Construction of $\mathbb{Z}_p$-extensions with prescribed Iwasawa $\lambda$-invariants

Satoshi Fujii $^{a,*}$, Yoshihiro Ohgi $^b$, Manabu Ozaki $^{c,1}$

$^a$ Department of Mathematical Sciences, School of Science and Engineering, Waseda University, Okubo 3-4-1, Shinjuku-ku, Tokyo 169-8555, Japan

$^b$ Yonago Test-Coaching School, Nishifukubara 20-2, Yonago 683-0805, Japan

$^c$ Department of Mathematics, School of Science and Engineering, Kinki University, Kowakae 3-4-1, Higashi-Osaka 577-8502, Japan

Received 17 October 2004; revised 10 June 2005
Available online 10 November 2005
Communicated by David Goss

Abstract

It is a basic problem in Iwasawa theory that the existence of a $\mathbb{Z}_p$-extension with prescribed Iwasawa invariants. Since the Iwasawa $\lambda$-invariant is regarded as an analogue of (twice of) the genus of an algebraic curve, we are especially interested in the problem on the Iwasawa $\lambda$-invariants. In this article, for a few prime numbers $p$, we show that there is a $\mathbb{Z}_p$-extension with prescribed Iwasawa $\lambda$-invariant by using Kida’s formula, which is a number field analogue of the Riemann–Hurwitz formula.

© 2005 Elsevier Inc. All rights reserved.

MSC: 11R23; 11R29

* Corresponding author.

E-mail addresses: fujii@ruri.waseda.jp (S. Fujii), ozaki@math.kindai.ac.jp (M. Ozaki).

1 The author was partially supported by the Ministry of Education, Science, Sports and Culture, Grant-in-Aid for Young Scientists (B), 15740016, 2005.
1. Introduction

Let $p$ be a fixed prime number. For any $\mathbb{Z}_p$-extension $K/k$ over a number field $k$ of finite degree, the Iwasawa module $X_K$ of $K/k$ is defined to be the projective limit $\lim \leftarrow A(k_n)$ with respect to the norm maps, $A(k_n)$ being the $p$-part of the ideal class group of the $n$th layer $k_n$ of $K/k$. Otherwise, we can also define $X_K$ to be the Galois group $\text{Gal}(L(K)/K)$ of the maximal unramified pro-$p$ abelian extension $L(K)/K$. Then the complete group ring $\Lambda_{K/k} = \mathbb{Z}_p[\text{Gal}(K/k)]$ acts on $X_K$ and Iwasawa showed that $X_K$ is a finitely generated torsion $\Lambda_{K/k}$-module. Iwasawa [5] studied the $\Lambda_{K/k}$-module structure of $X_K$ and deduced the following celebrated formula.

**Theorem A.** There exist nonnegative integers $\lambda(K/k)$, $\mu(K/k)$ and an integer $\nu(K/k)$ such that $\#A(k_n) = p^{\lambda(K/k)n + \mu(K/k)p^n + \nu(K/k)}$ for all sufficiently large $n$.

Here the integers $\lambda(K/k)$, $\mu(K/k)$ and $\nu(K/k)$ are called the 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 $X_K$, namely, $\lambda(K/k) = \dim_{\mathbb{Q}_p}(X_K \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$, and $\mu(K/k) = \sum_{i=1}^{s} m_i$ where $m_i \geq 1$ are defined by $\text{Tor}_{\mathbb{Z}_p} X_K \sim \bigoplus_{i=1}^{s} \Lambda_{K/k}/p^{m_i}$, $\sim$ denoting a pseudo isomorphism of $\Lambda_{K/k}$-modules.

Now it arises the following basic question on $\lambda$- and $\mu$-invariants:

**Question A.** Let $p$ be a prime number. For any given nonnegative integers $\ell$ and $m$, does there exist a $\mathbb{Z}_p$-extension $K/k$ with $\lambda(K/k) = \ell$ and $\mu(K/k) = m$?

