J. Math. Soc. Japan
Vol. 56, No. 3, 2004

Construction of Z_p-extensions with prescribed Iwasawa modules

By Manabu OZAKI

(Received Jun. 3, 2002)
(Revised Mar. 3, 2003)

Abstract. We construct $\boldsymbol{Z}_p$-extensions whose Iwasawa modules have prescribed structure. Specifically, we give a $\boldsymbol{Z}_p$-extension with prescribed finite Iwasawa module. Also we show that there exists a $\boldsymbol{Z}_p$-extension with arbitrarily given Iwasawa μ-invariant. We apply the construction of such $\boldsymbol{Z}_p$-extensions to a certain capitulation problem.

1. Introduction.

Let K/k be a $\boldsymbol{Z}_p$-extension and k_n its n-th layer. The Iwasawa module X_K of the $\boldsymbol{Z}_p$-extension K/k is defined to be the projective limit $\varprojlim A(k_n)$ of the Sylow p-subgroup $A(k_n)$ of the ideal class group of k_n with respect to the norm maps. Otherwise, we can also define X_K to be the Galois group $\mathrm{Gal}(L(K)/K)$ of the maximal unramified pro-p abelian extension $L(K)/K$. Then the completed group ring $\Lambda_{K/k} = \boldsymbol{Z}_p[[\mathrm{Gal}(K/k)]]$ acts on X_K and Iwasawa showed that X_K is a finitely generated torsion $\Lambda_{K/k}$-module. In the arithmetic of the $\boldsymbol{Z}_p$-extension K/k, Iwasawa module X_K plays a crucial role. Iwasawa studied the $\Lambda_{K/k}$-module structure of X_K and deduced the following celebrated formula:

THEOREM (Iwasawa). *There exist non-negative integers* $\lambda(K/k), \mu(K/k)$ *and an integer* $v(K/k)$ *such that*

$$\#A(k_n) = p^{\lambda(K/k)n+\mu(K/k)p^n+v(K/k)}$$

for all sufficiently large n.

Here the integers $\lambda(K/k), \mu(K/k)$ and $v(K/k)$ are called Iwasawa invariants of K/k. We remark that $\lambda(K/k)$ and $\mu(K/k)$ are the invariants of the $\Lambda_{K/k}$-module structure of X_K.

Now we raise the following natural question on the Iwasawa module:

QUESTION A. Let p be a prime number and Γ a topological group isomorphic to $\boldsymbol{Z}_p$. Put $\Lambda = \boldsymbol{Z}_p[[\Gamma]]$. Then, for any finitely generated torsion Λ-module X, does there exist a $\boldsymbol{Z}_p$-extension K/k such that X_K is isomorphic to X as Λ-modules, regarding X_K as a Λ-module via some isomorphism $\mathrm{Gal}(K/k) \simeq \Gamma$?

We also raise the following question, which relates to Question A:

2000 *Mathematics Subject Classification*. Primary 11R23; Secondary 11R29.

Key Words and Phrases. Iwasawa module, Iwasawa invariant, capitulation of ideals.

This research is partially supported by the Grant-in-Aid for Encouragement of Young Scientists, Ministry of Education, Science, Sports and Culture, Japan.

Question B. For any non-negative integers l and m, does there exist a $\boldsymbol{Z}_p$-extension K/k with $\lambda(K/k) = l$ and $\mu(K/k) = m$?

Here we note that if Question A is affirmative, then Question B is also affirmative.

In the present paper, we shall give partial answers to the above questions. Specifically, we shall answer to Question A affirmatively in the case where X is finite (Theorem 1). Also we shall answer to Question B for μ-invariants affirmatively (Theorem 2). In the final section, we shall apply the construction in the proof of Theorem 1 to a certain capitulation problem.

2. Main results.

On Question A, we shall give the following:

Theorem 1. *Let p be a prime number and Γ a topological group isomorphic to $\boldsymbol{Z}_p$. Put $\Lambda = \boldsymbol{Z}_p[[\Gamma]]$. Then for any* finite *$\Lambda$-module X, there exists a cyclotomic $\boldsymbol{Z}_p$-extension K/k over a totally real number field k such that*

$$X_K \simeq X$$

as Λ-modules, regarding X_K as a Λ-module via some isomorphism $\mathrm{Gal}(K/k) \simeq \Gamma$.

Greenberg conjectured that X_K is finite if K/k is the cyclotomic $\boldsymbol{Z}_p$-extension over a totally real number field k (see [**3**]). Therefore, assuming Greenberg's conjecture, Theorem 1 says that among the cyclotomic $\boldsymbol{Z}_p$-extensions over totally real number fields, every possible Λ-module could appear as an Iwasawa module.

On Question B, we shall give the following:

Theorem 2. *Let p be an odd prime number. For any non-negative integer m, there exist a number field k and a $\boldsymbol{Z}_p$-extension K/k with $\mu(K/k) = m$ (and $\lambda(K/k) = 0$), specifically, $X_K \simeq (\Lambda_{K/k}/p)^{\oplus m}$. Furthermore, we can take k to be an imaginary cyclic extension of degree $2p$ over $\boldsymbol{Q}$.*

Iwasawa conjectured that $\mu(K/k) = 0$ for any cyclotomic $\boldsymbol{Z}_p$-extension K/k. This conjecture is valid if the base field k is abelian over $\boldsymbol{Q}$ (the Ferrero-Washington theorem [**1**]). However Iwasawa [**7**] constructed non-cyclotomic $\boldsymbol{Z}_p$-extensions with arbitrarily large μ-invariant. Our method of construction of $\boldsymbol{Z}_p$-extension K/k in Theorem 2 is based on [**7**], hence K/k is a certain non-cyclotomic $\boldsymbol{Z}_p$-extension, so called the anti-cyclotomic $\boldsymbol{Z}_p$-extension.

To prove the theorems, we refine the idea in Yahagi [**13**], in which he constructed number fields with prescribed Sylow p-subgroup of the ideal class group. We extend his method so that we can impose the prescribed Galois module structure on the Sylow p-subgroup of the ideal class group.

3. Proof of Theorem 1.

Since X is finite, X is a $\boldsymbol{Z}/p^{m_0}[\Gamma_{n_0}]$-module for some integers $m_0 \geq 1$ and $n_0 \geq 0$, where $\Gamma_n = \Gamma/\Gamma^{p^n} \simeq \boldsymbol{Z}/p^n$ for $n \geq 0$.

LEMMA 1. *Assume that a $\boldsymbol{Z}_p$-extension K/k satisfies the following three conditions*:

(i) *K/k is totally ramified at every ramified prime.*

(ii) *$A(k_{n_0}) \simeq X$ as Γ_{n_0}-modules, viewing $A(k_{n_0})$ as a Γ_{n_0}-module by some identification* $\mathrm{Gal}(K/k)$ *with Γ.*

(iii) $A(k_{n_0}) \simeq A(k_{n_0+1})$.

Then we have $X_K \simeq X$ as Λ-modules.

PROOF. It follows from assumptions (i), (iii) and Fukuda [**2**] that $X_K \simeq A(k_{n_0})$ as $\Lambda_{K/k}$-modules. Hence the assertion follows from assumption (ii). □

By virtue of Lemma 1, our main aim is to construct a number field with prescribed Sylow p-subgroup of the ideal class group and Galois action on it. Yahagi [**13**] constructed number fields with prescribed Sylow p-subgroup of the ideal class group. We refine his method to construct a desired number field. Outline of the construction is as follows: We construct a cyclic extension $k/\boldsymbol{Q}_N$ of degree p^{m_0} for suitable N, $\boldsymbol{Q}_N$ being the N-th layer of the cyclotomic $\boldsymbol{Z}_p$-extension over $\boldsymbol{Q}$, such that $A(k_{n_0})/(\sigma - 1) \simeq A(k_{n_0+1})/(\sigma - 1) \simeq X$ as Γ-modules (identifying Γ with $\mathrm{Gal}(k_\infty/k)$) by "genus theoretic" method, where k_∞/k is the cyclotomic $\boldsymbol{Z}_p$-extension, k_n $(n \geq 0)$ is its n-th layer and σ is a generator of $\mathrm{Gal}(k_{n_0+1}/\boldsymbol{Q}_{N+n_0+1})$. By selecting the ramified primes of $k/\boldsymbol{Q}_N$ carefully, we can make the ideal classes in $A(k_{n_0+\delta})$ containing σ-invariant ideals generate $A(k_{n_0+\delta})/(\sigma - 1)$ for $\delta = 0, 1$. Hence $A(k_{n_0+\delta}) = A(k_{n_0+\delta})/(\sigma - 1) \simeq X$ for $\delta = 0, 1$ by Nakayama's lemma. Thus the cyclotomic $\boldsymbol{Z}_p$-extension k_∞/k is a desired $\boldsymbol{Z}_p$-extension by Lemma 1.

We fix a topological generator γ_∞ of Γ and put $\gamma_n = \gamma_\infty \bmod \Gamma^{p^n} \in \Gamma_n$. Let

$$r := \dim_{\boldsymbol{F}_p} X/(p, \gamma_{n_0} - 1). \tag{1}$$

Then r is the number of minimal generators of X over $\boldsymbol{Z}/p^{m_0}[\Gamma_{n_0}]$, and there exists an exact sequence of $\boldsymbol{Z}/p^{m_0}[\Gamma_{n_0}]$-modules

$$0 \to R_{n_0} \to \boldsymbol{Z}/p^{m_0}[\Gamma_{n_0}]^{\oplus r} \to X \to 0. \tag{2}$$

Let π'_{n_0+1,n_0} be the natural map from $\boldsymbol{Z}/p^{m_0}[\Gamma_{n_0+1}]^{\oplus r}$ to $\boldsymbol{Z}/p^{m_0}[\Gamma_{n_0}]^{\oplus r}$ induced by the natural projection $\Gamma_{n_0+1} \to \Gamma_{n_0}$, and put $R_{n_0+1} = {\pi'_{n_0+1,n_0}}^{-1}(R_{n_0})$. Then π'_{n_0+1,n_0} induces the isomorphism

$$\boldsymbol{Z}/p^{m_0}[\Gamma_{n_0+1}]^{\oplus r}/R_{n_0+1} \simeq X. \tag{3}$$

We identify $\boldsymbol{Z}/p^{m_0}[\Gamma_{n_0+1}]^{\oplus r}/R_{n_0+1}$ with X via the natural isomorphism (3).

