On minus quotients of ideal class groups of cyclotomic fields

Satoshi FUJII *

October 15, 2019

Abstract

Let C_n^- be the minus quotient of the ideal class group of the n-th cyclotomic field. In this article, first, we show that each finite abelian group appears as a subgroup of C_n^- for some n. Second, we show that, for all pair of integers n and m with $n \mid m$, the kernel of the lifting map $C_n^- \to C_m^-$ is contained in the 4-torsion $C_n^-[4]$ of C_n^-. Such an evaluation of the exponent is an individuality of cyclotomic fields.

1 Introduction

Let $\mathbb{Q}$ be the field of rational numbers. Throughout this article, all algebraic extensions of $\mathbb{Q}$ are assumed to be contained in a fixed algebraic closure of $\mathbb{Q}$. Let C_F be the ideal class group of a number field of F, not necessary finite over $\mathbb{Q}$. Let K be a CM-field and K^+ the totally real subfield of K. Let $\iota : C_{K^+} \to C_K$ be the lifting map of ideal class groups induced from the inclusion $K^+ \hookrightarrow K$. In this article, we adopt the definition of the minus quotient C_K^- of C_K as the cokernel

$$C_K^- = \mathrm{Coker}(C_{K^+} \to C_K) = C_K/\iota(C_{K^+})$$

with respect to the lifting map ι. It is known that the relative class number h_K^- of K is equal to the order or the twice of the order of C_K^-. Okazaki [7]

*Faculty of Education, Shimane University, 1060 Nishikawatsucho, Matsue, Shimane, 690–8504, Japan. e-mail : fujiisatoshi@edu.shimane-u.ac.jp

2000 *Mathematics Subject Classification.* Primary : 11R29. Secondary : 11R18, 11R23.

showed that, for CM-fields K_0 and K_1 with $K_0 \subseteq K_1$, $h^-_{K_0}$ divides $4h^-_{K_1}$, and also showed that this divisibility is best possible. To know the structures of C^-_K when K runs CM-fields is also a basic and important problem in number theory. In this article, we study behaviors of the structures and the "capitulations" of C^-_K specifically on the case where the fields K are cyclotomic fields.

For a positive integer n, let μ_n be the group of all n-th roots of unity in a suitable algebraically closed field. Let $k_n = \mathbb{Q}(\mu_n)$ be the n-th cyclotomic field. Let C_n and C^+_n be ideal class groups of k_n and k^+_n. We then denote by C^-_n the minus quotient of C_n. The first result of this article is as follows.

Theorem 1. *Let C be a finite abelian group. Then there is a positive integer n such that C^-_n contains a subgroup isomorphic to C.*

Cornell [3] showed that C_n contains a subgroup isomorphic to C for some n. Based on Cornell's argument, we can obtain a refined result.

The second result is dealing with the "capitulations" of C^-_n for $n \geq 1$. When an integer n divides an integer m, we will write $n \mid m$ as usual.

Theorem 2. *Let n and m be positive integers with $n \mid m$. Then the kernel* $\mathrm{Ker}(C^-_n \to C^-_m)$ *of the lifting map $C^-_n \to C^-_m$ is contained in the 4-torsion subgroup $C^-_n[4]$ of C^-_n.*

In particular, for each odd prime number p and each pair of positive integers m and n with $n \mid m$, the p-part of the linting map $C^-_n \otimes \mathbb{Z}_p \to C^-_m \otimes \mathbb{Z}_p$ is always injective, which can be seen as a generalization of proposition 13.26 of [10] for finite extension of cyclotomic fields. As we will see later, in general, the assertion of theorem 2 does not hold for imaginary abelian fields. In fact, we will show that there are finite extensions K/F of imaginary abelian fields with large $\mathrm{Ker}(C^-_F \to C^-_K)$ (see proposition 3). Thus we can say that the validity of theorem 2 is an individuality of cyclotomic fields. In contrast to theorem 2, Kurihara [6] showed that, for each positive integer n, there exists a positive integer m divided by n such that $C^+_n \to C^+_m$ is trivial. The author do not know whether there is a pair of positive integers m and n with $n \mid m$ such that $C^-_n \to C^-_m$ is really not injective or not. To find out such an example of a pair of integers would be an interesting problem.

Let $C^-_\infty = \varinjlim_n C^-_n$, the inductive limit is taken with respect to lifting maps. By combining theorem 1 and theorem 2, we can obtain the following.

Theorem 3. *There is an isomorphism $C^-_\infty \simeq (\mathbb{Q}/\mathbb{Z})^{\oplus \mathbb{N}}$, the direct sum of countably infinitely many copies of $\mathbb{Q}/\mathbb{Z}$, of abelian groups.*

Brumer [2] showed that $\varinjlim_n C_n \simeq (\mathbb{Q}/\mathbb{Z})^{\oplus \mathbb{N}}$, and hence $C_\infty^- \simeq (\mathbb{Q}/\mathbb{Z})^{\oplus \mathbb{N}}$ by Kurihara's result [6] stated in the above. We will give an alternative proof of theorem 3.

Here we set some notations. For a prime number p, let $\mathbb{Z}_p$ and $\mathbb{Q}_p$ be the ring of p-adic integers and the field of p-adic numbers, respectively. For a field F, denote by μ_F the group of all roots of unity in F. When F is a number field not necessary finite over $\mathbb{Q}$, for an ideal I of F, let $[I]$ be the ideal class containing I. For a finite Galois extension K/F and a $\mathrm{Gal}(K/F)$-module M, denote by $H^i(K/F, M)$ the i-th cohomology group $H^i(\mathrm{Gal}(K/F), M)$ for short. When M is equipped a multiplicative operation, for $\sigma \in \mathrm{Gal}(K/F)$ and $m \in M$, we will use the notation $(\sigma - 1)m = \sigma(m)m^{-1}$.

Let K/F be a Galois extension and L/K an abelian extensions such that L/F is a Galois extension. For $g \in \mathrm{Gal}(K/F)$ and $x \in \mathrm{Gal}(L/K)$, we define the action of $\mathrm{Gal}(K/F)$ on $\mathrm{Gal}(L/K)$ via the inner automorphism $x \mapsto \tilde{g}x\tilde{g}^{-1}$, here denote by $\tilde{g} \in \mathrm{Gal}(L/F)$ an extension of g.

For an abelian group A and a positive integer n, let $A[n]$ be the n-torsion subgroup of A.