The third author [8] investigated “the $\mu$-part” of the above question, and gave the following:

**Theorem B.** Let $p$ be an odd prime number. For any nonnegative integer $m$, there exists a $\mathbb{Z}_p$-extension $K/k$ with $\mu(K/k) = m$ (and $\lambda(K/k) = 0$), specifically, $X_K \simeq (\Lambda_{K/k}/p)^{\oplus m}$.

At present, it is difficult to consider the $\lambda$- and $\mu$-invariants simultaneously in Question A. Hence, in the present paper, we will investigate the following simpler question, “the $\lambda$-part” of Question A:

**Question B.** Let $p$ be a prime number. For any given nonnegative integer $\ell$, does there exist a $\mathbb{Z}_p$-extension $K/k$ with $\lambda(K/k) = \ell$?

One may have a feeling that this question is easier than that on $\mu$-invariants because $\mu > 0$ usually causes many difficulties in Iwasawa theory. However, Question B seems much more difficult than the question on $\mu$-invariants. In fact, we can answer to Question B affirmatively only for a few prime numbers $p$ (see Theorem 1 below).

The Iwasawa $\lambda$-invariants may be regarded as an analogous invariant to the genus (or twice of the genus) of algebraic curves defined over finite fields. In contrast to the difficulty of Question B, one can easily find that the genus of algebraic curves takes an arbitrary
nonnegative value by using the Riemann–Hurwitz formula. In the case of number fields, we have not known whether this simple question is affirmatively answered for a given prime number \( p \). However, we will give the following partial answer to Question B by using Kida’s formula, which is a number field analogy to the Riemann–Hurwitz formula:

**Theorem 1.** Question B is affirmatively answered if \( p = 2, 3 \) or 5.

2. **Main result**

Throughout this paper, we denote by \( k_\infty \) the cyclotomic \( \mathbb{Z}_p \)-extension of a number field \( k \) for a fixed prime number \( p \).

First of all, we will see that Question B for \( p = 2 \) is affirmatively answered. Let \( \ell \) be any nonnegative integer. If we choose \( \ell + 1 \) distinct prime numbers \( p_1, \ldots, p_{\ell+1} \) with \( p_i \equiv \pm 3 \mod 8 \) and \( p_1 p_2 \cdots p_{\ell+1} \equiv 3 \mod 4 \), then the Iwasawa module of the cyclotomic \( \mathbb{Z}_2 \)-extension \( \mathbb{Q}(\sqrt{-p_1 \cdots p_{\ell+1}})_\infty/\mathbb{Q}(\sqrt{-p_1 \cdots p_{\ell+1}}) \) is isomorphic to \( \mathbb{Z}^{\oplus \ell} \) as \( \mathbb{Z}_2 \)-modules by the theorems of Ferrero [1] and Kida [6], hence \( \lambda(\mathbb{Q}(\sqrt{-p_1 \cdots p_{\ell+1}})_\infty/\mathbb{Q}(\sqrt{-p_1 \cdots p_{\ell+1}})) = \ell \).

For odd prime numbers \( p \), we will show the following, from which one can derive Theorem 1 in introduction:

**Theorem 2.** Let \( p \) be an odd prime number, and put \( S_p = \{0\} \cup \{ap - b(p - 1) \mid a, b \in \mathbb{Z}, 1 \leq b \leq a \leq p - 2\} \). Assume that for every \( t \in S_p \), there exists an imaginary quadratic field \( E \) (not \( \mathbb{Q}(\sqrt{-3}) \) if \( p = 3 \)) such that the \( \lambda \)-invariant of the cyclotomic \( \mathbb{Z}_p \)-extension \( E_\infty/E \) is equal to \( t \). Then, for any \( \ell \in \mathbb{Z}_{\geq 0} \), there exists a CM-field \( k \) with \( \lambda(k_\infty/k) = \ell \), specifically, \( X_{k_\infty} \cong \mathbb{Z}^{\oplus \ell}_p \) as \( \mathbb{Z}_p \)-modules.