We define the submodule $\tilde{R}_{n_0+\delta}$ $(\delta = 0, 1)$ of $\boldsymbol{Z}/p^{m_0}[\Gamma_{n_0+\delta}]^{\oplus r+1}$ as follows:

$$\tilde{R}_{n_0+\delta} = \left\{ (\alpha_i)_{1 \leq i \leq r+1} \in \boldsymbol{Z}/p^{m_0}[\Gamma_{n_0+\delta}]^{\oplus r+1} \mid (\alpha_i)_{1 \leq i \leq r} \in R_{n_0+\delta}, \alpha_{r+1} \equiv \sum_{i=1}^{r} \alpha_i \pmod{\gamma_{n_0+\delta} - 1} \right\}. \tag{4}$$

We put

$$\tilde{X} = \boldsymbol{Z}/p^{m_0}[\Gamma_{n_0+1}]^{\oplus r+1}/\tilde{R}_{n_0+1}. \tag{5}$$

We remark that there is a natural injection $X \to \tilde{X}$ given by $(x_i)_{1 \le i \le r} \bmod R_{n_0+1} \mapsto (x_1, \dots, x_r, \sum_{i=1}^{r} x_i) \bmod \tilde{R}_{n_0+1}$, whose cokernel is isomorphic to $\boldsymbol{Z}/p^{m_0}$.

Then the natural map $\pi_{n_0+1,n_0} : \boldsymbol{Z}/p^{m_0}[\Gamma_{n_0+1}]^{\oplus r+1} \to \boldsymbol{Z}/p^{m_0}[\Gamma_{n_0}]^{\oplus r+1}$ induced by the projection $\Gamma_{n_0+1} \to \Gamma_{n_0}$ gives the isomorphism

$$\tilde{X} = \boldsymbol{Z}/p^{m_0}[\Gamma_{n_0+1}]^{\oplus r+1}/\tilde{R}_{n_0+1} \simeq \boldsymbol{Z}/p^{m_0}[\Gamma_{n_0}]^{\oplus r+1}/\tilde{R}_{n_0} \tag{6}$$

because $\pi_{n_0+1,n_0}^{-1}(\tilde{R}_{n_0}) = \tilde{R}_{n_0+1}$.

Let g be the number of minimal generators of $\tilde{R}_{n_0+1}$ over $\boldsymbol{Z}/p^{m_0}[\Gamma_{n_0+1}]$, and we choose and fix once for all an integer N with the property

$$p^N - 1 \ge g \quad \text{and} \quad N \ge m_0. \tag{7}$$

Now we shall identify Γ with $\mathrm{Gal}(\boldsymbol{Q}_\infty/\boldsymbol{Q}_N)$ by a fixed isomorphism $\Gamma \simeq \mathrm{Gal}(\boldsymbol{Q}_\infty/\boldsymbol{Q}_N)$, where $\boldsymbol{Q}_\infty$ is the cyclotomic $\boldsymbol{Z}_p$-extension field of $\boldsymbol{Q}$. Then $\Gamma_t = \mathrm{Gal}(\boldsymbol{Q}_{N+t}/\boldsymbol{Q}_N)$ for $t \ge 0$.

Let $\mathfrak{l}_i$ $(1 \le i \le r+1)$ be distinct degree one primes of $\boldsymbol{Q}_N$ which decompose completely in $\boldsymbol{Q}_{N+n_0+1}$, say $\mathfrak{l}_i = \prod_{\gamma \in \Gamma_{n_0+1}} \gamma \mathfrak{L}_{i,n_0+1}$. Furthermore, we assume that $\mathfrak{l}_i$ decomposes completely in $\tilde{\boldsymbol{Q}}_{N+n_0+1} := \boldsymbol{Q}_{N+n_0+1}(\mu_p)$ (if $p \ne 2$) or $\boldsymbol{Q}_{N+n_0+1}(\mu_4)$ (if $p = 2$). Put $\mathfrak{m} = \prod_{i=1}^{r+1} \mathfrak{l}_i$, and denote by $\mathfrak{L}_{i,n_0}$ the prime of $\boldsymbol{Q}_{N+n_0}$ below $\mathfrak{L}_{i,n_0+1}$. For $t \ge 0$, we denote by $L_t/\boldsymbol{Q}_{N+t}$ the maximal abelian p-extension such that the conductor of $L_t/\boldsymbol{Q}_{N+t}$ divides $\mathfrak{m}$ and the exponent of $\mathrm{Gal}(L_t/\boldsymbol{Q}_{N+t})$ is less than or equal to p^{m_0}. Since the class number of $\boldsymbol{Q}_{N+n_0+\delta}$ is prime to p as well known, we get the exact sequence of Γ-modules

$$\mathcal{O}_{N+n_0+\delta}^\times/p^{m_0} \xrightarrow{\rho_{n_0+\delta}} (\mathcal{O}_{N+n_0+\delta}/\mathfrak{m})^\times/p^{m_0} \xrightarrow{r_{n_0+\delta}} \mathrm{Gal}(L_{n_0+\delta}/\boldsymbol{Q}_{N+n_0+\delta}) \to 0, \tag{8}$$

for $\delta = 0, 1$ by class field theory, where $\mathcal{O}_{N+n_0+\delta}$ denotes the ring of integers of $\boldsymbol{Q}_{N+n_0+\delta}$, $\rho_{n_0+\delta}$ is the natural map, and $r_{n_0+\delta}$ is the map induced by the reciprocity map. We can see that the middle term $(\mathcal{O}_{N+n_0+\delta}/\mathfrak{m})^\times/p^{m_0}$ of (8) is isomorphic to $\boldsymbol{Z}_p[\Gamma_{n_0+\delta}]^{\oplus r+1}$ via the following map:

$$(\mathcal{O}_{N+n_0+\delta}/\mathfrak{m})^\times/p^{m_0} \simeq \boldsymbol{Z}/p^{m_0}[\Gamma_{n_0+\delta}]^{\oplus r+1}, \tag{9}$$

$$\text{the class of } \alpha \mapsto \left(\sum_{\gamma \in \Gamma_{n_0+\delta}} \varphi\left(\left(\frac{\alpha}{\tilde{\gamma}\tilde{\mathfrak{L}}_{i,n_0+\delta}} \right)_{n_0+\delta} \right) \gamma \right)_{1 \le i \le r+1}.$$

Notations in (9) are as follows: $\tilde{\gamma} \in \mathrm{Gal}(\tilde{\boldsymbol{Q}}_{N+n_0+\delta}/\tilde{\boldsymbol{Q}}_N)$ is the image of γ via the natural isomorphism $\Gamma_{n_0+\delta} \simeq \mathrm{Gal}(\tilde{\boldsymbol{Q}}_{N+n_0+\delta}/\tilde{\boldsymbol{Q}}_N)$, where $\tilde{\boldsymbol{Q}}_{N+n_0+\delta} = \boldsymbol{Q}_{N+n_0+\delta}(\mu_p)$ (if $p \ne 2$) or $\boldsymbol{Q}_{N+n_0+\delta}(\mu_4)$ (if $p = 2$). $\tilde{\mathfrak{L}}_{i,n_0+1}$ are fixed primes of $\tilde{\boldsymbol{Q}}_{N+n_0+1}$ lying above $\mathfrak{L}_{i,n_0+1}$, and $\tilde{\mathfrak{L}}_{i,n_0}$ is the prime of $\tilde{\boldsymbol{Q}}_{N+n_0}$ below $\tilde{\mathfrak{L}}_{i,n_0+1}$. $(*/*)_{n_0+\delta} \in \mu_{p^{m_0}}$ is the p^{m_0}-th power residue symbol for $\tilde{\boldsymbol{Q}}_{N+n_0+\delta}$. φ is a fixed isomorphism $\mu_{p^{m_0}} \simeq \boldsymbol{Z}/p^{m_0}$. Here we note that $\mu_{p^{m_0}} \subseteq \tilde{\boldsymbol{Q}}_N$ by (7) hence $(\alpha/\tilde{\gamma}\tilde{\mathfrak{L}}_{i,n_0+\delta})_{n_0+\delta} = (\gamma^{-1}\alpha/\tilde{\mathfrak{L}}_{i,n_0+\delta})_{n_0+\delta}$, and that $\mathcal{O}_{N+n_0+\delta}/\gamma\mathfrak{L}_{i,n_0+\delta} \simeq \tilde{\mathcal{O}}_{N+n_0+\delta}/\tilde{\gamma}\tilde{\mathfrak{L}}_{i,n_0+\delta}$, $\tilde{\mathcal{O}}_{N+n_0+\delta}$ being the ring of integers of $\tilde{\boldsymbol{Q}}_{N+n_0+\delta}$, since $\mathfrak{l}_i$ decomposes completely in $\tilde{\boldsymbol{Q}}_{N+n_0+1}$.

In what follows we fix $\tilde{\mathfrak{L}}_{i,n_0+1}$ and φ once for all and identify $(\mathcal{O}_{N+n_0+\delta}/\mathfrak{m})^\times/p^{m_0}$ with $\boldsymbol{Z}/p^{m_0}[\Gamma_{n_0+\delta}]^{\oplus r+1}$ via the above isomorphism. Then we get the exact sequence

$$\mathcal{O}_{N+n_0+\delta}^\times/p^{m_0} \xrightarrow{\rho_{n_0+\delta}} \boldsymbol{Z}/p^{m_0}[\Gamma_{n_0+\delta}]^{\oplus r+1} \xrightarrow{r_{n_0+\delta}} \mathrm{Gal}(L_{n_0+\delta}/\boldsymbol{Q}_{N+n_0+\delta}) \to 0, \tag{10}$$

from (8), and the map $\rho_{n_0+\delta}$ is given by

$$\rho_{n_0+\delta}(\varepsilon) = \left(\sum_{\gamma \in \Gamma_{n_0+\delta}} \varphi \left(\left(\frac{\varepsilon}{\tilde{\gamma} \tilde{\mathfrak{Q}}_{i, n_0+\delta}} \right)_{n_0+\delta} \right) \gamma \right)_{1 \le i \le r+1}. \tag{11}$$

It follows from (7) that $\mu_{2^{m_0+1}} \subseteq \tilde{\boldsymbol{Q}}_{N+n_0+\delta}$ when $p=2$. Hence $\rho_{n_0+\delta}(-1)=0$ for any prime number p by (11) since $-1 \in (\mu_{2^{m_0+1}})^{2^{m_0}}$ when $p=2$. From exact sequences (10) for $\delta = 0,1$ and the fact that $\rho_{n_0+\delta}(-1)=0$, we get the following exact commutative diagram:

$$\begin{array}{ccccccc}
\overline{\mathcal{O}_{N+n_0+1}^{\times}}/p^{m_0} & \xrightarrow{\rho_{n_0+1}} & \boldsymbol{Z}/p^{m_0}[\Gamma_{n_0+1}]^{\oplus r+1} & \xrightarrow{r_{n_0+1}} & \mathrm{Gal}(L_{n_0+1}/\boldsymbol{Q}_{N+n_0+1}) & \longrightarrow & 0 \\
{\scriptstyle N_{n_0+1,n_0}} \downarrow & & {\scriptstyle \pi_{n_0+1,n_0}} \downarrow & & {\scriptstyle \mathrm{res}_{n_0+1,n_0}} \downarrow & & \\
\overline{\mathcal{O}_{N+n_0}^{\times}}/p^{m_0} & \xrightarrow{\rho_{n_0}} & \boldsymbol{Z}/p^{m_0}[\Gamma_{n_0}]^{\oplus r+1} & \xrightarrow{r_{n_0}} & \mathrm{Gal}(L_{n_0}/\boldsymbol{Q}_{N+n_0}) & \longrightarrow & 0,
\end{array} \tag{12}$$

where $\overline{\mathcal{O}_{N+n_0+\delta}^{\times}} = \mathcal{O}_{N+n_0+\delta}^{\times}/\{\pm 1\}$ for $\delta = 0,1$, N_{n_0+1,n_0} is the norm map from $\boldsymbol{Q}_{N+n_0+1}$ to $\boldsymbol{Q}_{N+n_0}$, π_{n_0+1,n_0} is the map induced by the natural projection $\Gamma_{n_0+1} \to \Gamma_{n_0}$, and res_{n_0+1,n_0} is the restriction map (Note that $L_{n_0} \subseteq L_{n_0+1}$). Commutativity follows from the fact $\tilde{\mathfrak{Q}}_{i,n_0+1} | \tilde{\mathfrak{Q}}_{i,n_0}$ and the properties of the p^{m_0}-th power residue symbol and the reciprocity map.