2 Proof of theorem 1

Let C be a finite abelian group. Suppose that $C \simeq \oplus_{i=1}^r \mathbb{Z}/n_i\mathbb{Z}$ for some integers r and $n_1, \cdots, n_r$. Choose distinct prime numbers p_i with $1 \leq i \leq r$ such that $p_i \equiv 1 \bmod 4n_i$. For each i with $1 \leq i \leq r$, let $(p_i) = (\pi_i)(\overline{\pi_i})$ be the prime decomposition of the prime number p_i in k_4. Denote by $k_4^{(\pi_i)}$ and $k_4^{(\overline{\pi_i})}$ the ray class fields over k_4 of conductors (π_i) and $(\overline{\pi_i})$. Since the unit group of k_4 is μ_4, it follows that $k_4^{(\pi_i)}$ and $k_4^{(\overline{\pi_i})}$ are cyclic extensions over k_4 of degree $\frac{p_i-1}{4}$, and are tamely ramified. For each i with $1 \leq i \leq r$, put $F_i = k_4^{(\pi_i)} k_4^{(\overline{\pi_i})}$, and put $F = F_1 \cdots F_r$. Then $F/\mathbb{Q}$ is a Galois extension. Since the fields $F_1, \cdots, F_r$ are linearly disjoint over k_4, we have a decomposition

$$\mathrm{Gal}(F/k_4) \simeq \oplus_{i=1}^r \mathrm{Gal}(F_i/k_4),$$

and similarly we have

$$\mathrm{Gal}(F_i/k_4) \simeq \left(\mathbb{Z}/\frac{p_i - 1}{4}\mathbb{Z}\right)^2$$

for each i with $1 \leq i \leq r$.

Let J be a generator of $\mathrm{Gal}(k_4/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$. Then J acts on $\mathrm{Gal}(F/k_4)$. In particular, J induces an isomorphism $\mathrm{Gal}(k_4^{(\pi_i)}/k_4) \simeq \mathrm{Gal}(k_4^{(\overline{\pi_i})}/k_4)$, $g \mapsto$

$\tilde{J}g\tilde{J}^{-1}$ since $k_4^{(\pi_i)}$ and $k_4^{(\overline{\pi_i})}$ are conjugate over $\mathbb{Q}$, and this isomorphism gives the action of J on $\mathrm{Gal}(F/k_4) \simeq \oplus_{i=1}^r \left(\mathrm{Gal}(k_4^{(\pi_i)}/k_4) \times \mathrm{Gal}(k_4^{(\overline{\pi_i})}/k_4)\right)$. Put

$$(J-1)\mathrm{Gal}(F/k_4) = \{\tilde{J}g\tilde{J}^{-1}g^{-1} \mid g \in \mathrm{Gal}(F/k_4)\}.$$

The subgroup $(J-1)\mathrm{Gal}(F/k_4)$ of $\mathrm{Gal}(F/\mathbb{Q})$ coincides with the commutator subgroup of $\mathrm{Gal}(F/\mathbb{Q})$. Let F^{ab} be the fixed field of $(J-1)\mathrm{Gal}(F/k_4)$, and then $F^{\mathrm{ab}}/\mathbb{Q}$ is an abelian extension. Since F/k_4 is tamely ramified and F does not contain μ_8, the conductor of $F^{\mathrm{ab}}/\mathbb{Q}$ is equal to $4p_1 \cdots p_r\infty$, where ∞ is the infinite prime of $\mathbb{Q}$. Put $n = 4p_1 \cdots p_r$. Then we can see that F^{ab} is contained in k_n, and hence we have $F^{\mathrm{ab}} = k_n \cap F$.

We show that

$$\mathrm{Gal}(F/F^{\mathrm{ab}}) \simeq \oplus_{i=1}^r \left(\mathbb{Z}/\frac{p_i-1}{4}\mathbb{Z}\right),$$

and that F/F^{ab} is an unramified extension. First, we shall show $\mathrm{Gal}(F/F^{\mathrm{ab}}) \simeq \oplus_{i=1}^r \left(\mathbb{Z}/\frac{p_i-1}{4}\mathbb{Z}\right)$. Recall that

$$\mathrm{Gal}(F/k_4) \simeq \oplus_{i=1}^r \mathrm{Gal}(F_i/k_4) \simeq \oplus_{i=1}^r \left(\mathrm{Gal}(k_4^{(\pi_i)}/k_4) \times \mathrm{Gal}(k_4^{(\overline{\pi_i})}/k_4)\right).$$

Let σ_i be a generator of $\mathrm{Gal}(k_4^{(\pi_i)}/k_4)$. Then $\overline{\sigma_i} = \tilde{J}\sigma_i\tilde{J}^{-1}$ is a generator of $\mathrm{Gal}(k_4^{(\overline{\pi_i})}/k_4)$. Remark that the elements

$$(1, \cdots, 1, \underbrace{\sigma_i}_{\text{in } \mathrm{Gal}(k_4^{(\pi_i)}/k_4)}, 1, \cdots, 1)$$

and

$$(1, \cdots, 1, \underbrace{\overline{\sigma_i}}_{\text{in } \mathrm{Gal}(k_4^{(\overline{\pi_i})}/k_4)}, 1, \cdots, 1)$$

generate the inertia subgroups of $\mathrm{Gal}(F/k_4)$ at (π_i) and $(\overline{\pi_i})$ respectively. Let $(\sigma_1^{a_1}, \overline{\sigma_1}^{b_1}, \cdots, \sigma_r^{a_r}, \overline{\sigma_r}^{b_r}) \in \mathrm{Gal}(F/k_4)$ with $a_1, b_1, \cdots, a_r, b_r \in \mathbb{Z}$. Since the action of J on $\mathrm{Gal}(F/k_4)$ is given by

$$J(\sigma_1^{a_1}, \overline{\sigma_1}^{b_1}, \cdots, \sigma_r^{a_r}, \overline{\sigma_r}^{b_r}) = (\sigma_1^{b_1}, \overline{\sigma_1}^{a_1}, \cdots, \sigma_r^{b_r}, \overline{\sigma_r}^{a_r}),$$

we have

$$\begin{aligned} &(J-1)(\sigma_1^{a_1}, \overline{\sigma_1}^{b_1}, \cdots, \sigma_r^{a_r}, \overline{\sigma_r}^{b_r}) \\ =&(\sigma_1^{b_1-a_1}, \overline{\sigma_1}^{-(b_1-a_1)}, \cdots, \sigma_r^{b_r-a_r}, \overline{\sigma_r}^{-(b_r-a_r)}). \end{aligned}$$

Thus we have

$$(J-1)\mathrm{Gal}(F/k_4) = \left\{(\sigma_1^{c_1}, \overline{\sigma_1}^{-c_1}, \cdots, \sigma_r^{c_r}, \overline{\sigma_r}^{-c_r}) \mid c_1, \cdots, c_r \in \mathbb{Z}\right\}.$$

Hence the following map

$$\begin{aligned}&\oplus_{i=1}^r \left(\mathbb{Z}/\tfrac{p_i-1}{4}\mathbb{Z}\right) \to (J-1)\mathrm{Gal}(F/k_4),\\ &(c_1 \bmod \tfrac{p_1-1}{4}, \cdots, c_r \bmod \tfrac{p_r-1}{4}) \mapsto (\sigma_1^{c_1}, \overline{\sigma_1}^{-c_1}, \cdots, \sigma_r^{c_r}, \overline{\sigma_r}^{-c_r})\end{aligned}$$

is an isomorphism.