For \( p = 3 \) and 5, we obtain Theorem 1 by using Theorem 2 and the calculation of \( \lambda \)-invariants by Fukuda [3]. In fact, we see that \( S_3 = \{0, 1\} \) and \( S_5 = \{0, 1, 2, 3, 6, 7, 11\} \), and that the \( \lambda \)-invariants of the cyclotomic \( \mathbb{Z}_3 \)-extensions over \( \mathbb{Q}(\sqrt{-m}) \) are 0 and 1 for \( m = 1 \) and 2, respectively, and those of the cyclotomic \( \mathbb{Z}_5 \)-extensions over \( \mathbb{Q}(\sqrt{-m}) \) are 0, 1, 2, 3, 6, 7, and 11 for \( m = 2, 6, 11, 166, 32911, 48570, 8105865 \), respectively.

3. **Proof of Theorem 2**

Theorem 2 follows from the following theorem as we shall see later:

**Theorem 3.** Let \( p \) be an odd prime number and \( k \) a CM-field with the maximal real subfield \( k^+ \), and put \( N = [k : \mathbb{Q}] = [k^+ : \mathbb{Q}] \). Assume that

(i) the Iwasawa \( \mu \)-invariant of \( k_\infty/k \) is 0,
(ii) the class number of \( k^+ \) is prime to \( p \),
(iii) there is a unique prime of \( k^+ \) lying above \( p \),
(iv) \( \xi_p \notin k \).
Then for any $s$ with $0 \leq s \leq N$ there exist infinitely many cyclic extensions $F$ over $k^+$ of degree $p$ such that $X(F_k) \simeq \mathbb{Z}_p^{\oplus p\lambda(k_{\infty}/k)+s(p-1)}$ as $\mathbb{Z}_p$-modules.

First, we will observe that Theorem 2 follows from Theorem 3. We see that

$$\mathbb{Z}_{\geq 0} = S_p \cup \{ pt + s(p-1) \mid t \in S_p, s \in \mathbb{Z}_{\geq 0} \} \tag{1}$$

as follows: Let $n \in \mathbb{Z}_{\geq 0}$ be any integer. Then we can write $n = u(p-1) + v$ with some integers $u \geq 0$ and $v$ with $0 \leq v \leq p - 2$. If $u \geq v$, then $n = pv + (u-v)(p-1)$ with $u - v \geq 0$ and $v \in \{ 0, 1, \ldots, p-2 \} \subset S_p$. If $v > u$, then $n = pv - (v-u)(p-1)$ with $1 \leq v - u \leq v \leq p - 2$, hence $n \in S_p$. Thus we obtain (1).

Let $\ell$ be any nonnegative integer. If $\ell \in S_p$, then we have nothing to do because $\ell$ is the $\lambda$-invariant of the cyclotomic $\mathbb{Z}_p$-extension over a certain imaginary quadratic field by the assumption of Theorem 2. Then, by using (1), we may assume that there exist $t \in S_p$ and $s \in \mathbb{Z}_{\geq 0}$ such that $\ell = pt + s(p-1)$. By the assumption of Theorem 2, there is an imaginary quadratic field $E(\neq \mathbb{Q}(\sqrt{-3})$ if $p = 3$) with the property $\lambda(E_{\infty}/E) = t$.