LEMMA 2. (i) *For any* $t \geq 0$, *we have*

$$\overline{\mathcal{O}_{N+t}^{\times}}/p^{m_0} \simeq \boldsymbol{Z}/p^{m_0}[\Gamma_t]^{\oplus p^N - 1} \oplus \boldsymbol{Z}/p^{m_0}[\Gamma_t]/N_{\Gamma_t},$$

as $\boldsymbol{Z}/p^{m_0}[\Gamma_t]$*-modules, where* $N_{\Gamma_t} = \sum_{\gamma \in \Gamma_t} \gamma$.

(ii) *In commutative diagram* (12), *the norm map* $N_{n_0+1,n_0} : \overline{\mathcal{O}_{N+n_0+1}^{\times}}/p^{m_0} \to \overline{\mathcal{O}_{N+n_0}^{\times}}/p^{m_0}$ *is surjective.*

PROOF. Let $\eta = N_{\boldsymbol{Q}(\mu_{p^{N+t+1}})/\boldsymbol{Q}_{N+t}}(\zeta_{p^{N+t+1}} - 1)^{\sigma - 1}$ (when $p \neq 2$), or $\eta = \zeta_{2^{N+t+2}}^{-2} \cdot ((\zeta_{2^{N+t+2}}^5 - 1)/(\zeta_{2^{N+t+2}} - 1))$ (when $p=2$), where σ is a generator of $\mathrm{Gal}(\boldsymbol{Q}_{N+t}/\boldsymbol{Q})$ and ζ_d denotes a primitive d-th root of unity for $d \geq 1$. Then

$$C_{N+t} = \langle -1, \tau\eta \mid \tau \in \mathrm{Gal}(\boldsymbol{Q}_{N+t}/\boldsymbol{Q}) \rangle$$

is the group of cyclotomic units of $\boldsymbol{Q}_{N+t}$ and $p \nmid [\mathcal{O}_{N+t}^{\times} : C_{N+t}]$ (for the various properties of the cyclotomic unit group, see [**12**, Chapter 8] for example). Hence $\overline{\mathcal{O}_{N+t}^{\times}}/p^{m_0} \simeq (C_{N+t}/\{\pm 1\})/p^{m_0}$. Because

$$C_{N+t}/\{\pm 1\} \simeq \boldsymbol{Z}[\mathrm{Gal}(\boldsymbol{Q}_{N+t}/\boldsymbol{Q})]/N_{\mathrm{Gal}(\boldsymbol{Q}_{N+t}/\boldsymbol{Q})},$$

as $\mathrm{Gal}(\boldsymbol{Q}_{N+t}/\boldsymbol{Q})$-modules and

$$\boldsymbol{Z}[\mathrm{Gal}(\boldsymbol{Q}_{N+t}/\boldsymbol{Q})] = \bigoplus_{\tau \in \mathrm{Gal}(\boldsymbol{Q}_{N+t}/\boldsymbol{Q})/\Gamma_t} \boldsymbol{Z}[\Gamma_t]\tau,$$

we can see that $C_{N+t}/\{\pm 1\} \simeq \boldsymbol{Z}[\Gamma_t]^{\oplus p^N - 1} \oplus \boldsymbol{Z}[\Gamma_t]/N_{\Gamma_t}$. Thus we have proved assertion (i).

Assertion (ii) follows from $\overline{\mathcal{O}_{N+n_0+\delta}^{\times}}/p^{m_0} \simeq (C_{N+n_0+\delta}/\{\pm 1\})/p^{m_0}$ and the fact that the norm map $N_{n_0+1,n_0} : C_{N+n_0+1}/\{\pm 1\} \to C_{N+n_0}/\{\pm 1\}$ is surjective. □

Lemma 3. *For any Γ_{n_0+1}-homomorphism $f:\overline{\mathcal{O}_{N+n_0+1}^\times}/p^{m_0}\to \boldsymbol{Z}/p^{m_0}[\Gamma_{n_0+1}]$, there exist infinitely many degree one primes $\tilde{\mathfrak{L}}$ of $\tilde{\boldsymbol{Q}}_{N+n_0+1}$ such that*

$$f(\varepsilon)=\sum_{\gamma\in\Gamma_{n_0+1}}\varphi\left(\left(\frac{\varepsilon}{\tilde{\gamma}\tilde{\mathfrak{L}}}\right)_{n_0+1}\right)\gamma,$$

for any $\varepsilon\in\overline{\mathcal{O}_{N+n_0+1}^\times}/p^{m_0}$, where the notations in the above are as in (9). *Furthermore, for any fixed finite abelian extension $M/\tilde{\boldsymbol{Q}}_{N+n_0+1}$ with $M\cap\tilde{\boldsymbol{Q}}_{N+n_0+1}(\sqrt[p^{m_0}]{\mathcal{O}_{N+n_0+1}^\times})=\tilde{\boldsymbol{Q}}_{N+n_0+1}$ and $\tau\in\mathrm{Gal}(M/\tilde{\boldsymbol{Q}}_{N+n_0+1})$, we can impose the condition*

$$\left(\frac{M/\tilde{\boldsymbol{Q}}_{N+n_0+1}}{\tilde{\mathfrak{L}}}\right)=\tau$$

on $\tilde{\mathfrak{L}}$.

Proof. From Lemma 2 (i), there exist $\varepsilon_j,\xi\in\mathcal{O}_{N+n_0+1}^\times$ $(1\le j\le p^N-1)$ such that

$$\overline{\mathcal{O}_{N+n_0+1}^\times}/p^{m_0}=\bigoplus_{j=1}^{p^N-1}\boldsymbol{Z}/p^{m_0}[\Gamma_{n_0+1}]\bar{\varepsilon}_j\oplus(\boldsymbol{Z}/p^{m_0}[\Gamma_{n_0+1}]/N_{\Gamma_{n_0+1}})\bar{\xi},\tag{13}$$

where $\bar{\varepsilon}_j,\bar{\xi}\in\overline{\mathcal{O}_{N+n_0+1}^\times}/p^{m_0}$ are the classes of ε_j and ξ, respectively.

Assume that $f(\varepsilon_j)=\sum_{\gamma\in\Gamma_{n_0+1}}c_{j,\gamma}\gamma$ and $f(\xi)=\sum_{\gamma\in\Gamma_{n_0+1}}d_\gamma\gamma$. We shall show that there exist infinitely many degree one primes $\tilde{\mathfrak{L}}$ of $\tilde{\boldsymbol{Q}}_{N+n_0+1}$ such that

$$\begin{aligned}&\left(\frac{\varepsilon_j}{\tilde{\gamma}\tilde{\mathfrak{L}}}\right)_{n_0+1}=\varphi^{-1}(c_{j,\gamma})\quad(1\le j\le p^N-1,\gamma\in\Gamma_{n_0+1}),\\&\left(\frac{\xi}{\tilde{\gamma}\tilde{\mathfrak{L}}}\right)_{n_0+1}=\varphi^{-1}(d_\gamma)\quad(\gamma\in\Gamma_{n_0+1}-\{1\}).\end{aligned}\tag{14}$$

We note that if the above conditions hold, then the condition

$$\left(\frac{\xi}{\tilde{\mathfrak{L}}}\right)_{n_0+1}=\varphi^{-1}(d_1)$$

also holds, because $\prod_{\gamma\in\Gamma_{n_0+1}}(\xi/(\tilde{\gamma}\tilde{\mathfrak{L}}))_{n_0+1}=(\prod_{\gamma\in\Gamma_{n_0+1}}\gamma\xi/\tilde{\mathfrak{L}})_{n_0+1}=1$ and $\sum_{\gamma\in\Gamma_{n_0+1}}d_\gamma=0$. We also note that

$$\left(\frac{\varepsilon}{\tilde{\gamma}\tilde{\mathfrak{L}}}\right)_{n_0+1}=\left(\frac{\tilde{\boldsymbol{Q}}_{N+n_0+1}(\sqrt[p^{m_0}]{\tilde{\gamma}^{-1}\varepsilon})/\tilde{\boldsymbol{Q}}_{N+n_0+1}}{\tilde{\mathfrak{L}}}\right)(\sqrt[p^{m_0}]{\tilde{\gamma}^{-1}\varepsilon})/(\sqrt[p^{m_0}]{\tilde{\gamma}^{-1}\varepsilon})\tag{15}$$

for any $\varepsilon\in\mathcal{O}_{N+n_0+1}^\times$.

We need the following lemma:

Lemma 4. *The natural map $\overline{\mathcal{O}_{N+n_0+1}^\times}/p^{m_0}\to\tilde{\mathcal{O}}_{N+n_0+1}^\times/p^{m_0}$ is injective* (*note that $-1\in(\tilde{\mathcal{O}}_{N+n_0+1}^\times)^{p^{m_0}}$*).

Proof. From the exact sequence

$$0\longrightarrow\mu_{p^{m_0}}\longrightarrow\tilde{\boldsymbol{Q}}_{N+n_0+1}^\times\xrightarrow{p^{m_0}}(\tilde{\boldsymbol{Q}}_{N+n_0+1}^\times)^{p^{m_0}}\longrightarrow 0,$$

we get the exact $G = \mathrm{Gal}(\tilde{\boldsymbol{Q}}_{N+n_0+1}/\boldsymbol{Q}_{N+n_0+1})$-cohomology sequence

$$\boldsymbol{Q}_{N+n_0+1}^{\times} \xrightarrow{p^{m_0}} (\tilde{\boldsymbol{Q}}_{N+n_0+1}^{\times})^{p^{m_0}} \cap \boldsymbol{Q}_{N+n_0+1} \longrightarrow H^1(G, \mu_{p^{m_0}}) \longrightarrow 0.$$

If $p \neq 2$, $H^1(G, \mu_{p^{m_0}}) = 0$ since $\# G$ is prime to p. Hence we have $(\tilde{\boldsymbol{Q}}_{N+n_0+1}^{\times})^{p^{m_0}} \cap \boldsymbol{Q}_{N+n_0+1} = (\boldsymbol{Q}_{N+n_0+1}^{\times})^{p^{m_0}}$. Therefore the assertion of the lemma follows.

