have not proved this for general Γ .

6.2. The case of cyclic groups. In this subsection, we prove Theorem 1.3(1) for cyclic groups Γ . Thanks to Corollary 6.2, it is enough to show the following:

Proposition 6.5. *When Γ is cyclic, the homomorphism $\beta' : \mathbb{N}^{S'} \rightarrow \mathbb{N}^{\mathcal{T}}$ is injective.*

Proof. As in Proposition 6.3, we have

$$S' = S'' = \coprod_{p \mid \#\Gamma} \{(I, D) \in \mathcal{S} \mid \#I \text{ is a } p\text{-power}\}.$$

By definition, \mathcal{T} is also decomposed as a disjoint union

$$\mathcal{T} = \coprod_p (\{H \subset \Gamma\} \times \mathcal{S}_p),$$

where $\{H \subset \Gamma\}$ denotes the set of subgroups such that Γ/H is cyclic of order prime to p . Also, the homomorphism β respects these decompositions. Therefore, it is enough to check the injectivity for each components. The proposition follows from the next lemma, applied for the prime-to- p -component of Γ as Δ . \square

Lemma 6.6. *For a finite abelian group Δ , let*

$$\bigoplus_{D \subset \Delta} \mathbb{N} \rightarrow \bigoplus_{H \subset \Delta} \mathbb{N},$$

where D and H run over all subgroups of Δ , be the homomorphism defined by

$$\sum_D a_D [D] \mapsto \sum_H \left(\sum_{D \subset H} a_D \right) [H].$$

Then this homomorphism is injective.

Proof. Indeed, we can recover a_D from the family of values $(\sum_{D \subset H} a_D)_H$ by induction on the size of D . \square

Note that in this lemma, it is important that H runs over all subgroups. However, in the definition of \mathcal{T} , the quotient group Γ/H must be cyclic. So we need to use the assumption that Γ is cyclic again.

Before closing this subsection, it is worth mentioning the cardinality of \mathcal{S} and \mathcal{T} when Γ is a cyclic group.

Lemma 6.7. *Suppose*

$$\#\Gamma = p_1^{e_1} \cdots p_s^{e_s},$$

where p_1, \dots, p_s are distinct primes and $e_i \geq 1$. Then we have

$$\#\mathcal{S} = \prod_{i=1}^s \frac{1}{2}(e_i + 1)(e_i + 2) - \prod_{i=1}^s (e_i + 1)$$

and

$$\#\mathcal{T} = \frac{1}{2} \left(\sum_{i=1}^s e_i \right) \prod_{i=1}^s (e_i + 1).$$

Example 6.8. If $e_1 = \dots = e_s = 1$, then $\#\mathcal{S} = 3^s - 2^s$ and $\#\mathcal{T} = s \cdot 2^{s-1}$.

Proof. Since Γ is cyclic, the set \mathcal{S} consists of pairs (I, D) such that $0 \neq I \subset D \subset \Gamma$. This corresponds to divisors $1 \neq \#I \mid \#D \mid \#\Gamma$. The number of such pairs is

$$\prod_{i=1}^s \#\{0 \leq a \leq b \leq e_i\} - \prod_{i=1}^s \#\{0 \leq b \leq e_i\},$$

which is equal to the claimed formula.

Next we consider \mathcal{T} . For each $1 \leq i \leq s$, the number of subgroups $H \subset \Gamma$ such that Γ/H is cyclic of order prime to p_i is equal to

$$\prod_{j \neq i} \#\{0 \leq c \leq e_j\} = \prod_{j \neq i} (e_j + 1).$$

Therefore, we obtain

$$\#\mathcal{T} = \sum_{i=1}^s \left(\prod_{j \neq i} (e_j + 1) \right) \cdot \#\mathcal{S}_{p_i}.$$

We also have

$$\#\mathcal{S}_{p_i} = \#\{1 \leq a \leq b \leq e_i\} = \frac{1}{2}e_i(e_i + 1).$$

By combining these, we obtain the lemma. \square

6.3. The case of non-cyclic groups. In this subsection we prove Theorem 1.3(2). To show a monoid is non-free, we will count the irreducible elements of the monoid as in [5, §5.2].

Recall that an irreducible element of a commutative monoid is a non-invertible element that cannot be represented as a sum of two non-invertible elements. Then the basis of a free commutative monoid is determined as the set of irreducible elements.