Let $d$ be a nonnegative integer with $s \leq p^d$. Then the CM-field $k = E_d$ (the $d$th layer of $E_{\infty}/E$) with the maximal real subfield $Q_d$ (the $d$th layer of $\mathbb{Q}_{\infty}/\mathbb{Q}$) satisfies the assumption of Theorem 3, because $\mu(E_{\infty}/E) = 0$ by the Ferrero–Washington theorem [2] and the class number of $Q_d$ is prime to $p$ as well known (see Iwasawa [4], or Washington [9, Theorem 10.4]). Then there is a cyclic extension $F$ over $Q_d$ of degree $p$ such that $X(F_k) \simeq \mathbb{Z}_p^{\oplus pt + s(p-1)} = \mathbb{Z}_p^{\oplus N}$ as $\mathbb{Z}_p$-modules. This proves Theorem 2.

Now we start with the proof of Theorem 3. We first introduce some basic notations. Let $\zeta_n \in \bar{\mathbb{Q}}$ be a fixed primitive $n$th root of unity for any integer $n \geq 1$, and we write $\mu_{p^n}$ for the group of all $p$-power-th roots of unity. For any number field $L$, we denote by $O_L$ and $E_L$ the ring of integers and the unit group of $L$, respectively. We let $e_0$ be the positive integer such that $k^+(\zeta_p) \cap Q(\mu_{p^n}) = Q(\zeta_{p^{e_0}})$, and let $b$ be the order of the ideal class containing the prime $p$ of $k^+$ lying above $p$ in the ideal class group of $k^+$. Then $b$ is prime to $p$ by assumption (ii), and $p^b = aO_{k^+}$ for some $a \in O_{k^+}$. Put $M = k^+(\zeta_p)$, and let $\{ \epsilon_1, \ldots, \epsilon_{N-1} \}$ be a system of fundamental units of $k^+$.

**Lemma 1.** The elements $\alpha(M^x)^p$, $\zeta_{p^{e_0}}(M^x)^p$, $\epsilon_1(M^x)^p$, $\ldots$, $\epsilon_{N-1}(M^x)^p$ of $M^x/(M^x)^p$ are independent over $\mathbb{F} := \mathbb{Z}/p$.

**Proof.** Assume that

$$\alpha^d \zeta_{p^{e_0}}^{c} \epsilon_1^{a_1} \cdots \epsilon_{N-1}^{a_{N-1}} = \beta_1^p$$

for some $a_i, c, d \in \mathbb{Z}$, and $\beta_1 \in M^x$. Let $v$ be the normalized $\mathfrak{P}$-adic valuation with respect to a prime $\mathfrak{P}$ of $M$ lying above $p$. By the above equality, we have $bde(\mathfrak{P}) = dv(\alpha) = pv(\beta_1)$, $e(\mathfrak{P})$ being the ramification index of the prime $\mathfrak{P}$ in $M/k^+$. Since $[M : k^+]$ is prime to $p$, $e(\mathfrak{P})$ is also prime to $p$. Hence we deduce $p/d$ from the above equality and the fact $p \nmid b$. Then we have

$$\zeta_{p^{e_0}}^{c} \epsilon_1^{a_1} \cdots \epsilon_{N-1}^{a_{N-1}} = \beta_2^p$$
for some $\beta_2 \in M^\times$. Let $\sigma$ be a generator of the cyclic group $\text{Gal}(M/k^+)$.

By operating $\sigma - 1$ to the both sides of the above equality, we have $(\zeta_{p^r_0}^{-1})^c = (\beta_2^{\sigma - 1})^p$. Let $f$ be an integer such that $\zeta_{p^r_0}^f = \zeta_{p^r_0}^{\beta_2}$, so that $f \not\equiv 1 \mod p$. Since $\zeta_{p^r_0}^{(f-1)c} = (\beta_2^{\sigma - 1})^p$, we see that $\beta_2^{\sigma - 1}$ is a $p$-power-th root of unity in $M$. Then $\beta_2^{\sigma - 1} = \zeta_{p^r_0}^h$ for some $h \in \mathbb{Z}$. This implies $(f-1)c \equiv ph \mod p^{r_0}$, and, therefore, $p \mid (f-1)c$. Since $p \nmid f - 1$, we have $p \nmid c$. Hence, we have