We assume that $p = 2$. Then we can see $H^1(G, \mu_{2^{m_0}}) \simeq \boldsymbol{Z}/2$. Hence we have $((\tilde{\boldsymbol{Q}}_{N+n_0+1}^{\times})^{2^{m_0}} \cap \boldsymbol{Q}_{N+n_0+1})/(\boldsymbol{Q}_{N+n_0+1}^{\times})^{2^{m_0}} \simeq \boldsymbol{Z}/2$. Since $-1 \in (\tilde{\boldsymbol{Q}}_{N+n_0+1}^{\times})^{2^{m_0}} - (\boldsymbol{Q}_{N+n_0+1}^{\times})^{2^{m_0}}$, the kernel of the natural map $\mathcal{O}_{N+n_0+1}^{\times}/2^{m_0} \to \tilde{\mathcal{O}}_{N+n_0+1}^{\times}/2^{m_0}$, which is contained in $((\tilde{\boldsymbol{Q}}_{N+n_0+1}^{\times})^{2^{m_0}} \cap \boldsymbol{Q}_{N+n_0+1})/(\boldsymbol{Q}_{N+n_0+1}^{\times})^{2^{m_0}}$, is generated by the class of -1. Thus we also obtain the lemma in the case $p = 2$. □

Proof of Lemma 3. Put $F_j = \tilde{\boldsymbol{Q}}_{N+n_0+1}(\sqrt[p^{m_0}]{\tilde{\gamma}^{-1}\varepsilon_j} \mid \gamma \in \Gamma_{n_0+1})$ and $E = \tilde{\boldsymbol{Q}}_{N+n_0+1} \cdot (\sqrt[p^{m_0}]{\tilde{\gamma}^{-1}\xi} \mid \gamma \in \Gamma_{n_0+1})$. Then it follows from Lemma 4 and (13) that the abelian extensions $F_j/\tilde{\boldsymbol{Q}}_{N+n_0+1}$ $(1 \leq j \leq p^N - 1)$ and $E/\tilde{\boldsymbol{Q}}_{N+n_0+1}$ are independent, and that

$$\mathrm{Gal}(F_j/\tilde{\boldsymbol{Q}}_{N+n_0+1}) \simeq \bigoplus_{\gamma \in \Gamma_{n_0+1}} \mu_{p^{m_0}}, \quad \sigma \mapsto (\sigma(\sqrt[p^{m_0}]{\tilde{\gamma}^{-1}\varepsilon_j})/\sqrt[p^{m_0}]{\tilde{\gamma}^{-1}\varepsilon_j})_{\gamma \in \Gamma_{n_0+1}},$$

$$\mathrm{Gal}(E/\tilde{\boldsymbol{Q}}_{N+n_0+1}) \simeq \bigoplus_{\gamma \in \Gamma_{n_0+1} - \{1\}} \mu_{p^{m_0}}, \quad \sigma \mapsto (\sigma(\sqrt[p^{m_0}]{\tilde{\gamma}^{-1}\xi})/\sqrt[p^{m_0}]{\tilde{\gamma}^{-1}\xi})_{\gamma \in \Gamma_{n_0+1} - \{1\}}.$$

Therefore, by the Čebotarev density theorem and (15), there exist infinitely many degree one primes of $\tilde{\boldsymbol{Q}}_{N+n_0+1}$ satisfying (14). Furthermore, we can impose the condition

$$\left(\frac{M/\tilde{\boldsymbol{Q}}_{N+n_0+1}}{\tilde{\mathfrak{L}}}\right) = \tau$$

on $\tilde{\mathfrak{L}}$, since $M \cap \tilde{\boldsymbol{Q}}_{N+n_0+1}(\sqrt[p^{m_0}]{\mathcal{O}_{N+n_0+1}^{\times}}) = \tilde{\boldsymbol{Q}}_{N+n_0+1}$. □

Now we choose the primes $\tilde{\mathfrak{L}}_{i,n_0+1}$ and $\mathfrak{l}_i$. From (7) and Lemma 2 (i), there exists a Γ_{n_0+1}-homomorphism $h : \overline{\mathcal{O}_{N+n_0+1}^{\times}}/p^{m_0} \to \boldsymbol{Z}/p^{m_0}[\Gamma_{n_0+1}]^{\oplus r+1}$ such that $\mathrm{Im}(h) = \tilde{R}_{n_0+1}$. Assume the following condition on the primes $\tilde{\mathfrak{L}}_{i,n_0+1}$ $(1 \leq i \leq r+1)$:

Condition A.

$$\mathrm{pr}_i \circ h = \sum_{\gamma \in \Gamma_{n_0+1}} \varphi\left(\left(\frac{*}{\tilde{\gamma}\tilde{\mathfrak{L}}_{i,n_0+1}}\right)_{n_0+1}\right)\gamma$$

for $1 \leq i \leq r+1$, where $\mathrm{pr}_i : \boldsymbol{Z}/p^{m_0}[\Gamma_{n_0+1}]^{\oplus r+1} \to \boldsymbol{Z}/p^{m_0}[\Gamma_{n_0+1}]$ denotes the projection map to the i-th component.

By virtue of Lemma 3, there exist degree one primes $\tilde{\mathfrak{L}}_{i,n_0+1}$ of $\tilde{\boldsymbol{Q}}_{N+n_0+1}$ satisfying Condition A such that $\tilde{\mathfrak{L}}_{i,n_0+1}$'s are lying over distinct rational primes. We choose the prime of $\boldsymbol{Q}_N$ (resp. $\boldsymbol{Q}_{N+n_0+\delta}$) below $\tilde{\mathfrak{L}}_{i,n_0+1}$ as $\mathfrak{l}_i$ (resp. $\mathfrak{L}_{i,n_0+\delta}$ $(\delta = 0, 1)$), and put $\mathfrak{m} = \prod_{i=1}^{r+1} \mathfrak{l}_i$. Then we have $\mathrm{Im}(\rho_{n_0+1}) = \mathrm{Im}(h) = \tilde{R}_{n_0+1}$ by (11), hence r_{n_0+1} induces the isomorphism

$$\tilde{X} = \boldsymbol{Z}/p^{m_0}[\Gamma_{n_0+1}]^{\oplus r+1}/\tilde{R}_{n_0+1} \simeq \mathrm{Gal}(L_{n_0+1}/\boldsymbol{Q}_{N+n_0+1}). \tag{16}$$

Also we have

$$\text{(17)} \qquad \mathrm{Gal}(L_{n_0+1}/\boldsymbol{Q}_{N+n_0+1}) \simeq \mathrm{Gal}(L_{n_0}/\boldsymbol{Q}_{N+n_0}),$$

because $\mathrm{Im}(\rho_{n_0}) = \tilde{R}_{n_0}$ and $\mathrm{Gal}(L_{n_0}/\boldsymbol{Q}_{N+n_0}) \simeq \boldsymbol{Z}[\Gamma_{n_0}]^{\oplus r+1}/\tilde{R}_{n_0} \simeq \tilde{X}$ by Lemma 2 (ii), commutative diagram (12), and the fact $\tilde{R}_{n_0+1} = \pi^{-1}_{n_0+1,n_0}(\tilde{R}_{n_0})$. We identify $\mathrm{Gal}(L_{n_0+1}/\boldsymbol{Q}_{N+n_0+1})$ with $\tilde{X}$ via the isomorphism (16).

We regard $X = \boldsymbol{Z}/p^{m_0}[\Gamma_{n_0+1}]^{\oplus r}/R_{n_0+1}$ as a submodule of $\tilde{X} = \boldsymbol{Z}/p^{m_0}[\Gamma_{n_0+1}]^{\oplus r+1}/\tilde{R}_{n_0+1}$ via the embedding $(x_i)_{1\le i\le r} \bmod R_{n_0+1} \mapsto (x_1,\dots,x_r,\sum_{i=1}^r x_i) \bmod \tilde{R}_{n_0+1}$. We define F to be the intermediate field of $L_{n_0+1}/\boldsymbol{Q}_{N+n_0+1}$ with

$$\text{(18)} \qquad X = \mathrm{Gal}(L_{n_0+1}/F).$$

Lemma 5. (i) *There exists the unique cyclic extension $k/\boldsymbol{Q}_N$ of degree p^{m_0} with conductor dividing $\mathfrak{m}$ such that $F = k_{n_0+1} (= k\boldsymbol{Q}_{N+n_0+1})$.*

(ii) *Primes $\gamma\mathfrak{L}_{i,n_0+\delta}$ $(\gamma \in \Gamma_{n_0+\delta}, 1 \le i \le r+1)$ are totally ramified in $k_{n_0+\delta}/\boldsymbol{Q}_{N+n_0+\delta}$. Also primes $\mathfrak{l}_i$ $(1 \le i \le r+1)$ are totally ramified in k.*

(iii) *$L_{n_0+\delta}$ is the genus p-class field of $k_{n_0+\delta}/\boldsymbol{Q}_{N+n_0+\delta}$ for $\delta = 0,1$.*

Proof. (i) Since $\tilde{X}/X$ is generated by the class of $(0,\dots 0,1)$, $\mathrm{Gal}(F/\boldsymbol{Q}_{N+n_0+1}) \simeq \tilde{X}/X \simeq \boldsymbol{Z}/p^{m_0}$ with trivial Γ_{n_0+1}-action. Hence $F/\boldsymbol{Q}_N$ is an abelian extension and $\mathrm{Gal}(F/\boldsymbol{Q}_N) = \mathrm{Gal}(F/\boldsymbol{Q}_{N+n_0+1}) \times I_p$, where $I_p \subseteq \mathrm{Gal}(F/\boldsymbol{Q}_N)$ is the inertia subgroup for the unique prime of $\boldsymbol{Q}_N$ lying over p. Let k be the fixed field of I_p. Then k is the desired field.