Next, we show that F/F^{ab} is unramified. If

$$(1, \cdots, 1, \sigma_i^c, 1, \cdots, 1) = (\sigma_1^{c_1}, \overline{\sigma_1}^{-c_1}, \cdots, \sigma_r^{c_r}, \overline{\sigma_r}^{-c_r})$$

for some integers $c, c_1, \cdots, c_r$, then we can see that $c \equiv 0 \bmod \frac{p_i-1}{4}$ and that $c_j \equiv 0 \bmod \frac{p_j-1}{4}$ for each j with $1 \le j \le r$. This shows that (π_i) is unramified in F/F^{ab}. Similarly, $(\overline{\pi_i})$ is also unramified in F/F^{ab}.

By class field theory, the Artin map induces a surjective map

$$C_n \to \mathrm{Gal}(Fk_n/k_n).$$

Since $\mathrm{Gal}(Fk_n/k_n) \simeq \mathrm{Gal}(F/F \cap k_n) = (J-1)\mathrm{Gal}(F/k_4)$, the above surjective map factors through C_n^-. Then we have isomorphic or surjective maps

$$\begin{aligned} C_n^- &\twoheadrightarrow (J-1)\mathrm{Gal}(F/k_4)\\ &\simeq \oplus_{i=1}^r \left(\mathbb{Z}/\frac{p_i-1}{4}\mathbb{Z}\right)\\ &\twoheadrightarrow \oplus_{i=1}^r \mathbb{Z}/n_i\mathbb{Z}\\ &= C.\end{aligned}$$

From the duality theorem of finite abelian groups, C_n^- contains a subgroup isomorphic to C. □

Remark 1. An alternative proof of theorem 1 based on Iwasawa theory of ideal class groups exists. For each prime number p and each positive integer r, we can show that there is a positive integer s such that the minus part of the Iwasawa λ-invariant of the cyclotomic $\mathbb{Z}_p$-extension of k_{2ps} is greater than or equal to r. Hence, each finite abelian p-group appears as a quotient of C_t^- for some t. Then, C_n^- has a quotient isomorphic to given finite abelian group C for some n, and hence C_n^- has a subgroup isomorphic to C. We shall omit a precise proof here.

3 Proof of theorem 2

3.1 Preliminaries

For a finite extension $K/\mathbb{Q}$, let E_K be the unit group of K.

Lemma 1. *Let K/F be a Galois extension of number fields of finite degrees over $\mathbb{Q}$. For each prime $\mathfrak{q}$ of F, let $F_{\mathfrak{q}}$ be the localization of F at $\mathfrak{q}$, and $K_{\mathfrak{q}}$ the localization of K at a prime lying above $\mathfrak{q}$. Let $U_{K_{\mathfrak{q}}}$ be the unit group of $K_{\mathfrak{q}}$. Then there is the following exact sequence*

$$0 \to \mathrm{Ker}(C_F \to C_K) \to H^1(K/F, E_K) \to \bigoplus_{\mathfrak{q}:primes\ of\ F} H^1(K_{\mathfrak{q}}/F_{\mathfrak{q}}, U_{K_{\mathfrak{q}}})$$

of abelian groups. Here, the second map denotes the direct sum of restriction maps.

Proof. See for example corollary of proposition 1 in [9]. □

Let K be a CM-field. Let J be the generator of $\mathrm{Gal}(K/K^+) \simeq \mathbb{Z}/2\mathbb{Z}$, that is, J is the complex conjugation of K. Let $Q_K = [E_K : \mu_K E_{K^+}]$ be the unit index of K. It is known that $Q_K = 1$ or 2, and $Q_K = 2$ if and only if for each root of unity $\zeta \in \mu_K$ of K there exists $\varepsilon \in E_K$ such that $\zeta = (J-1)\varepsilon$. When $K = k_n$, $Q_{k_n} = 2$ if and only if n is not a prime power. If readers want to know proofs of these facts on the unit index, see for example theorem 4.12 and corollary 4.13 of [10].

Let F be a CM-field. Suppose that $F \subseteq K$. Since $\mathrm{Gal}(K/K^+) \simeq \mathrm{Gal}(F/F^+)$, we may identify these groups. From an argument similar to the proof of proposition 13.26 of [10], we can obtain a fundamental map and a complex for the proof.

Lemma 2. *Suppose that K/F^+ is a Galois extension. Then, there is a complex*

$$\mathrm{Ker}(C_F^- \to C_K^-) \to H^1(K/F, \mu_K) \to \bigoplus_{\mathfrak{q}} H^1(K_{\mathfrak{q}}/F_{\mathfrak{q}}, U_{K_{\mathfrak{q}}})$$

of finite abelian groups. Here the second map is the composition of the natural map $H^1(K/F, \mu_K) \to H^1(K/F, E_K)$ and the direct sum of restriction maps.

Proof. Remark that $J\sigma = \sigma J$ for each $\sigma \in \mathrm{Gal}(K/F)$ since K is a CM-field and K/F^+ is a Galois extension. Recall that for an ideal I of F, we denote by $[I]$ the ideal class of F containing I. Suppose that $[I]\iota(C_{F^+}) \in \mathrm{Ker}(C_F^- \to$

C_K^-). Then there exist $\alpha \in K^\times$ and an ideal I^+ of K^+ such that $I = (\alpha)I^+$ in K. It holds that $(J-1)I = ((J-1)\alpha)$. Let $\sigma \in \mathrm{Gal}(K/F)$. Then it holds that $(\sigma-1)(J-1)\alpha \in E_K$, and the absolute value of $(\sigma-1)(J-1)\alpha$ is 1. This implies that $(\sigma-1)(J-1)\alpha \in \mu_K$. We then obtain a map

$$\mathrm{Ker}(C_F^- \to C_K^-) \to H^1(K/F, \mu_K),\ [I]\iota(C_{F^+}) \mapsto \text{class of } f_\alpha,$$

here f_α is defined by the formula

$$f_\alpha(\sigma) = (\sigma-1)(J-1)\alpha$$

for all $\sigma \in \mathrm{Gal}(K/F)$. We show that the above map is well-defined. Put

$$\mathfrak{I}_{K/F} = \{I : \text{ideal of } F \mid \exists\alpha \in K^\times,\ \exists I^+ : \text{ideal of } K^+ \text{ s.t. } I = (\alpha)I^+ \text{ in } K\}.$$