$$\varepsilon_1^{a_1} \cdots \varepsilon_{N-1}^{a_{N-1}} = \beta_3^p$$

for some $\beta_3 \in M^\times$. By taking the norm from $M$ to $k^+$, we have $\varepsilon_1^{a_1[M:k^+]} \cdots \varepsilon_{N-1}^{a_{N-1}[M:k^+]} = (N_{M/k+\beta_3})^p$. Since $[M : k^+]$ is prime to $p$, we have $p \mid a_i$ for $1 \leq i \leq N - 1$ because $\{\varepsilon_1, \ldots, \varepsilon_{N-1}\}$ is a system of fundamental units of $k^+$. Thus we have completed a proof of Lemma 1. \( \square \)

Put $r = s$ if $s \geq 1$, and $r = 1$ if $s = 0$. It follows from Lemma 1 and the Kummer theory that the fields $M(\sqrt[3]{a})$, $M(\zeta_{p^r_0+1})$, $M(\sqrt[3]{1})$, $M(\sqrt[3]{N-1})$ are linearly disjoint cyclic extensions of degree $p$ over $M$. Therefore, by the Čebotarev density theorem, we can choose $r$ degree one primes $\mathcal{L}_1, \ldots, \mathcal{L}_r$ of $M$ satisfying the following conditions:

(I) $\mathcal{L}_i$ are prime to $p$ and lying over distinct rational primes,

(II) $\mathcal{L}_i$ remains prime in $M(\zeta_{p^r_0+1})/M$ for $1 \leq i \leq r$,

(III) if $r \geq 2$, then

(a) $\mathcal{L}_1$ remains prime in $M(\sqrt[3]{1})/M$ and splits in $M(\sqrt[3]{j})/M$ for $2 \leq j \leq N - 1$,

(b) $\mathcal{L}_i$ ($2 \leq i \leq r - 1$) remains prime in $M(\sqrt[3]{i-1})/M$ and $M(\sqrt[3]{j})/M$, and splits in $M(\sqrt[3]{j})/M$ for $1 \leq j \leq N - 1$, $j \neq i - 1, i$,

(c) $\mathcal{L}_r$ remains prime in $M(\sqrt[3]{N-1})/M$ and splits in $M(\sqrt[3]{j})/M$ for $1 \leq j \leq N - 1$, $j \neq r - 1$,

(III') if $r = 1$, then $\mathcal{L}_1$ splits in $M(\sqrt[3]{N-1})/M$ for $1 \leq j \leq N - 1$,

(IV) $\mathcal{L}_1$ remains prime and $\mathcal{L}_i$ ($2 \leq i \leq r$) splits in $M(\sqrt[3]{a})/M$,

(V) if $s \geq 1$, then $\mathcal{L}_s$ splits in $Mk/M$ for $1 \leq i \leq s$, and if $s = 0$ (hence $r = 1$), then $\mathcal{L}_1$ remains prime in $Mk/M$ (we see $[Mk : M] = 2$ from assumption (iv), hence $Mk/M$ is linearly disjoint from cyclic extensions of degree $p \neq 2$ over $M$).

Let $l_i$ be the prime of $k^+$ below $\mathcal{L}_i$ ($1 \leq i \leq r$) and $m = \prod_{1 \leq i \leq r} l_i$. Denote by $F/k^+$ the maximal elementary abelian $p$-extension of $k^+$ whose conductor divides $m$. We will show that $F$ is a desired field in what follows.

**Lemma 2.**

1. $F/k^+$ is ramified at exactly $r$ primes $l_1, \ldots, l_r$.
2. $\text{Gal}(F/k^+) = \langle (p, F/k^+) \rangle \cong \mathbb{Z}/p$, where $(\cdot, F/k^+)$ stands for the Artin symbol.