(ii) In (12), the inertia subgroup of $\mathrm{Gal}(L_{n_0+1}/\boldsymbol{Q}_{N+n_0+1})$ for $\gamma\mathfrak{L}_{i,n_0+1}$ is generated by $r_{n_0+1}((0,\dots,\overset{i}{\check{\gamma}}\dots,0))$ over $\boldsymbol{Z}/p^{m_0}$. One can easily see that the order of $(0,\dots,\overset{i}{\check{\gamma}}\dots,0) \bmod \tilde{R}_{n_0+1}$ is p^{m_0} and that $\boldsymbol{Z}/p^{m_0}((0,\dots,\overset{i}{\check{\gamma}}\dots,0) \bmod \tilde{R}_{n_0+1}) \cap X = 0$. Hence the prime $\gamma\mathfrak{L}_{i,n_0+1}$ is totally ramified in $k_{n_0+1}/\boldsymbol{Q}_{N+n_0+1}$ and L_{n_0+1}/k_{n_0+1} is an unramified extension. The remaining assertions follow from this fact because $k_{n_0+1} = k_{n_0}\boldsymbol{Q}_{N+n_0+1} = k\boldsymbol{Q}_{N+n_0+1}$.

(iii) Let L' be the genus p-class field of $k_{n_0+1}/\boldsymbol{Q}_{N+n_0+1}$. Then $L_{n_0+1} \subseteq L'$ since L_{n_0+1}/k_{n_0+1} is an unramified abelian p-extension and $L_{n_0+1}/\boldsymbol{Q}_{N+n_0+1}$ is abelian. Now we show $L' \subseteq L_{n_0+1}$. Since the class number of $\boldsymbol{Q}_{N+n_0+1}$ is prime to p, $\mathrm{Gal}(L'/k_{n_0+1})$ is annihilated by $p^{m_0} = [k_{n_0+1} : \boldsymbol{Q}_{N+n_0+1}]$. Since the prime $\mathfrak{L}_{i,n_0+1}$ is totally ramified in $k_{n_0+1}/\boldsymbol{Q}_{N+n_0+1}$, we have $\mathrm{Gal}(L'/\boldsymbol{Q}_{N+n_0+1}) \simeq \mathrm{Gal}(L'/k_{n_0+1}) \times \mathrm{Gal}(k_{n_0+1}/\boldsymbol{Q}_{N+n_0+1})$. Hence $\mathrm{Gal}(L'/\boldsymbol{Q}_{N+n_0+1})$ is annihilated by p^{m_0}. Since the conductor of $L'/\boldsymbol{Q}_{N+n_0+1}$ divides $\mathfrak{m}$, we obtain $L' \subseteq L_{n_0+1}$. Thus we have shown that L_{n_0+1} is the genus p-class field of k_{n_0+1}. The assertion for L_{n_0} also follows by the same argument. □

It follows from Lemmas 1, 5, (18), and (17) that if $L_{n_0+\delta}$ is the Hilbert p-class field of $k_{n_0+\delta}$ for $\delta = 0,1$, the cyclotomic $\boldsymbol{Z}_p$-extension over k is a desired $\boldsymbol{Z}_p$-extension.

Let $H^{(p)}_{n_0+\delta}$ be the Hilbert p-class field of $k_{n_0+\delta}$ for $\delta = 0,1$ and σ a generator of $\mathrm{Gal}(k_{n_0+1}/\boldsymbol{Q}_{N+n_0+1})$. Then we have

$$\text{(19)} \qquad \mathrm{Gal}(L_{n_0+1}/k_{n_0+1}) \simeq \mathrm{Gal}(H^{(p)}_{n_0+1}/k_{n_0+1})/(\sigma-1),$$

by Lemma 5 (iii). Denote by $\bar{\mathfrak{L}}_{i,n_0+1}$ the unique prime of k_{n_0+1} lying over $\mathfrak{L}_{i,n_0+1}$ (Lemma 5 (ii)). If $\{(\bar{\mathfrak{L}}_{i,n_0+1}, L_{n_0+1}/k_{n_0+1}) \mid 1 \le i \le r+1\}$ generates $\mathrm{Gal}(L_{n_0+1}/k_{n_0+1})$

over $\boldsymbol{Z}/p^{m_0}[\Gamma_{n_0+1}]$, then $L_{n_0+1} = H_{n_0+1}^{(p)}$ by (19) and Nakayama's lemma because $\gamma\bar{\mathfrak{L}}_{i,n_0+1}$ $(\gamma \in \Gamma_{n_0+1}, 1 \le i \le r+1)$ is invariant under the action of σ. Since $H_{n_0}^{(p)}k_{n_0+1} \subseteq H_{n_0+1}^{(p)}$ and $L_{n_0+1} = L_{n_0}k_{n_0+1}$ by (17), if $L_{n_0+1} = H_{n_0+1}^{(p)}$ holds then $L_{n_0} = H_{n_0}^{(p)}$ also holds.

Lemma 6. *The restriction induces the isomorphisms*

$$\mathrm{Gal}(L_{n_0+1}/\boldsymbol{Q}_{N+n_0+1})_{\Gamma_{n_0+1}} \simeq \mathrm{Gal}(L_0/\boldsymbol{Q}_N)$$

and

$$\mathrm{Gal}(L_{n_0+1}/k_{n_0+1})_{\Gamma_{n_0+1}} \simeq \mathrm{Gal}(L_0/k).$$

Proof. Let M be the intermediate field of $L_{n_0+1}/\boldsymbol{Q}_{N+n_0+1}$ with $\mathrm{Gal}(L_{n_0+1}/M) = (\gamma_{n_0+1}-1)\,\mathrm{Gal}(L_{n_0+1}/\boldsymbol{Q}_{N+n_0+1})$, γ_{n_0+1} being a generator of Γ_{n_0+1}.

Then $\mathrm{Gal}(L_{n_0+1}/\boldsymbol{Q}_{N+n_0+1})_{\Gamma_{n_0+1}} = \mathrm{Gal}(M/\boldsymbol{Q}_{N+n_0+1})$ and $M/\boldsymbol{Q}_N$ is an abelian extension. It is obvious that $L_0\boldsymbol{Q}_{N+n_0+1} \subseteq M$. Let $I_p \subseteq \mathrm{Gal}(M/\boldsymbol{Q}_N)$ be the inertia subgroup for the unique prime of $\boldsymbol{Q}_N$ lying over p. Then $\mathrm{Gal}(M/\boldsymbol{Q}_N) = \mathrm{Gal}(M/\boldsymbol{Q}_{N+n_0+1}) \times I_p$ and the fixed field of I_p is contained in L_0. Therefore we have $L_0\boldsymbol{Q}_{N+n_0+1} = M$ and $\mathrm{Gal}(L_{n_0+1}/\boldsymbol{Q}_{N+n_0+1})_{\Gamma_{n_0+1}} \simeq \mathrm{Gal}(L_0/\boldsymbol{Q}_N)$ since $L_0 \cap \boldsymbol{Q}_{N+n_0+1} = \boldsymbol{Q}_N$.

To show the second assertion, it is enough to show $(\gamma_{n_0+1}-1)X = (\gamma_{n_0+1}-1)\tilde{X}$ because $(\gamma_{n_0+1}-1)\tilde{X} = \mathrm{Gal}(L_{n_0+1}/L_0\boldsymbol{Q}_{N+n_0+1})$ by the first assertion. Let $\overline{(x_i)} \in \tilde{X} = \boldsymbol{Z}/p^{m_0}[\Gamma_{n_0+1}]^{\oplus r+1}/\tilde{R}_{n_0+1}$ be any element. Since

$$\left(0,\dots,0,(\gamma_{n_0+1}-1)\left(\sum_{i=1}^{r} x_i - x_{r+1}\right)\right) \in \tilde{R}_{n_0+1},$$

we have

$$\begin{aligned}(20)\qquad (\gamma_{n_0+1}-1)\overline{(x_i)} &= \overline{((\gamma_{n_0+1}-1)x_i)}\\ &= \overline{\left((\gamma_{n_0+1}-1)x_1,\dots,(\gamma_{n_0+1}-1)x_r,(\gamma_{n_0+1}-1)\sum_{i=1}^{r} x_i\right)}\\ &= (\gamma_{n_0+1}-1)\overline{\left(x_1,\dots,x_r,\sum_{i=1}^{r} x_i\right)} \in (\gamma_{n_0+1}-1)X.\end{aligned}$$

Hence $(\gamma_{n_0+1}-1)\tilde{X} \subseteq (\gamma_{n_0+1}-1)X$. Thus we have shown $(\gamma_{n_0+1}-1)\tilde{X} = (\gamma_{n_0+1}-1)X$. □

Let $L_0^{(p)}$ and $L_k^{(p)}$ be the maximal elementary abelian p-subextension of $L_0/\boldsymbol{Q}_N$ and L_0/k, respectively. Denote by $k^{(p)}$ the intermediate field of $k/\boldsymbol{Q}_N$ with $[k^{(p)} : \boldsymbol{Q}_N] = p$. Then we have

$$\begin{aligned}(21)\qquad \mathrm{Gal}(L_0^{(p)}/\boldsymbol{Q}_N) &\simeq (\mathrm{Gal}(L_{n_0+1}/\boldsymbol{Q}_{N+n_0+1})_{\Gamma_{n_0+1}})/p\\ &\simeq ((\mathrm{Gal}(L_{n_0+1}/k_{n_0+1}) \times \mathrm{Gal}(k_{n_0+1}/\boldsymbol{Q}_{N+n_0+1}))_{\Gamma_{n_0+1}})/p\\ &\simeq (\boldsymbol{Z}/p)^{\oplus r+1}\end{aligned}$$

by Lemmas 5, 6, (1) and (18). We find that $\mathrm{Gal}(L_k^{(p)}/\boldsymbol{Q}_N) = \mathrm{Gal}(L_k^{(p)}/k) \times \mathrm{Gal}(k/\boldsymbol{Q}_N)$ because $\mathfrak{l}_i$ is totally ramified in $k/\boldsymbol{Q}_N$ and $L_k^{(p)}/k$ is unramified extension by Lemma 5. Hence $L_k^{(p)} = kL_0^{(p)}$ and

$$(22) \qquad (\mathrm{Gal}(L_{n_0+1}/k_{n_0+1})_{\Gamma_{n_0+1}})/p \simeq \mathrm{Gal}(L_k^{(p)}/k) \simeq \mathrm{Gal}(L_0^{(p)}/k^{(p)})$$