Then, we shall remark here that $\mathrm{Ker}(C_F^- \to C_K^-)$ is a quotient of $\mathfrak{I}_{K/F}$. Let $I \in \mathfrak{I}_{K/F}$, then there are $\alpha \in K^\times$ and an ideal I^+ of K^+ such that $I = (\alpha)I^+$ in K. Suppose that $I = (\alpha)I^+ = (\alpha_0)I_0^+$ for some $\alpha_0 \in K^\times$ and an ideal I_0^+ of K^+ in K. Then we have $((J-1)\alpha) = ((J-1)\alpha_0)$, and hence $(J-1)\alpha = \zeta(J-1)\alpha_0$ for some $\zeta \in E_K$. Since $\zeta = (J-1)(\alpha\alpha_0^{-1})$, it holds that $\zeta \in \mu_K$. For each $\sigma \in \mathrm{Gal}(K/F)$, we have

$$f_\alpha(\sigma) = (\sigma-1)\zeta \cdot f_{\alpha_0}(\sigma),$$

and hence f_α and f_{α_0} define the same cohomology class of $H^1(K/F, \mu_K)$. This shows that

$$\mathfrak{I}_{K/F} \to H^1(K/F, \mu_K),\ I \mapsto \text{class of } f_\alpha$$

is well-defined. Suppose that $\alpha \in F^\times$, I^+ is an ideal of F^+ and $I = (\alpha)I^+$ in F. Since $\alpha \in F^\times$, we have $f_\alpha(\sigma) = 1$ for each $\sigma \in \mathrm{Gal}(K/F)$. This shows that the map $\mathrm{Ker}(C_F^- \to C_K^-) \to H^1(K/F, \mu_K)$ is well-defined.

Next, we show that the composition of $\mathrm{Ker}(C_F^- \to C_K^-) \to H^1(K/F, \mu_K)$ and $H^1(K/F, \mu_K) \to \bigoplus_{\mathfrak{q}} H^1(K_{\mathfrak{q}}/F_{\mathfrak{q}}, U_{K_{\mathfrak{q}}})$ is trivial. Recall $(J-1)I = ((J-1)\alpha)$ in K. Since $(J-1)I$ is an ideal of F, for each finite prime $\mathfrak{q}$ of F, there exist $\pi_{\mathfrak{q}} \in F^\times$ and $\varepsilon_{\mathfrak{q}} \in U_{K_{\mathfrak{q}}}$ such that $(J-1)\alpha = \pi_{\mathfrak{q}}\varepsilon_{\mathfrak{q}}$. Then, for each $\sigma \in \mathrm{Gal}(K_{\mathfrak{q}}/F_{\mathfrak{q}})$, it follows that

$$(\sigma-1)(J-1)\alpha = (\sigma-1)(\pi_{\mathfrak{q}}\varepsilon_{\mathfrak{q}}) = (\sigma-1)\varepsilon_{\mathfrak{q}},$$

and hence the restriction $f_\alpha|_{\mathrm{Gal}(K_{\mathfrak{q}}/F_{\mathfrak{q}})}$ of f_α to a decomposition group $\mathrm{Gal}(K_{\mathfrak{q}}/F_{\mathfrak{q}})$ at $\mathfrak{q}$ defines the trivial class of $H^1(K_{\mathfrak{q}}/F_{\mathfrak{q}}, U_{K_{\mathfrak{q}}})$. Since all infinite primes of F are unramified in K/F, we have finished the proof of lemma 2. □

Proposition 1. *Suppose that K/F^+ is a Galois extension. If $Q_K = 2$ then the kernel of the map* $\mathrm{Ker}(C_F^- \to C_K^-) \to H^1(K/F, \mu_K)$ *is contained in* $C_F^-[2]$. *If $Q_K = 1$ then the kernel of* $\mathrm{Ker}(C_F^- \to C_K^-) \to H^1(K/F, \mu_K)$ *is contained in* $C_F^-[4]$.

Proof. Suppose that $[I]\iota(C_{F^+})$ is contained in the kernel of $\mathrm{Ker}(C_F^- \to C_K^-) \to H^1(K/F, \mu_K)$. Let $I = (\alpha)I^+$ for some $\alpha \in K^\times$ and an ideal I^+ of K^+. Then, there exists $\zeta \in \mu_K$ such that

$$f_\alpha(\sigma) = (\sigma - 1)(J - 1)\alpha = (\sigma - 1)\zeta$$

for each $\sigma \in \mathrm{Gal}(K/F)$. Suppose first that $Q_K = 2$. Then there exists $\varepsilon \in E_K$ such that $\zeta = (J-1)\varepsilon^{-1}$. Thus, for each $\sigma \in \mathrm{Gal}(K/F)$, we have

$$(\sigma - 1)(J - 1)\alpha = (\sigma - 1)(J - 1)\varepsilon^{-1},$$

and hence

$$\sigma((J - 1)(\alpha\varepsilon)) = (J - 1)(\alpha\varepsilon).$$

Therefore, $(J - 1)(\alpha\varepsilon) \in F^\times$.

Remark that $I = (\alpha\varepsilon)I^+$. By operating J and then multiplying $(1 - J)(\alpha\varepsilon)$ to both terms, we have $J(I)(1 - J)(\alpha\varepsilon) = (\alpha\varepsilon)I^+ = I$. Therefore, since $(J - 1)(\alpha\varepsilon) \in F^\times$, it follows that

$$[I^2]\iota(C_{F^+}) = [IJ(I)(1 - J)(\alpha\varepsilon)]\iota(C_{F^+}) = [IJ(I)]\iota(C_{F^+}) = \iota(C_{F^+}),$$

therefore $[I]\iota(C_{F^+}) \in C_F^-[2]$.

Next, suppose that $Q_K = 1$. Since $I^2 = (\alpha^2)(I^+)^2$, we have

$$f_{\alpha^2}(\sigma) = (\sigma - 1)(J - 1)\alpha^2 = (\sigma - 1)\zeta^2 = (\sigma - 1)(J - 1)\zeta.$$

This implies that

$$\sigma((J - 1)(\alpha^2\zeta^{-1})) = (J - 1)(\alpha^2\zeta^{-1}),$$

and hence $(J - 1)(\alpha^2\zeta^{-1}) \in F^\times$. Remark that $I^2 = (\alpha^2\zeta^{-1})(I^+)^2$. By operating J and then multiplying $(1 - J)(\alpha^2\zeta^{-1})$ to both terms, we have $J(I^2)(1 - J)(\alpha^2\zeta^{-1}) = (\alpha^2\zeta^{-1})(I^+)^2 = I^2$. Therefore,

$$[I^4]\iota(C_{F^+}) = [I^2J(I^2)(1 - J)(\alpha^2\zeta^{-1})]\iota(C_{F^+}) = [I^2J(I^2)]\iota(C_{F^+}) = \iota(C_{F^+}),$$

as desired. □

Lemma 3. *Suppose that K/F^+ is a Galois extension and that $[K:F] = n$. Then* $\mathrm{Ker}(C_F^- \to C_K^-) \subseteq C_F^-[n]$.