*In particular, the prime $p$ remains prime in $F/k^+$.***
Proof. Let \( I_m \) and \( S_m \) be the group of the fractional ideals which are prime to \( m \) and the ray group of modulo \( m \) of \( k^+ \), respectively, and define \( P_m \) to be the group of the principal ideals contained in \( I_m \). It follows from assumption (ii) that \( p \mid [I_m : P_m] \), hence we find that the natural inclusion \( P_m \subseteq I_m \) induces the isomorphism \((P_m/S_m)/p \simeq (I_m/S_m)/p\). By class field theory, the Artin map induces the isomorphism \((I_m/S_m)/p \simeq \text{Gal}(F/k^+)\), so that we have \((P_m/S_m)/p \simeq \text{Gal}(F/k^+)\). Let \( \varphi : E_{k^+} \to (\mathcal{O}_{k^+}/m)^\times /p \) be the natural map induced by the inclusion \( E_{k^+} \subseteq \mathcal{O}_{k^+} \). Then we obtain

\[
\text{Coker} \varphi \simeq (P_m/S_m)/p \simeq \text{Gal}(F/k^+). \tag{2}
\]

On the other hand, we have the following isomorphisms by condition (I):

\[
(\mathcal{O}_{k^+}/m)^\times /p \simeq \bigoplus_{1 \leq i \leq r} (\mathcal{O}_{k^+}/I_i)^\times /p \simeq \bigoplus_{1 \leq i \leq r} (\mathcal{O}_M/I_i)^\times /p \simeq \mathbb{F}_p^\oplus r,
\]

where the 1st and 2nd isomorphisms are the natural ones, and the 3rd isomorphism is induced by \((\mathcal{O}_M/I_i)^\times /p \ni (\text{the class of } \zeta_p) \mapsto 1 \in \mathbb{F}_p\). We identifies \((\mathcal{O}_{k^+}/m)^\times /p \) with \( \mathbb{F}_p^\oplus r \) via the above isomorphisms. Then it follows from conditions (III) and (III') on the primes \( \mathcal{L}_i \) that \( \varphi(E_{k^+}) = 0 \) if \( r = 1 \), and that if \( r \geq 2 \) then \( \varphi(E_{k^+}) \) is the subspace of \( \mathbb{F}_p^\oplus r \) generated by the following \( r - 1 \) elements:

\[
\varphi(\varepsilon_1) = (a_{1,1}, a_{1,2}, 0, \ldots, 0),
\]

\[
\varphi(\varepsilon_2) = (0, a_{2,2}, a_{2,3}, 0, \ldots, 0),
\]

\[
\ldots,
\]

\[
\varphi(\varepsilon_i) = (0, \ldots, 0, a_{i,i}, a_{i,i+1}, 0, \ldots, 0),
\]

\[
\ldots,
\]

\[
\varphi(\varepsilon_{r-1}) = (0, \ldots, 0, a_{r-1,r-1}, a_{r-1,r}) \tag{3}
\]

with some \( a_{i,j} \in \mathbb{F}_p \setminus \{0\} \). Since the above generators are clearly linearly independent over \( \mathbb{F}_p \), we have \( \dim_{\mathbb{F}_p} \text{Coker} \varphi = 1 \). Hence \( F/k^+ \) is a cyclic extension of degree \( p \) by (2). The extension \( F/k^+ \) is unramified outside the primes \( l_1, \ldots, l_r \) by class field theory. In the case of \( r = 1 \), then the prime \( l_1 \) must ramify in \( F/k^+ \) because the class number of \( k^+ \) is prime to \( p \). In the case of \( r \geq 2 \), suppose that \( l_j \) is unramified in \( F/k^+ \) for some \( 1 \leq j \leq r \). Since the inertia subgroup of \( \text{Gal}(F/k^+) \) for the prime \( l_j \) is generated by the image of

\[
((0, \ldots, 0, 1, 0, \ldots, 0) \mod \varphi(E_{k^+})) \in \text{Coker} \varphi
\]