by Lemma 6, where isomorphisms in the above are given by the restriction. It follows from (22), the fact $(\gamma\bar{\mathfrak{L}}_{i,n_0+1}, L_{n_0+1}/k_{n_0+1})|_{L_0^{(p)}} = (\bar{\mathfrak{l}}_i, L_0^{(p)}/k^{(p)})$, $\bar{\mathfrak{l}}_i$ being the unique prime of $k^{(p)}$ lying over $\mathfrak{l}_i$, and Nakayama's lemma that if $\{(\bar{\mathfrak{l}}_i, L_0^{(p)}/k^{(p)}) \mid 1 \le i \le r+1\}$ generates $\mathrm{Gal}(L_0^{(p)}/k^{(p)})$, then $\mathrm{Gal}(L_{n_0+1}/k_{n_0+1})$ is generated by $\{(\bar{\mathfrak{L}}_{i,n_0+1}, L_{n_0+1}/k_{n_0+1}) \mid 1 \le i \le r+1\}$ over $\boldsymbol{Z}/p^{m_0}[\Gamma_{n_0+1}]$, hence $L_{n_0+\delta}$ is the Hilbert p-class field of $k_{n_0+\delta}$ $(\delta = 0, 1)$ as mentioned above. Let I_i $(1 \le i \le r+1)$ be the inertia subgroup of $\mathrm{Gal}(L_0^{(p)}/\boldsymbol{Q}_N)$ for the prime $\mathfrak{l}_i$. Then we have $I_i \simeq \boldsymbol{Z}/p$ and

$$(23) \qquad \mathrm{Gal}(L_0^{(p)}/\boldsymbol{Q}_N) = \bigoplus_{i=1}^{r+1} I_i$$

because $\mathfrak{l}_i$ ramifies in $k^{(p)}$ by Lemma 5 and $\mathrm{Gal}(L_0^{(p)}/\boldsymbol{Q}_N) \simeq (\boldsymbol{Z}/p)^{\oplus r+1}$ by (21). Hence $L^{(p)}/\boldsymbol{Q}_N$ is the composite of the abelian extensions $\boldsymbol{Q}_N^{(p)}(\mathfrak{l}_i)/\boldsymbol{Q}_N$ $(1 \le i \le r+1)$ of degree p with conductor $\mathfrak{l}_i$, and the restriction induces the isomorphism

$$(24) \qquad \mathrm{Gal}(L_0^{(p)}/k^{(p)}) \simeq \bigoplus_{i=1}^{r} \mathrm{Gal}(\boldsymbol{Q}_N^{(p)}(\mathfrak{l}_i)/\boldsymbol{Q}_N).$$

Assume the following condition on $\mathfrak{l}_i$ $(1 \le i \le r+1)$:

Condition B. The prime $\mathfrak{l}_2$ is inert in $\boldsymbol{Q}_N^{(p)}(\mathfrak{l}_1)$. If $3 \le i \le r+1$, then the prime $\mathfrak{l}_i$ splits in $\boldsymbol{Q}_N^{(p)}(\mathfrak{l}_j)$ for all j such that $1 \le j \le i-2$ and is inert in $\boldsymbol{Q}_N^{(p)}(\mathfrak{l}_{i-1})$.

Then, under isomorphism (24),

$$\left(\frac{L_0^{(p)}/k^{(p)}}{\bar{\mathfrak{l}}_2}\right) \mapsto (\sigma_1, \dots), \quad \sigma_1 \in \mathrm{Gal}(\boldsymbol{Q}_N^{(p)}(\mathfrak{l}_i)/\boldsymbol{Q}_N),\ \sigma_1 \ne 1,$$

$$\left(\frac{L_0^{(p)}/k^{(p)}}{\bar{\mathfrak{l}}_i}\right) \mapsto (1, \dots, 1, \sigma_{i-1}, \dots), \quad \sigma_{i-1} \in \mathrm{Gal}(\boldsymbol{Q}_N^{(p)}(\mathfrak{l}_{i-1})/\boldsymbol{Q}_N),\ \sigma_{i-1} \ne 1 \ \ (3 \le i \le r+1).$$

Therefore $\{(\bar{\mathfrak{l}}_i, L_0^{(p)}/k^{(p)}) \mid 1 \le i \le r+1\}$ generates $\mathrm{Gal}(L_0^{(p)}/k^{(p)})$, which implies $L_{n_0+\delta} = H_{n_0+\delta}^{(p)}$ $(\delta = 0, 1)$, under Condition B. Condition B is equivalent to the following condition on $\tilde{\mathfrak{L}}_{i,n_0+1}$:

Condition B′. The prime $\tilde{\mathfrak{L}}_{2,n_0+1}$ is inert in $\boldsymbol{Q}_N^{(p)}(\mathfrak{l}_1)\tilde{\boldsymbol{Q}}_{N+n_0+1}$. If $3 \le i \le r+1$, then the prime $\tilde{\mathfrak{L}}_{i,n_0+1}$ splits in $\boldsymbol{Q}_N^{(p)}(\mathfrak{l}_j)\tilde{\boldsymbol{Q}}_{N+n_0+1}$ for all j such that $1 \le j \le i-2$ and is inert in $\boldsymbol{Q}_N^{(p)}(\mathfrak{l}_{i-1})\tilde{\boldsymbol{Q}}_{N+n_0+1}$.

By virtue of Lemma 3, we can choose inductively the degree one primes $\tilde{\mathfrak{L}}_{i,n_0+1}$ of $\tilde{\boldsymbol{Q}}_{N+n_0+1}$ from $i = 1$ to $r+1$ such that $\tilde{\mathfrak{L}}_{i,n_0+1}$'s satisfy Conditions A and B′, and that $\tilde{\mathfrak{L}}_{i,n_0+1}$'s are lying over distinct rational primes, because $\boldsymbol{Q}_N^{(p)}(\mathfrak{l}_j)\tilde{\boldsymbol{Q}}_{N+n_0+1}$'s $(1 \le j \le i-1)$ and $\tilde{\boldsymbol{Q}}_{N+n_0+1}(\sqrt[p^{m_0}]{\mathcal{O}_{N+n_0+1}^{\times}})$ are independent over $\tilde{\boldsymbol{Q}}_{N+n_0+1}$. Thus the cyclotomic $\boldsymbol{Z}_p$-extension over totally real number field k given in Lemma 5 is a desired $\boldsymbol{Z}_p$-extension.

□

4. Proof of Theorem 2.

Let p be a given odd prime number and F an imaginary quadratic field such that the class number of F is prime to p and the prime p is inert in F. Such field F certainly exists by Horie [**4**]. Denote by F_∞/F the anti-cyclotomic $\boldsymbol{Z}_p$-extension, namely, the unique $\boldsymbol{Z}_p$-extension over F which is non-abelian (dihedral) Galois extension over $\boldsymbol{Q}$. We write F_n for the n-th layer of F_∞/F and put $\Gamma_n = \mathrm{Gal}(F_n/F)$. It follows from Iwasawa [**7**, section 2] (see also [**10**, chapter 13, Theorem 5.2]) that if a prime $\mathfrak{l}$ of F with $\mathfrak{l} \nmid p$ is inert in $F/\boldsymbol{Q}$, then $\mathfrak{l}$ decomposes completely in F_∞. Let l_i $(1 \le i \le m+1)$ be distinct rational primes such that

$$l_i \text{ is inert in } F \text{ and } l_i \equiv 1 \pmod{p}, \tag{25}$$

and put $f = \prod_{i=1}^{m+1} l_i$. For $n \ge 0$, we define the field L_n to be the maximal elementary abelian p-extension field over F_n whose conductor divides f. It follows from the assumption on F and Iwasawa [**5**] that the class number of F_n is prime to p. Then we have the following exact sequence of Γ_n-modules by class field theory:

$$\mathcal{O}_n^\times/p \to (\mathcal{O}_n/f)^\times/p \to \mathrm{Gal}(L_n/F_n) \to 0, \tag{26}$$

where $\mathcal{O}_n$ denotes the integer ring of F_n. Since the prime l_i of F splits completely in F_n, we can see that $(\mathcal{O}_n/f)^\times/p \simeq \boldsymbol{Z}/p[\Gamma_n]^{\oplus m+1}$ as in the proof of Theorem 1. Then, by taking the projective limit of exact sequence (26) for $n \ge 0$, we get the exact sequence of $\Lambda_{F_\infty/F}$-modules

$$\varprojlim(\mathcal{O}_n^\times/p) \to (\Lambda_{F_\infty/F}/p)^{\oplus m+1} \to \mathrm{Gal}(L_\infty/F_\infty) \to 0, \tag{27}$$

where the projective limit $\varprojlim(\mathcal{O}_n^\times/p)$ is taken with respect to the norm maps and $L_\infty = \bigcup_{n \ge 0} L_n$.

Lemma 7. *We have* $\mathcal{O}_n^\times/p \simeq \boldsymbol{Z}/p[\Gamma_n]/\sum_{\gamma \in \Gamma_n} \gamma$, *and* $\varprojlim(\mathcal{O}_n^\times/p) \simeq \Lambda_{F_\infty/F}/p$.

Proof. We assume that $\mathcal{O}_n^\times/p \simeq \bigoplus_{i=1}^s \boldsymbol{Z}/p[\Gamma_n]/(\gamma_n - 1)^{a_i}$ for $1 \le a_i \le p^n$. Then $\sum_{i=1}^s a_i = \dim_{\boldsymbol{Z}/p} \mathcal{O}_n^\times/p = p^n - 1$. From the exact sequence

$$0 \to \mathcal{O}_n^\times \xrightarrow{p} \mathcal{O}_n^\times \to \mathcal{O}_n^\times/p \to 0$$

and the fact that $\hat{H}^{2i}(\Gamma_n, \mathcal{O}_n^\times) = 0$ $(i \in \boldsymbol{Z})$ (This follows from the fact that $\hat{H}^0(\Gamma_n, \mathcal{O}_n^\times) = \mathcal{O}_0^\times/(\sum_{\gamma \in \Gamma_n} \gamma)\mathcal{O}_n^\times = 0$ since $\#\mathcal{O}_0^\times$ is finite and prime to p), we get the following exact cohomology sequence:

$$0 \to \hat{H}^0(\Gamma_n, \mathcal{O}_n^\times/p) \to H^1(\Gamma_n, \mathcal{O}_n^\times) \xrightarrow{p} H^1(\Gamma_n, \mathcal{O}_n^\times) \to H^1(\Gamma_n, \mathcal{O}_n^\times/p) \to 0. \tag{28}$$

One can show that $H^1(\Gamma_n, \mathcal{O}_n^\times) \simeq P_n^{\Gamma_n}/P_0$, P_n being the principal ideal group of F_n. Because the class number h_n of F_n is prime to p and the prime $\mathfrak{P}_n$ of F_n lying over p is the unique ramified prime in F_n/F, which is totally ramified, $P_n^{\Gamma_n}/P_0$ (note that $P_n^{\Gamma_n}/P_0$ has p-power order) is generated by the class of $\mathfrak{P}_n^{h_n}$, whose order is p^n. Hence $H^1(\Gamma_n, \mathcal{O}_n^\times) \simeq \boldsymbol{Z}/p^n$, which implies $H^1(\Gamma_n, \mathcal{O}_n^\times/p) \simeq \boldsymbol{Z}/p$ by (28). Since $H^1(\Gamma_n, \mathcal{O}_n^\times/p) = \bigoplus_{i=1}^s H^1(\Gamma_n, \boldsymbol{Z}/p[\Gamma_n]/(\gamma_n - 1)^{a_i})$ and $H^1(\Gamma_n, \boldsymbol{Z}/p[\Gamma_n]/(\gamma_n - 1)^{a_i}) = 0$ if and only if $a_i = p^n$, we have $\mathcal{O}_n^\times \simeq \boldsymbol{Z}/p[\Gamma_n]/(\gamma_n - 1)^{p^n - 1} = \boldsymbol{Z}/p[\Gamma_n]/\sum_{\gamma \in \Gamma_n} \gamma$.