Proof. For a finite extension k'/k, let $N_{k'/k}$ be the norm map from k' to k. Suppose that $[I]\iota(C_{F^+}) \in \mathrm{Ker}(C_F^- \to C_K^-)$. Then there are $\alpha \in K^\times$ and an ideal I^+ of K^+ such that $I = (\alpha)I^+$. By taking the norm map from K to F on both terms, we have $I^n = (N_{K/F}\alpha)(N_{K/F}I^+)$. Since $\mathrm{Gal}(K/F) \simeq \mathrm{Gal}(K^+/F^+)$, if holds that $N_{K/F}I^+ = N_{K^+/F^+}I^+$. This implies that $[I^n] \in \iota(C_{F^+})$. □

3.2 Proof of theorem 2

From here, we prove theorem 2. Let n and m be positive integers with $n \mid m$. For a fixed prime number p, put $A_n^- = C_n^- \otimes \mathbb{Z}_p$. We will evaluate $\mathrm{Ker}(A_n^- \to A_m^-)$ by splitting into three cases.

(1) Suppose that p is an odd prime number. We show that $A_n^- \to A_m^-$ is injective. For this, we may assume that $m = 2n$ if $4 \mid n$, $m = 4n$ if $2 \nmid n$ or $m = \ell n$ for some odd prime number ℓ. Assume that $m = 2n$ if $4 \mid n$ or $m = 4n$ if $2 \nmid n$. Then it holds that $[k_m : k_n] = 2$, and hence $A_n^- \to A_m^-$ is injective by lemma 3.

Suppose that $m = \ell n$ for some odd prime number ℓ. Assume that $\ell = p$. If $p \nmid n$ then $[k_{pm} : k_n] = p-1$, and hence $A_n^- \to A_{pn}^-$ is injective by lemma 3. If $p \mid n$, then it is known that $A_n^- \to A_{pn}^-$ is injective (see proposition 13.26 of [10]). Assume that $\ell \neq p$. By lemma 1, we have the following exact sequence

$$0 \to \mathrm{Ker}(A_n^- \to A_{\ell n}^-) \to (H^1(k_{\ell n}/k_n, E_{k_{\ell n}}) \otimes \mathbb{Z}_p)^- \\ \to \bigoplus_{\mathfrak{q} \mid \ell} H^1(k_{\ell n,\mathfrak{q}}/k_{n,\mathfrak{q}}, U_{k_{\ell n,\mathfrak{q}}}) \otimes \mathbb{Z}_p,$$

only here, for a J-module M, we let $M^- = \{m \in M \mid Jm = -m\}$. It holds that

$$H^1(k_{\ell n}/k_n, E_{k_{\ell n}}) \otimes \mathbb{Z}_p = H^1(k_{\ell n}/k_n, E_{k_{\ell n}} \otimes \mathbb{Z}_p).$$

Since p is odd, we have

$$E_{k_{\ell n}} \otimes \mathbb{Z}_p = (\mu_{k_{\ell n}} \otimes \mathbb{Z}_p) \oplus (E_{k_{\ell n}^+} \otimes \mathbb{Z}_p),$$

and hence it follows that

$$(H^1(k_{\ell n}/k_n, E_{k_{\ell n}}) \otimes \mathbb{Z}_p)^- = H^1(k_{\ell n}/k_n, \mu_{k_{\ell n}} \otimes \mathbb{Z}_p).$$

Since $\ell \neq p$, one sees that $\mu_{k_{\ell n}} \otimes \mathbb{Z}_p = \mu_{k_n} \otimes \mathbb{Z}_p$. This implies that

$$H^1(k_{\ell n}/k_n, \mu_{k_{\ell n}} \otimes \mathbb{Z}_p) = \mathrm{Hom}(\mathrm{Gal}(k_{\ell n}/k_n), \mu_{k_n} \otimes \mathbb{Z}_p).$$

Also, since $U_{k_{\ell n,\mathfrak{q}}}$ is a product of a finite abelian group of order prime to ℓ and a pro-ℓ abelian group, we can see that

$$\bigoplus_{\mathfrak{q}|\ell} H^1(k_{\ell n,\mathfrak{q}}/k_{n,\mathfrak{q}}, U_{k_{\ell n,\mathfrak{q}}}) \otimes \mathbb{Z}_p = \bigoplus_{\mathfrak{q}|\ell} H^1(k_{\ell n,\mathfrak{q}}/k_{n,\mathfrak{q}}, \mu_{k_{\ell n,\mathfrak{q}}} \otimes \mathbb{Z}_p).$$

Let $\mathfrak{q}$ be a prime of k_n lying above ℓ, and $\mathfrak{Q}$ be a prime of $k_{\ell n}$ lying above $\mathfrak{q}$. Let O_n and $O_{\ell n}$ be the ring of integers of k_n and $k_{\ell n}$. Since $k_{\ell n}/k_n$ is totally ramified at $\mathfrak{q}$, we have

$$\mu_{k_{\ell n,\mathfrak{q}}} \otimes \mathbb{Z}_p \simeq (O_{\ell n}/\mathfrak{Q})^\times \otimes \mathbb{Z}_p \simeq (O_n/\mathfrak{q})^\times \otimes \mathbb{Z}_p \simeq \mu_{k_{n,\mathfrak{q}}} \otimes \mathbb{Z}_p,$$

and hence it follows that

$$\bigoplus_{\mathfrak{q}|\ell} H^1(k_{\ell n,\mathfrak{q}}/k_{n,\mathfrak{q}}, \mu_{k_{\ell n,\mathfrak{q}}} \otimes \mathbb{Z}_p) = \bigoplus_{\mathfrak{q}|\ell} \mathrm{Hom}(\mathrm{Gal}(k_{\ell n,\mathfrak{q}}/k_{n,\mathfrak{q}}), \mu_{k_{n,\mathfrak{q}}} \otimes \mathbb{Z}_p).$$

Combining the above, since $\mathrm{Gal}(k_{\ell n}/k_n) \simeq \mathrm{Gal}(k_{\ell n,\mathfrak{q}}/k_{n,\mathfrak{q}})$ for each $\mathfrak{q}$, we find that

$$\mathrm{Hom}(\mathrm{Gal}(k_{\ell n}/k_n), \mu_{k_n} \otimes \mathbb{Z}_p) \to \bigoplus_{\mathfrak{q}|\ell} \mathrm{Hom}(\mathrm{Gal}(k_{\ell n,\mathfrak{q}}/k_{n,\mathfrak{q}}), \mu_{k_{n,\mathfrak{q}}} \otimes \mathbb{Z}_p)$$

is injective. Therefore, $A_n^- \to A_{\ell n}^-$ is injective.

(2) Suppose that $p = 2$ and m is a prime power. Put $m = \ell^r$ for some prime number ℓ and a non-negative integer r. Put also $n = \ell^s$ for some non-negative integer s with $s \leq r$. If $s = 0$ then $k_{\ell^0} = \mathbb{Q}$, and hence we may assume that $s \geq 1$. Remark that k_{ℓ^r}/k_{ℓ^s} is an ℓ-extension. If ℓ is an odd prime number then $A_{\ell^s}^- \to A_{\ell^r}^-$ is injective by lemma 3. If $\ell = 2$, then it is well known that the class number of k_{2^r} is prime to 2 for each $r \geq 0$. In particular, $A_{2^s}^- \to A_{2^r}^-$ is injective.