Proposition 6.9. *For $(I, D) \in \mathcal{S}$, we have $\beta((I, D))$ is an irreducible element of $\beta(\mathbb{N}^{\mathcal{S}})$ if and only if $(I, D) \in \mathcal{S}'$. Also, β is injective on \mathcal{S}' .*

Proof. The “only if” part follows from the proof of Corollary 6.2. Let us show the “if” part. Let $(I, D) \in \mathcal{S}'$ and suppose that

$$\beta((I, D)) = \sum_{\lambda} \beta((I_{\lambda}, D_{\lambda}))$$

for a family $\{(I_{\lambda}, D_{\lambda})\}_{\lambda \in \Lambda}$ in \mathcal{S} . We want to show Λ is a singleton and the family coincides with $\{(I, D)\}$.

For each prime $p \mid \#\Gamma$, we have

$$\sum_{H \supset D} (p, H, I_p, D_p) = \sum_{\lambda \in \Lambda, p \mid \#I_{\lambda}} \sum_{H \supset D_{\lambda}} (p, H, (I_{\lambda})_p, (D_{\lambda})_p).$$

In the both sides, H satisfies Γ/H is cyclic and $p \nmid [\Gamma : H]$. Also, the left side should be understood to be zero unless $p \mid \#I$. This equality can be rephrased as the combination of

- (a) For any $p \mid \#I$ and $\lambda \in \Lambda$, we have either $p \nmid \#I_{\lambda}$ or $(I_p, D_p) = ((I_{\lambda})_p, (D_{\lambda})_p)$.
- (b) We have

$$\sum_{H \supset D} (p, H, I_p, D_p) = \sum_{\lambda \in \Lambda, p \mid \#I_{\lambda}} \sum_{H \supset D_{\lambda}} (p, H, I_p, D_p).$$

By considering the $H = \Gamma$ component, we can divide (b) as

- (b1) We have $\text{prime}(\#I) = \coprod_{\lambda \in \Lambda} \text{prime}(\#I_\lambda)$, where $\text{prime}(n)$ denotes the set of prime divisors of n . In other words, we have $\text{prime}(I_\lambda) \subset \text{prime}(I)$ for any $\lambda \in \Lambda$ and moreover, for each $p \mid \#I$, there exists a unique $\lambda_p \in \Lambda$ such that $p \mid \#I_{\lambda_p}$.
- (b2) For that λ_p , we have

$$\sum_{H \supset D} (p, H, I_p, D_p) = \sum_{H \supset D_{\lambda_p}} (p, H, I_p, D_p).$$

We claim that (b2) is equivalent to $D_{\lambda_p} = D$ (assuming (a)). To show this, we use the following:

Lemma 6.10. *Let Γ be a finite abelian group. Let D, D' be two subgroups of Γ . Suppose that for any subgroup $H \subset \Gamma$ such that Γ/H is cyclic, we have $H \supset D$ if and only if $H \supset D'$. Then we have $D = D'$.*

Proof. This is because any subgroup of Γ can be expressed as the intersection of subgroups $H \subset \Gamma$ with Γ/H is cyclic. \square

Since we impose an additional condition $p \nmid [\Gamma : H]$, we deduce from (b2) only that the prime-to- p component of D coincides with that of D_{λ_p} . But by combining this with (a), we obtain $D_{\lambda_p} = D$, as claimed.

Note that, since any λ is represented as λ_p for some p , we obtain $D_\lambda = D$ for any $\lambda \in \Lambda$. As a summary, we have observed:

- (b1) We have $\text{prime}(\#I) = \coprod_{\lambda \in \Lambda} \text{prime}(\#I_\lambda)$.
- (a)' For each p and the $\lambda_p \in \Lambda$, we have $(I_{\lambda_p})_p = I_p$.
- (b2)' For any $\lambda \in \Lambda$, we have $D_\lambda = D$.

Now we use the assumption that $(I, D) \in \mathcal{S}'$, that is, either D is non-cyclic or $\#I$ is a prime-power. If $\#I$ is a p -power, then (b1) implies that Λ is a singleton and then (a)' and (b2)' imply $(I_{\lambda_p}, D_{\lambda_p}) = (I, D)$, as desired.