under the isomorphism \( \text{Coker} \varphi \simeq \text{Gal}(F/k^+) \) in (2), we have \((0, \ldots, 0, 1, 0, \ldots, 0) \in \varphi(E_{k^+})\). However, this contradicts the fact that \( \varphi(E_{k^+}) \) is generated by elements (3). Thus we conclude that \( F/k^+ \) is ramified at primes \( l_1, \ldots, l_r \).
Finally, we will show that the prime $p$ remains prime in $F/k^+$. It follows from condition (IV) that the class number of $\text{Gal}(F/k^+)$ is equal to the image of the class number of $\text{Gal}(F/k^+)/\mathbb{F}_p$ under the identification $(\mathcal{O}_{k^+}/m)^\times /\mathbb{F}_p$. Since $(p, F/k^+) \in \text{Gal}(F/k^+)$ is equal to the image of the class of $\alpha$ under the isomorphism $\text{Coker} \varphi \simeq \text{Gal}(F/k^+)$ in (2) and $\sum_{i=0}^{p-1} \tau_i = 0$, which follows from the fact that $\varphi(E_{k^+})$ is generated by elements (3), we deduce that $\text{Gal}(F/k^+) = ((p, F/k^+)) \simeq \mathbb{Z}/p$. Thus we have completed a proof of Lemma 2. □

**Lemma 3.** The class number of $F$ is prime to $p$.

**Proof.** Let $H$ be the genus $p$-class field of $F/k^+$, namely, the maximal unramified abelian $p$-extension of $F$ which is an abelian extension over $k^+$, and let $\tau$ be a generator of $\text{Gal}(F/k^+).$ Then it follows from class field theory that

$$A(F)/(\tau - 1)A(F) \simeq \text{Gal}(H/F).$$

Since the class number of $k^+$ is prime to $p$ by assumption (ii), $\sum_{i=0}^{p-1} \tau_i$ kills $A(F)$, from which we deduce that $p$ kills $A(F)/(\tau - 1)A(F) \simeq \text{Gal}(H/F)$. In addition, because $F/k^+$ is a ramified cyclic extension of degree $p$ by Lemma 2 and $H/F$ is unramified, the inertia subgroup of $\text{Gal}(H/k^+)$ for a ramified prime gives a splitting $\text{Gal}(H/k^+) \simeq \text{Gal}(H/F) \times \text{Gal}(F/k^+).$ Hence we conclude that $H/k^+$ is an elementary abelian $p$-extension of conductor dividing $m$, which implies $H = F$ by the definition of $F$. Therefore it follows from (4) and Nakayama’s lemma that the class number of $F$ is prime to $p$. □

Recall that $F_{\infty}$ and $X_{F_{\infty}}$ denote the cyclotomic $\mathbb{Z}_p$-extension of $F$ and the Iwasawa module of $F_{\infty}/F$, respectively, and that $F_n$ stands for the $n$th layer of $F_{\infty}/F$ for $n \geq 0$. It follows from Lemma 2(2) and assumption (iii) that there is a unique prime of $F$ lying over $p$. Then we see that the class number of $F_n$ is prime to $p$ by Iwasawa [4], because the class number of $F_{\infty}$ is prime to $p$ by Lemma 3. Hence $X_{F_{\infty}} \simeq \lim_{\leftarrow} A(F_n)/p = 0$.