(3) Suppose that $p = 2$ and m is not a prime power. Suppose also that $m = 2^r m_0$ and $n = 2^s n_0$ for some non-negative integers r, s, m_0 and n_0 with $s \leq r$ and $(n_0 m_0, 2) = 1$. Let t be an integer greater than $r + 1$. We then have

$$k_{n_0} \subseteq k_n \subseteq k_m \subseteq k_{2^t m_0}.$$

We analyze here the extension $k_{2^t m_0}/k_{n_0}$.

Proposition 2. *The following assertions hold.*

(*i*) $\mathrm{Ker}(A^-_{n_0} \to A^-_{4n_0}) \subseteq A^-_{n_0}[2]$.

(*ii*) $\mathrm{Ker}(A^-_{2^v n_0} \to A^-_{2^u n_0}) = 0$ *for* $2 \leq v \leq u$.

(*iii*) $\mathrm{Ker}(A^-_{2^t n_0} \to A^-_{2^t m_0}) \subseteq A^-_{2^t n_0}[2]$ *for* $t \geq 2$.

Proof. (*i*) Since $[k_{4n_0} : k_{n_0}] = 2$, by lemma 3, we have $\mathrm{Ker}(A^-_{n_0} \to A^-_{4n_0}) \subseteq A^-_{n_0}[2]$.

(*ii*) Consider the cyclic 2-extension $k_{2^u n_0}/k_{2^v n_0}$. If $n_0 = 1$ then $C_{2^u} \otimes \mathbb{Z}_2 = 0$ as before. Suppose that n_0 has an odd prime factor. Since $\mathrm{Gal}(k_{2^u n_0}/k_{n_0})$ is the inertia subgroup in $k_{2^u n_0}/\mathbb{Q}$ at the prime 2, we find that $k_{2^u n_0}/k^+_{2^u n_0}$ is unramified at all primes lying above 2. We need the follwoing result of Iwasawa theory. Let $X^- = \varprojlim_u A^-_{2^u n_0}$, the projective limit is taken with respect to the norm maps. Then it is known that the formal power series ring $\mathbb{Z}_2[[T]]$ in one variable T with coefficients in $\mathbb{Z}_2$ acts on X^-, and X^- is a finitely generated torsion $\mathbb{Z}_2[[T]]$-module.

Lemma 4 (From corollary 1.4 of Atsuta [1])**.** *The module X^- has no non-trivial finite $\mathbb{Z}_2[[T]]$-submodule.*

Let $X = \varprojlim_u C_{2^u n_0} \otimes \mathbb{Z}_2$ and $X^+ = \varprojlim_u C^+_{2^u n_0} \otimes \mathbb{Z}_2$. For each u, since the sequence

$$0 \to C^+_{2^u n_0} \otimes \mathbb{Z}_2 \to C_{2^u n_0} \otimes \mathbb{Z}_2 \to A^-_{2^u n_0} \to 0$$

is exact, the sequence $0 \to X^+ \to X \to X^- \to 0$ is also exact. Let Y^+, Y and Y^- be kernels of the natural surjective projection maps $X^+ \to C^+_{4n_0} \otimes \mathbb{Z}_2$, $X \to C_{4n_0} \otimes \mathbb{Z}_2$ and $X^- \to A^-_{4n_0}$, respectively. For each u, put $\nu_u = \frac{(1+T)^{2^u}-1}{T} \in \mathbb{Z}_2[[T]]$. Then by Iwasawa theory, there are isomorphisms $C^+_{2^{u+2}n_0} \otimes \mathbb{Z}_2 \simeq X^+/\nu_u Y^+$ and $C_{2^{u+2}n_0} \otimes \mathbb{Z}_2 \simeq X/\nu_u Y$ of finite abelian groups. This implies that $X^+ \cap \nu_u Y = \nu_u Y^+$, and, since $\nu_u Y^+ \subseteq Y^+ \cap \nu_u Y \subseteq X^+ \cap \nu_u Y = \nu_u Y^+$, one sees that $\nu_u Y^+ = Y^+ \cap \nu_u Y$. We also find that $A^-_{2^{u+2}n_0} \simeq X/(X^+ + \nu_u Y)$. Therefore, one has the following exact sequence

$$0 \to \nu_u Y + Y^+/Y^+ \ (\simeq \nu_u Y/\nu_u Y^+) \to X^- \to A^-_{2^{u+2}n_0} \to 0$$

for each u. Since $\nu_u Y + Y^+/Y^+ = \nu_u Y^-$, we have $A^-_{2^{u+2}n_0} \simeq X^-/\nu_u Y^-$ for each non-negative integer u. Thus, by lemma 4 and by proposition of [8], one can see that $A^-_{2^u n_0} \to A^-_{2^\infty n_0} = \varinjlim_u A^-_{2^u n_0}$ is injective for each integer u with $u \geq 2$. In particular, for each pair of integers u and v with $2 \leq v \leq u$, $A^-_{2^v n_0} \to A^-_{2^u n_0}$ is injective.

(*iii*) For a positive integer u, put $k_{2^\infty u} = \bigcup_{t\geq 1} k_{2^t u}$. For each positive integer t greater than 1, by lemma 2, we have a complex

$$\begin{aligned}\mathrm{Ker}(A^-_{2^t n_0} \to A^-_{2^t m_0}) &\to H^1(k_{2^t m_0}/k_{2^t n_0}, \mu_{k_{2^t m_0}}) \otimes \mathbb{Z}_2 \\ &\to \bigoplus_{\mathfrak{q} \mid \frac{m_0}{n_0}} H^1(k_{2^t m_0,\mathfrak{q}}/k_{2^t n_0,\mathfrak{q}}, U_{k_{2^t m_0,\mathfrak{q}}}) \otimes \mathbb{Z}_2\end{aligned}$$

of abelian groups. Also, since $2 \nmid m_0$, for each finite prime $\mathfrak{q}$ of k_n with $\mathfrak{q} \mid \frac{m_0}{n_0}$, we find that

$$H^1(k_{2^t m_0,\mathfrak{q}}/k_{2^t n_0,\mathfrak{q}}, U_{k_{2^t m_0,\mathfrak{q}}}) \otimes \mathbb{Z}_2 = H^1(k_{2^t m_0,\mathfrak{q}}/k_{2^t n_0,\mathfrak{q}}, \mu_{k_{2^t m_0,\mathfrak{q}}} \otimes \mathbb{Z}_2).$$

from the same arguments as before.