By the similar way to the above, we can show that $H^1(F_t/F_n, \mathcal{O}_t^\times) \simeq \boldsymbol{Z}/p^{t-n}$ for $0 \le n \le t$. Then it follows from the fact $\#H^1(F_t/F_n, \mathcal{O}_t^\times)/\#\hat{H}^0(F_t/F_n, \mathcal{O}_t^\times) = [F_t : F_n] = p^{t-n}$ that $\hat{H}^0(F_t/F_n, \mathcal{O}_t^\times) = 0$, which implies the norm map $\mathcal{O}_t^\times/p \to \mathcal{O}_n^\times/p$ is surjective. Hence we have $\varprojlim \mathcal{O}_n^\times/p \simeq \varprojlim \boldsymbol{Z}/p[\Gamma_n]/\sum_{\gamma\in\Gamma_n}\gamma \simeq \varprojlim \boldsymbol{Z}/p[\Gamma_n] \simeq \Lambda_{F_\infty/F}/p$, where the projective limit in the second and third terms are taken with respect to the maps induced by the natural surjection $\Gamma_t \to \Gamma_n$ for $0 \le n \le t$. □

Let k/F be a degree p subextension of L_0/F in which all the primes l_i $(1 \le i \le m+1)$ ramify. Then we will see that L_n/k_n is an unramified abelian p-extension, where $k_n = kF_n$. If *L_n is the Hilbert p-class field of k_n for all $n \ge 0$ and the map* $\varprojlim(\mathcal{O}_n^\times/p) \to (\Lambda_{F_\infty/F}/p)^{\oplus m+1}$ *in* (27) *is injective*, then we have

$$X_{k_\infty} = \mathrm{Gal}(L_\infty/k_\infty) \sim \mathrm{Gal}(L_\infty/F_\infty) \simeq \mathrm{coker}(\varprojlim(\mathcal{O}_n^\times/p) \to (\Lambda_{F_\infty/F}/p)^{\oplus m+1})$$

$$\sim (\Lambda_{F_\infty/F}/p)^{\oplus m} \simeq (\Lambda_{k_\infty/k}/p)^{\oplus m}$$

by Lemma 7, where $k_\infty = kF_\infty$ and $\sim$ denotes a pseudo-isomorphism. In what follows, we shall choose the primes l_i and the field k so that the above conditions are satisfied.

For a prime $l \equiv 1 \pmod p$, we denote by $\boldsymbol{Q}^{(p)}(l)$ the unique subfield of $\boldsymbol{Q}(\mu_l)$ of degree p. Now we impose the following condition on primes l_i:

Condition. p is inert in $\boldsymbol{Q}^{(p)}(l_1)$ and splits in $\boldsymbol{Q}^{(p)}(l_i)$ for $2 \le i \le m+1$. If $2 \le i \le m+1$, then l_i splits in $\boldsymbol{Q}^{(p)}(l_j)$ for all j such that $1 \le j \le i-2$ and is inert in $\boldsymbol{Q}^{(p)}(l_{i-1})$.

Lemma 8. *There exist distinct prime numbers l_i $(1 \le i \le m+1)$ satisfying* (25) *and the above condition.*

Proof. We first note that p is inert in $\boldsymbol{Q}^{(p)}(l)$ if and only if $p^{(l-1)/p} \not\equiv 1 \pmod l$ for a prime number $l \equiv 1 \pmod p$. Hence if the decomposition subgroup of $\mathrm{Gal}(\boldsymbol{Q}(\mu_p, \sqrt[p]{p})/\boldsymbol{Q})$ for a prime of $\boldsymbol{Q}(\mu_p, \sqrt[p]{p})$ lying over l is $\mathrm{Gal}(\boldsymbol{Q}(\mu_p, \sqrt[p]{p})/\boldsymbol{Q}(\mu_p))$ (resp. trivial) then $l \equiv 1 \pmod p$ and p is inert (resp. splits) in $\boldsymbol{Q}^{(p)}(l)$. Applying the Čebotarev density theorem to $\boldsymbol{Q}(\mu_p, \sqrt[p]{p})F/\boldsymbol{Q}$, we can choose prime l_1 satisfying (25) and the Condition since $\boldsymbol{Q}(\mu_p, \sqrt[p]{p})$ and F are independent over $\boldsymbol{Q}$. We can choose the prime l_i $(2 \le i \le m+1)$ satisfying (25) and the Condition inductively from $i = 2$ to $m+1$ by applying the Čebotarev density theorem to $\boldsymbol{Q}(\mu_p, \sqrt[p]{p})F\boldsymbol{Q}^{(p)}(l_1)\cdots\boldsymbol{Q}^{(p)}(l_{i-1})/\boldsymbol{Q}$ since $\boldsymbol{Q}(\mu_p, \sqrt[p]{p})$, F and $\boldsymbol{Q}^{(p)}(l_j)$'s $(1 \le j \le i-1)$ are independent over $\boldsymbol{Q}$. □

We assume that distinct prime numbers l_i $(1 \le i \le m+1)$ satisfy the Condition and (25). It follows from (26) for $n = 0$ that $L_0 = F\boldsymbol{Q}^{(p)}(l_1)\cdots\boldsymbol{Q}^{(p)}(l_{m+1})$ and $\mathrm{Gal}(L_0/F) = \bigoplus_{i=1}^{m+1} I_{l_i}$ where $I_{l_i} \simeq \boldsymbol{Z}/p$ is the inertia subgroup of $\mathrm{Gal}(L_0/F)$ for the prime l_i. Since the decomposition subgroup of $\mathrm{Gal}(L_0/F)$ for the prime p is I_{l_1} by the Condition, there exists an intermediate field k of L_0/F with $[k : F] = p$ such that p is inert and l_i ramifies in k/F for any i. Then $k/\boldsymbol{Q}$ is a cyclic extension of degree $2p$ and k *has the unique prime lying over* p.

Lemma 9. (i) *L_n is the genus p-class field of k_n/F_n* $(k_n := F_nk)$.

(ii) *The restriction induces* $\mathrm{Gal}(L_n/k_n)_{\Gamma_n} \simeq \mathrm{Gal}(L_0/k)$.

Proof. (i) Since the prime l_i ramifies in L_0/F and $L_0 \subseteq L_n$, every prime of F_n lying over l_i ramifies in k_n/F_n. Hence L_n/k_n is an unramified p-extension, because in L_n/F_n, the ramification index of a prime of F_n lying over l_i is p. By a similar argument to the proof of Lemma 5 (iii), we have the assertion.

(ii) Let M be the maximal intermediate field of L_n/k_n which is abelian over k. Then $\mathrm{Gal}(L_n/k_n)_{\Gamma_n} \simeq \mathrm{Gal}(M/k_n)$ and M/F is abelian. We shall show that $M = k_n L_0$. $k_n L_0 \subseteq M$ is obvious. Denote by I_p the inertia subgroup of $\mathrm{Gal}(M/k)$ for the unique prime of k lying over p. Then $\mathrm{Gal}(M/k) = I_p \times \mathrm{Gal}(M/k_n)$ and the fixed subfield M^{I_p} of M by I_p is contained in L_0, because M^{I_p}/k is unramified p-extension, M/F is abelian, and L_0 is the genus p-class field of k/F by (i). Hence it follows that $M \subseteq L_0 k_n$. Therefore we have $M = L_0 k_n$ and $\mathrm{Gal}(L_n/k_n)_{\Gamma_n} \simeq \mathrm{Gal}(M/k_n) \simeq \mathrm{Gal}(L_0/k)$. □

By virtue of Lemma 9 and Nakayama's lemma, we find that if $\{(\mathfrak{l}_i, L_0/k) \mid 1 \le i \le m+1\}$ generates $\mathrm{Gal}(L_0/k)$, then L_n is the Hilbert p-class field of k_n as in the proof of Theorem 1, where $\mathfrak{l}_i$ denotes the unique prime of k lying over l_i. It follows from the Condition on l_i's and the fact $L_0 = k\boldsymbol{Q}^{(p)}(l_1)\cdots\boldsymbol{Q}^{(p)}(l_m)$ that $\{(\mathfrak{l}_i, L_0/k) \mid 1 \le i \le m+1\}$ generates $\mathrm{Gal}(L_0/k)$. Therefore L_n is the Hilbert p-class field of k_n for all $n \ge 0$.

Next we shall show the injectivity of the map $\varprojlim \mathcal{O}_n^\times/p \to (\Lambda_{F_\infty/F}/p)^{\oplus m+1}$ in (27). It is enough to show that the map $\mathcal{O}_n^\times/p \to (\mathcal{O}_n/l_1)^\times/p$ is injective for all $n \ge 0$. Let $F_n^{(p)}(l_1)$ be the maximal elementary abelian p-extension field over F_n whose conductor divides l_1. Then we get the exact sequence

$$\mathcal{O}_n^\times/p \to (\mathcal{O}_n/l_1)^\times/p \to \mathrm{Gal}(F_n^{(p)}(l_1)/F_n) \to 0. \tag{29}$$

It follows from the above exact sequence for $n=0$ that $[F_0^{(p)}(l_1) : F_0] = p$ and the prime l_1 ramifies in $F_0^{(p)}(l_1)/F_0$. Hence $F_n^{(p)}(l_1)/F_n F_0^{(p)}(l_1)$ is an unramified abelian p-extension. The class number of $F_0^{(p)}(l_1)$ is prime to p because the class number of F is prime to p and l_1 is the only ramified prime in $F_0^{(p)}(l_1)/F$ (see Iwasawa [**5**]). Since there is the unique prime of $F_0^{(p)}(l_1) = F\boldsymbol{Q}^{(p)}(l_1)$ lying above p by the Condition, which is the unique prime ramifying in $F_n F_0^{(p)}(l_1)/F_0^{(p)}(l_1)$, the class number of $F_n F_0^{(p)}(l_1)$ is prime to p by Iwasawa's result mentioned above. Hence we have $F_n^{(p)}(l_1) = F_n F_0^{(p)}(l_1)$ and $\mathrm{Gal}(F_n^{(p)}(l_1)/F_n) \simeq \boldsymbol{Z}/p$, which implies the injectivity of the map $\mathcal{O}_n^\times/p \to (\mathcal{O}_n/l_1)^\times/p$ by (29) and the fact $\#((\mathcal{O}_n/l_1)^\times/p)/\#(\mathcal{O}_n^\times/p) = p$.