Suppose D is non-cyclic. Then there is $p \mid \#D$ such that the p -group D_p is non-cyclic. Then (b2)' implies that $(D_\lambda)_p$ is also non-cyclic for any λ . Since D_λ/I_λ is cyclic, this implies that $(I_\lambda)_p$ is non-zero for any λ . By (b1), we must have Λ is a singleton. By (b1), (a)', and (b2)', we have $(I_{\lambda_p}, D_{\lambda_p}) = (I, D)$, as desired.

This completes the proof of Proposition 6.9. \square

Now we show Theorem 1.3(2). Suppose $\beta(\mathbb{N}^{\mathcal{S}})$ is a free monoid. As a summary of Corollary 6.2 and Proposition 6.9, we have a surjective homomorphism

$$\beta' : \mathbb{N}^{\mathcal{S}'} \rightarrow \beta(\mathbb{N}^{\mathcal{S}}),$$

which yields a bijection from \mathcal{S}' to the set of irreducible elements of $\beta(\mathbb{N}^{\mathcal{S}})$. Therefore, the rank of $\beta(\mathbb{N}^{\mathcal{S}})$ is equal to $\#\mathcal{S}'$. On the other hand, since $\beta(\mathbb{N}^{\mathcal{S}})$ is a submonoid of $\mathbb{N}^{\mathcal{T}}$, its rank must be $\leq \#\mathcal{T}$. As a consequence, we must have $\#\mathcal{S}' \leq \#\mathcal{T}$. By Proposition 6.3, we deduce that either Γ is cyclic or $\#\Gamma$ is a prime-power. This completes the proof of Theorem 1.3(2).

ACKNOWLEDGMENTS

We sincerely thank the anonymous referees for providing valuable comments to improve this paper. The second author is supported by JSPS KAKENHI Grant Number 22K13898.

REFERENCES

- [1] M. Atsuta and T. Kataoka. Fitting ideals of class groups for CM abelian extensions. *Algebra Number Theory*, 17(11):1901–1924, 2023.
- [2] C. W. Curtis and I. Reiner. *Methods of representation theory. Vol. I*. Wiley Classics Library. John Wiley & Sons, Inc., New York, 1990. With applications to finite groups and orders, Reprint of the 1981 original, A Wiley-Interscience Publication.
- [3] S. Dasgupta and M. Kakde. On the Brumer–Stark conjecture. *Ann. of Math. (2)*, 197(1):289–388, 2023.
- [4] C. Greither. Determining Fitting ideals of minus class groups via the equivariant Tamagawa number conjecture. *Compos. Math.*, 143(6):1399–1426, 2007.
- [5] C. Greither and T. Kataoka. Fitting ideals and various notions of equivalence for modules. *Manuscripta Math.*, 173(1-2):259–291, 2024.
- [6] F. Hajir, C. Maire, and R. Ramakrishna. On Ozaki’s theorem realizing prescribed p -groups as p -class tower groups. *Algebra Number Theory*, 18(4):771–786, 2024.
- [7] A. Heller and I. Reiner. Representations of cyclic groups in rings of integers. I. *Ann. of Math. (2)*, 76:73–92, 1962.
- [8] A. Heller and I. Reiner. Representations of cyclic groups in rings of integers. II. *Ann. of Math. (2)*, 77:318–328, 1963.
- [9] T. Kataoka. Fitting invariants in equivariant Iwasawa theory. In *Development of Iwasawa theory—the centennial of K. Iwasawa’s birth*, volume 86 of *Adv. Stud. Pure Math.*, pages 413–465. Math. Soc. Japan, Tokyo, 2020.
- [10] M. Kurihara. Notes on the dual of the ideal class groups of CM-fields. *J. Théor. Nombres Bordeaux*, 33(3, part 2):971–996, 2021.
- [11] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008.

FAKULTÄT INFORMATIK, UNIVERSITÄT DER BUNDESWEHR MÜNCHEN, 85577 NEUBIBERG, GERMANY
Email address: `cornelius.greither@unibw.de`

DEPARTMENT OF MATHEMATICS, FACULTY OF SCIENCE DIVISION II, TOKYO UNIVERSITY OF SCIENCE.
 1-3 KAGURAZAKA, SHINJUKU-KU, TOKYO 162-8601, JAPAN
Email address: `tkataoka@rs.tus.ac.jp`