Put $\mu_{2^\infty} = \bigcup_{u\geq 1} \mu_{2^u}$. From the fact that inductive limits preserve complexes, by taking the inductive limits with respect to positive integers t, lifting maps and inflation maps, we also obtain a complex

$$\begin{aligned}\mathrm{Ker}(A^-_{2^\infty n_0} \to A^-_{2^\infty m_0}) &\to H^1(k_{2^\infty m_0}/k_{2^\infty n_0}, \mu_{2^\infty}) \\ &\to \bigoplus_{\mathfrak{q} \mid \frac{m_0}{n_0}} H^1(k_{2^\infty m_0,\mathfrak{q}}/k_{2^\infty n_0,\mathfrak{q}}, \mu_{2^\infty})\end{aligned}$$

of abelian groups. It follows from proposition 1 that the kernel of a map

$$\mathrm{Ker}(A^-_{2^\infty n_0} \to A^-_{2^\infty m_0}) \to H^1(k_{2^\infty m_0}/k_{2^\infty n_0}, \mu_{2^\infty})$$

is contained in $A^-_{2^\infty n_0}[2]$ because $m = 2^r m_0$ is not a prime power. Since $\mathrm{Gal}(k_{2^\infty m_0}/k_{2^\infty n_0})$ acts on μ_{2^∞} trivially, one sees that

$$H^1(k_{2^\infty m_0}/k_{2^\infty n_0}, \mu_{2^\infty}) = \mathrm{Hom}(\mathrm{Gal}(k_{2^\infty m_0}/k_{2^\infty n_0}), \mu_{2^\infty}),$$

and that similarly

$$H^1(k_{2^\infty m_0,\mathfrak{q}}/k_{2^\infty n_0,\mathfrak{q}}, \mu_{2^\infty}) = \mathrm{Hom}(\mathrm{Gal}(k_{2^\infty m_0,\mathfrak{q}}/k_{2^\infty n_0,\mathfrak{q}}), \mu_{2^\infty})$$

for each prime $\mathfrak{q}$ with $\mathfrak{q} \mid \frac{m_0}{n_0}$. Let

$$\frac{m_0}{n_0} = \prod_{i=1}^{d} q_i^{a_i}$$

be the prime decomposition of $\frac{m_0}{n_0}$. Then we have a decomposition

$$\mathrm{Gal}(k_{2^\infty m_0}/k_{2^\infty n_0}) = \oplus_{i=1}^{d} \mathrm{Gal}(k_{2^\infty m_0}/k_{2^\infty \frac{m_0}{q_i^{a_i}}})$$

by inertia subgroups $\mathrm{Gal}(k_{2^\infty m_0}/k_{2^\infty \frac{m_0}{q_i^{a_i}}})$ at a prime lying above q_i for all $1 \leq i \leq d$. From the above decomposition of $\mathrm{Gal}(k_{2^\infty m_0}/k_{2^\infty n_0})$, it follows that each element of $\mathrm{Gal}(k_{2^\infty m_0}/k_{2^\infty n_0})$ is a product of elements of decomposition groups. That is, it holds that

$$\mathrm{Gal}(k_{2^\infty m_0}/k_{2^\infty n_0}) = \langle \mathrm{Gal}(k_{2^\infty m_0,\mathfrak{q}}/k_{2^\infty n_0,\mathfrak{q}}) \mid \mathfrak{q} \mid \frac{m_0}{n_0} \rangle$$

Hence one sees that the direct sum of restriction maps

$$\mathrm{Hom}(\mathrm{Gal}(k_{2^\infty m_0}/k_{2^\infty n_0}), \mu_{2^\infty}) \to \oplus_{\mathfrak{q} \mid \frac{m_0}{n_0}} \mathrm{Hom}(\mathrm{Gal}(k_{2^\infty m_0,\mathfrak{q}}/k_{2^\infty n_0,\mathfrak{q}}), \mu_{2^\infty})$$

is injective. Indeed, suppose that $f \in \mathrm{Hom}(\mathrm{Gal}(k_{2^\infty m_0}/k_{2^\infty n_0}), \mu_{2^\infty})$ maps to 0. Then, for each prime $\mathfrak{q}$ and each element $\sigma_\mathfrak{q} \in \mathrm{Gal}(k_{2^\infty m_0,\mathfrak{q}}/k_{2^\infty n_0,\mathfrak{q}})$, it holds that $f(\sigma_\mathfrak{q}) = 1$. As stated in the above, each element $\sigma \in \mathrm{Gal}(k_{2^\infty m_0}/k_{2^\infty n_0})$ can be written as $\sigma = \prod_\mathfrak{q} \sigma_\mathfrak{q}$ for some $\sigma_\mathfrak{q} \in \mathrm{Gal}(k_{2^\infty m_0,\mathfrak{q}}/k_{2^\infty n_0,\mathfrak{q}})$. Thus, we find that $f(\sigma) = \prod_\mathfrak{q} f(\sigma_\mathfrak{q}) = 1$, and hence $f = 0$. Therefore, since

$$\mathrm{Ker}(A^-_{2^\infty n_0} \to A^-_{2^\infty m_0}) \to H^1(k_{2^\infty m_0}/k_{2^\infty n_0}, \mu_{2^\infty})$$

is trivial, we find that $\mathrm{Ker}(A^-_{2^\infty n_0} \to A^-_{2^\infty m_0}) \subseteq A^-_{2^\infty n_0}[2]$ by proposition 1. To finish the proof, we need the following elementary lemma.

Lemma 5. *Let A, B and C be abelian groups and let $f : A \to B$ and $g : B \to C$ be morphisms of groups. If $\mathrm{Ker} f \subseteq A[m]$ and $\mathrm{Ker} g \subseteq B[n]$ for some integers m and n, then $\mathrm{Ker} g \circ f \subseteq A[mn]$.*

Proof. Let $a \in \mathrm{Ker} g \circ f$. Then $g(f(a)) = 0$, and hence $f(a) \in B[n]$. This implies that $0 = nf(a) = f(na)$, and hence $na \in A[m]$. Therefore $(mn)a = 0$. □

Since $\mathrm{Ker}(A^-_{2^t n_0} \to A^-_{2^t m_0}) \subseteq \mathrm{Ker}(A^-_{2^t n_0} \to A^-_{2^\infty m_0})$ and since $A^-_{2^t n_0} \to A^-_{2^\infty n_0}$ is injective, we have $\mathrm{Ker}(A^-_{2^t n_0} \to A^-_{2^t m_0}) \subseteq A^-_{2^t n_0}[2]$ by lemma 5. □

We finish the proof of theorem 2. Suppose that $2 \nmid n$, that is, $n = n_0$. Then it holds that $\mathrm{Ker}(A^-_{n_0} \to A^-_m) \subseteq \mathrm{Ker}(A^-_{n_0} \to A^-_{2^t m_0}) \subseteq A^-_n[4]$ by proposition 2 and lemma 5. Suppose that $4 \mid n$. Recall that $n = 2^s n_0$ with $s \geq 2$. Then it holds that

$$\mathrm{Ker}(A^-_{2^s n_0} \to A^-_m) \subseteq \mathrm{Ker}(A^-_{2^s n_0} \to A^-_{2^t m_0}) \subseteq A^-_n[2] \subseteq A^-_n[4]$$

by proposition 2 and lemma 5. This completes the proof of theorem 2. □

3.3 On finite extensions of imaginary abelian fields.

Proposition 3. *Let p be an odd prime number and m a positive integer. Then there are infinitely many finite extensions K/F of imaginary abelian fields such that* $\mathrm{Ker}(C_F^- \to C_K^-) \simeq \mathbb{Z}/p^m\mathbb{Z}$.