Thus we have shown that k_∞/k is a $\boldsymbol{Z}_p$-extension with $X_{k_\infty} \sim (\Lambda_{k_\infty/k}/p)^{\oplus m}$.

Finally we shall show that $X_{k_\infty} \simeq (\Lambda_{k_\infty/k}/p)^{\oplus m}$. Since $pX_{k_\infty} = p \varprojlim \mathrm{Gal}(L_n/k_n) = 0$, X_{k_∞} is a finitely generated module over the principal ideal domain $\Lambda_{k_\infty/k}/p$. Because $X_{k_\infty} \sim (\Lambda_{k_\infty/k}/p)^{\oplus m}$, we have

$$X_{k_\infty} \simeq (\Lambda_{k_\infty/k}/p)^{\oplus m} \oplus \mathrm{Tor}_{\Lambda_{k_\infty/k}/p} X_{k_\infty} \tag{30}$$

as $\Lambda_{k_\infty/k}/p$-modules. From the fact that there is the unique prime of k lying over p and k_∞/k is a totally ramified at that prime, we have $\mathrm{Gal}(L_0/k) \simeq X_{k_\infty/k}/(\gamma_\infty - 1)$, where γ_∞ is a topological generator of $\mathrm{Gal}(k_\infty/k)$ (see [**6**]). Hence it follows from $\mathrm{Gal}(L_0/k) = \mathrm{Gal}(F\boldsymbol{Q}^{(p)}(l_1)\cdots\boldsymbol{Q}^{(p)}(l_{m+1})/k) \simeq (\boldsymbol{Z}/p)^{\oplus m}$ and (30) that $\mathrm{Tor}_{\Lambda_{k_\infty/k}/p} X_{k_\infty} = 0$. Thus we have $X_{k_\infty} \simeq (\Lambda_{k_\infty/k}/p)^{\oplus m}$ as $\Lambda_{k_\infty/k}$-modules. □

Example. Put $p = 3$, $F = \boldsymbol{Q}(\sqrt{-1})$, and let F_∞/F be the anti-cyclotomic $\boldsymbol{Z}_3$-extension. Then p is inert in F and the class number of F is prime to p. Put

$f_1 = 7 \cdot 19$, $f_2 = 7 \cdot 19 \cdot 43$, $f_3 = 7 \cdot 19 \cdot 43 \cdot 1597$, and denote by $M_s/\boldsymbol{Q}$ $(s = 1, 2, 3)$ a cubic cyclic extension of conductor f_s such that the prime 3 is inert in M_s. Then it holds that $\mu(M_s F_\infty / M_s F) = s$ for $s = 1, 2, 3$.

5. Application to a certain capitulation problem.

In this section we shall apply Theorem 1 to a certain capitulation problem. Let F be a number field with the ideal class group $\mathrm{Cl}(F)$. Then the principal ideal theorem says that:

Principal ideal theorem. *Every ideal of F capitulates in the Hilbert class field H_F of F, namely, the natural map $\mathrm{Cl}(F) \to \mathrm{Cl}(H_F)$ is the zero map.*

However it happens that all the ideals of F capitulate in a proper subextension field of H_F/F. Iwasawa constructed an infinite family of such number fields F by using the theory of $\boldsymbol{Z}_p$-extensions in [**9**]:

Theorem (Iwasawa [**8**], [**9**]). *For any prime number p, there exist infinitely many number fields F with the following properties*:

(i) $\mathrm{Cl}(F)(p) \simeq \boldsymbol{Z}/p^r$ *with* $r \geq 2$, $\mathrm{Cl}(F)(p)$ *being the Sylow p-subgroup of* $\mathrm{Cl}(F)$,

(ii) $\mathrm{Cl}(F)(p)$ *capitulates in an unramified cyclic extension F'/F of degree p.*

In the above theorem, let M be the compositium of F' and the Hilbert l-class fields of F for all the prime numbers $l \neq p$. Then $F \subseteq M \subsetneq H_F$ and $\mathrm{Cl}(F)$ capitulates in M.

In the paper [**11**], the author showed that for any given number N, there exists a number field F such that $\mathrm{Cl}(F)(p) \simeq \boldsymbol{Z}/p^r$ with $r \geq N$ and that F has property (ii) in Iwasawa's theorem. By using the construction of Theorem 1, we further improve the theorem:

Theorem 3. *For any prime number p and finite abelian p-group A, there exists a number field F with the following properties*:

(i) $\mathrm{Cl}(F)(p) \simeq A$,

(ii) $\mathrm{Cl}(F)(p)$ *capitulates in an unramified cyclic extension F'/F of degree* $\exp(\mathrm{Cl}(F)(p))$, $\exp(\mathrm{Cl}(F)(p))$ *being the exponent of* $\mathrm{Cl}(F)(p)$.

Proof. Let p^e be the exponent of A and A' a subgroup of A with $A \simeq A' \oplus \boldsymbol{Z}/p^e$. By the construction in the proof of Theorem 1 for $X = A'$ with trivial Γ-action, $n_0 = 0$ and $m_0 = e$, we get the cyclic extension $k/\boldsymbol{Q}_N$ of degree p^e such that $\mathrm{Cl}(k_t)(p) \simeq A'$ for any $t \geq 0$ and the Hilbert p-class field $H_k^{(p)}$ of k is the genus p-class field L_0 of $k/\boldsymbol{Q}_N$ (recall Lemma 5 (iii)). Let F be an intermediate field of $k_e/\boldsymbol{Q}_N$ such that $\mathrm{Gal}(F/\boldsymbol{Q}_N) \simeq \boldsymbol{Z}/p^e$ and $F \cap k = F \cap \boldsymbol{Q}_{N+e} = \boldsymbol{Q}_N$. Then we can see that k_e/F is an unramified cyclic extension of degree p^e. Denote by $H_{k_e}^{(p)}$ the Hilbert p-class field of k_e. Then $H_{k_e}^{(p)} = L_0 k_e = L_0 \boldsymbol{Q}_{N+e}$, hence $H_{k_e}^{(p)}/\boldsymbol{Q}_N$ is an abelian extension since $L_0/\boldsymbol{Q}_N$ is abelian. Therefore $H_{k_e}^{(p)}/F$ is an unramified abelian p-extension. Consequently, $H_{k_e}^{(p)}$ is the Hilbert p-class field of F. Since $H_{k_e}^{(p)} = L_0 F$ and $L_0 \cap F = \boldsymbol{Q}_N$, we have $\mathrm{Cl}(F)(p) \simeq \mathrm{Gal}(H_{k_e}^{(p)}/F) = \mathrm{Gal}(L_0 F/F) \simeq \mathrm{Gal}(L_0/\boldsymbol{Q}_N) \simeq A' \oplus \boldsymbol{Z}/p^e \simeq A$. Hence the field F satisfies condition (i).

Next we shall show that the field F satisfies condition (ii). From class field theory, we get the following commutative diagram:

$$\begin{array}{ccc} \mathrm{Cl}(k_e)(p) & \xrightarrow{\sim} & \mathrm{Gal}(H_{k_e}^{(p)}/k_e) \\ \uparrow & & \uparrow \text{transfer} \\ \mathrm{Cl}(F)(p) & \xrightarrow{\sim} & \mathrm{Gal}(H_{k_e}^{(p)}/F) \simeq A, \end{array}$$

where the horizontal maps are the reciprocity maps, the left vertical map is the natural map and the right vertical map is the transfer map from $\mathrm{Gal}(H_{k_e}^{(p)}/F)^{\mathrm{ab}} = \mathrm{Gal}(H_{k_e}^{(p)}/F)$ to $\mathrm{Gal}(H_{k_e}^{(p)}/k_e)^{\mathrm{ab}} = \mathrm{Gal}(H_{k_e}^{(p)}/k_e)$. Since the transfer map $\mathrm{Gal}(H_{k_e}^{(p)}/F) \to \mathrm{Gal}(H_{k_e}^{(p)}/k_e)$ is equal to the multiplication-by-p^e-map when we regard $\mathrm{Gal}(H_{k_e}^{(p)}/k_e)$ as a subgroup of $\mathrm{Gal}(H_{k_e}^{(p)}/F)$, it is equal to the zero-map by $\mathrm{Gal}(H_{k_e}^{(p)}/F) \simeq A$. Hence the natural map $\mathrm{Cl}(F)(p) \to \mathrm{Cl}(k_e)(p)$ is also the zero-map. Therefore $\mathrm{Cl}(F)(p)$ capitulates in an unramified cyclic extension k_e/F of degree $p^e = \exp(\mathrm{Cl}(F)(p))$. □

References

[1] B. Ferrero and L. C. Washington, The Iwasawa invariant μ_p vanishes for abelian number fields, Ann. of Math. (2), **109** (1979), 377–395.

[2] T. Fukuda, Remarks on $\boldsymbol{Z}_p$-extensions of number fields, Proc. Japan Acad. Ser. A Math. Sci., **70** (1994), 264–266.

[3] R. Greenberg, On the Iwasawa invariants of totally real number fields, Amer. J. Math., **98** (1976), 263–284.

[4] K. Horie, A note on basic Iwasawa λ-invariants of imaginary quadratic fields, Invent. Math., **88** (1987), 31–38.

[5] K. Iwasawa, A note on class numbers of algebraic number fields, Abh. Math. Sem. Univ. Hamburg, **20** (1956), 257–258.

[6] K. Iwasawa, On Γ-extensions of algebraic number fields, Bull. Amer. Math. Soc., **65** (1959), 183–226.

[7] K. Iwasawa, On the μ-invariants of $\boldsymbol{Z}_\ell$-extensions, Number Theory, Algebraic Geometry and Commutative Algebra, in honor of Y. Akizuki, Kinokuniya, Tokyo, 1973, 1–11.

[8] K. Iwasawa, A note on capitulation problem for number fields I, Proc. Japan Acad. Ser. A Math. Sci., **65** (1989), 59–61.

[9] K. Iwasawa, A note on capitulation problem for number fields II, Proc. Japan Acad. Ser. A Math. Sci., **65** (1989), 183–186.

[10] S. Lang, Cyclotomic Fields I and II (2nd edition), Grad. Texts in Math., **121**, Springer-Verlag, New York, 1990.

[11] M. Ozaki, Iwasawa invariants of p-extensions of totally real number fields, preprint.

[12] L. C. Washington, Introduction to Cyclotomic Fields (2nd. edition), Grad. Texts in Math., **83**, Springer-Verlag, New York, 1997.

[13] O. Yahagi, Construction of Number fields with prescribed l-class groups, Tokyo J. Math., **1** (1978), 275–283.

Manabu Ozaki
Department of Mathematics
Faculty of Science and Engineering
Shimane University
Nishikawatsu-Cho 1060
Matsue 690-8504
Japan
E-mail: ozaki@math.shimane-u.ac.jp