By proposition 3, the assertion of theorem 2 does not hold for finite extensions of imaginary abelian fields.

Proof. Let q_1 and q_2 be distinct prime numbers such that $q_1, q_2 \equiv 1 \bmod p^m$. For $i = 1$ and 2, let L_i be the unique subfield of k_{q_i} of degree p^m. Put $L = L_1 L_2$, and let $M/\mathbb{Q}$ be a cyclic subfield of L of degree p^m and of conductor $q_1 q_2$. Then L/M is an unramified cyclic extension of degree p^m. Put $K = L(\mu_{p^m})$ and $F = M(\mu_{p^m})$. Then K/F is also an unramified cyclic extension of degree p^m since $L \cap k_{p^t} = \mathbb{Q}$ for all non-negative integer t.

By lemma 1, since K/F is a p-extension, we have the following isomorphism

$$\mathrm{Ker}(C_F^- \to C_K^-) \simeq H^1(K/F, \mu_K \otimes \mathbb{Z}_p)$$

of finite abelian groups. Since $K \subseteq \mathbb{Q}(\mu_{q_1 q_2 p^m})$, it follows that

$$\mu_K \otimes \mathbb{Z}_p = \mu_{p^m},$$

and therefore

$$\begin{aligned}\mathrm{Ker}(C_F^- \to C_K^-) &\simeq H^1(K/F, \mu_{p^m}) \\ &= \mathrm{Hom}(\mathrm{Gal}(K/F), \mu_{p^m}) \\ &\simeq \mathbb{Z}/p^m\mathbb{Z}.\end{aligned}$$

This completes the proof. □

4 Proof of theorem 3

We need the following.

Lemma 6. (1) *An abelian group A is divisible if and only if A is p-divisible for all prime numbers p.*
(2) *A countable, torsion divisible abelian group A is isomorphic to $(\mathbb{Q}/\mathbb{Z})^{\oplus \mathbb{N}}$ if and only if, for each prime number p and each positive integer r, A contains a subgroup isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{\oplus r}$.*

Proof. The statement (1) is trivial. For (2), see some references about the structure theorem of divisible groups. For instance, see theorem 23.1 of [5]. □

For the divisibility of C_∞^-, we give a simple proof by using the following celebrated result of Iwasawa theory.

Lemma 7 (Ferrero–Washington [4]). *For each prime number p and each positive integer n, there is a non-negative integer λ_p^- depending only on k_n and p such that*

$$\varinjlim_r C_{p^r n}^- \otimes \mathbb{Z}_p \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^{\oplus \lambda_p^-}$$

as abelian groups.

For each pair of positive integers n and m with $n \mid m$, let $i_{n,m} : C_n^- \to C_m^-$ be the lifting map, and $i_{n,\infty} : C_n^- \to C_\infty^-$ the natural map. Let p be a prime number and $x \in C_\infty^-$. For the p-divisibility, we may assume that the order of x is a p-power. There exist a positive integer n and $x_n \in C_n^-$ such that $i_{n,\infty}(x_n) = x$. By lemma 7, there exist a non-negative integer r and $y_{p^r n} \in C_{p^r n}^-$ such that $i_{n,p^r n}(x_n) = y_{p^r n}^p$. This shows that C_∞^- is p-divisible. By lemma 6, C_∞^- is divisible.

Next, we show that C_∞^- is countable. Let $k_\infty = \cup_n k_n$ be the full cyclotomic field. We shall use a standard argument of Kummer theory. Let

$$M = \{a \otimes 1/r \in k_\infty^\times \otimes \mathbb{Q}/\mathbb{Z} \mid \exists n \text{ s.t. } a \in k_n,\ (a) = I_n^r \text{ for some ideal } I_n \text{ of } k_n\}.$$

We then have a surjective map

$$M \to C_\infty,\ a \otimes 1/r \mapsto i_{n,\infty}([I_n]).$$

Since $k_\infty^\times \otimes \mathbb{Q}/\mathbb{Z}$ is countable, a quotient C_∞^- of C_∞ is also countable. Thus C_∞^- is countable.

Again, let p be a prime number and r a positive integer. By theorem 1, there exists a positive integer n such that C_n^- contains a subgroup isomorphic to $(\mathbb{Z}/4p\mathbb{Z})^{\oplus r}$. By theorem 2, C_∞^- contains a subgroup isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{\oplus r}$. By lemma 6, the assertion of theorem 3 follows. □

Acknowledgments

The author would like to express his thanks to Tetsuya Taniguchi for having interesting conversations with him. The work of this article was motivated from a question of Taniguchi. The author also would like to express his thanks to Miho Aoki for informing improvements of the proof of theorem 2. The author also would like to express his thanks to Tsuyoshi Itoh and Lawrence C. Washington for giving valuable comments. This research was partly supported by JSPS KAKENHI Grant Numbers JP15K04791, JP18K03259.

References

[1] M. Atsuta, Finite Λ-submodules of Iwasawa modules for a CM-field for $p = 2$, J. Théor. Nombres Bordeaux 30 (2018), no. 3, 1017–1035.

[2] A. Brumer, The class group of all cyclotomic integers. J. Pure Appl. Algebra 20 (1981), no. 2, 107–111.

[3] G. Cornell, Abhyankar's lemma and the class group. Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979), pp. 82–88, Lecture Notes in Math., 751, Springer, Berlin, 1979.

[4] B. Ferrero and L. C. Washington, The Iwasawa invariant μ_p vanishes for abelian number fields. Ann. of Math. (2) 109 (1979), no. 2, 377–395.

[5] L. Fuchs, Infinite abelian groups. Vol. I. Pure and Applied Mathematics, Vol. 36 Academic Press, New York-London 1970.

[6] M. Kurihara, On the ideal class groups of the maximal real subfields of number fields with all roots of unity. J. Eur. Math. Soc. (JEMS) 1 (1999), no. 1, 35–49.

[7] R. Okazaki, Inclusion of CM-fields and divisibility of relative class numbers. Acta Arith. 92 (2000), no. 4, 319–338.

[8] M. Ozaki, A note on the capitulation in $\mathbb{Z}_p$-extensions, Proc. Japan Acad. Ser. A Math. Sci. Volume 71, Number 9 (1995), 218–219.

[9] R. Schoof and L. C. Washington, Visibility of ideal classes. J. Number Theory 130 (2010), no. 12, 2715–2731.

[10] L. C. Washington, Introduction to cyclotomic fields. Second edition. Graduate Texts in Mathematics, 83. Springer-Verlag, New York, 1997.