We note that $F_k$ is a CM-field with the maximal real subfield $F$. Let $J$ be the generator of $\text{Gal}(F_k/F)$, and let $X_{(F_k)\infty} = X_{(F_k)\infty}^+ + X_{(F_k)\infty}^-$ be the decomposition of $X_{(F_k)\infty}$ with respect to the action of $J$ as usual. Then we have $X_{(F_k)\infty}^+ = X_{F_{\infty}}$, hence $X_{(F_k)\infty} = X_{(F_k)\infty}^-$. Similarly to the above, we have $X_{k_{\infty}} = X_{k_{\infty}}^-$ because $X_{k_{\infty}}^+ = 0$ by assumptions (ii), (iii), and Iwasawa [4]. We will finish the proof of Theorem 3 by using following Kida’s formula [7]:

**Theorem C.** Let $p$ be an odd prime number and $L/k$ a $p$-extension of CM-fields. Put $\lambda^- (L_{\infty}/L) = \dim \mathbb{Q}_p(X_{L_{\infty}}^- \otimes \mathbb{Q}_p)$ and $\lambda^- (k_{\infty}/k) = \dim \mathbb{Q}_p(X_{k_{\infty}}^- \otimes \mathbb{Q}_p)$, where $X_{L_{\infty}}^-$ and $X_{k_{\infty}}^-$ are the minus parts of the Iwasawa modules of the cyclotomic $\mathbb{Z}_p$-extensions $L_{\infty}/L$ and $k_{\infty}/k$, respectively. We write $\mu^- (L_{\infty}/L)$ and $\mu^- (k_{\infty}/k)$ for the $\mu$-invariants of the $L_{\infty}/L$-module $X_{L_{\infty}}^-$ and the $k_{\infty}/k$-module $X_{k_{\infty}}^-$, respectively. Assume that $\mu^- (k_{\infty}/k) = 0$. Then, $\mu^- (L_{\infty}/L)$ is also 0, and

$$\lambda^- (L_{\infty}/L) - \delta = [L_{\infty} : k_{\infty}] (\lambda^- (k_{\infty}/k) - \delta) + \sum_{\emptyset \neq \mathcal{L} \in \Gamma^+} (e(\mathcal{L}^+)) - 1),$$
where \( \delta \) is 1 or 0 according as \( \zeta_p \in k \) or not, \( e(\Sigma^+) \) denotes the ramification index of a prime \( \Sigma^+ \) of \( L_\infty^+ \) in \( L_\infty^+/k_\infty^+ \), and the sum \( \sum' \) is taken with respect to all the primes \( \Sigma^+ \) of \( L_\infty^+ \) which are not lying over \( p \), ramify in \( L_\infty^+/k_\infty^+ \), and split in \( L_\infty^+/L_\infty^+ \).

Now we apply Theorem C to the \( p \)-extension of CM-fields \( Fk/k \) of degree \( p \) (the \( \mu \)-invariant of \( k_\infty^+/k \) is 0 by assumption (i)).

We first see that \( \delta = 0 \) by assumption (iv). In the case of \( r = s \geq 1 \), the ramified primes of \( F_\infty \) in \( F_\infty/k_\infty^+ \) which are not lying over \( p \) and split in \( (Fk)_\infty/F_\infty \) are just the primes of \( F_\infty \) lying over \( l_1, \ldots, l_r \) by Lemma 2 and condition (V). The number of such primes are exactly \( r = s \) because \( l_i \) is totally ramified in \( F/k^+ \) and remains prime in \( k_\infty^+/k^+ \) by condition (II) and the fact \( Mk_1^+ = M(\zeta_{p^{\alpha+1}}^+) \).

In the case of \( s = 0 \), there are no ramified primes of \( F_\infty \) in \( F_\infty/k_\infty^+ \) which split in \( (Fk)_\infty \) by condition (V).

Therefore, we have

\[
\lambda^-(Fk)_\infty/Fk = p\lambda^-(k_\infty/k) + s(p - 1)
\]

(5)

by Theorem C. Since \( \mu((Fk)_\infty/Fk) = \mu^-(Fk)_\infty/Fk) = 0 \), \( \lambda(k_\infty/k) = \lambda^-(k_\infty/k) \), and \( \lambda(Fk)_\infty/Fk = \lambda^-(Fk)_\infty/Fk) \) by \( X_{k_\infty} = X_{k_\infty}^- \) and \( X_{(Fk)_\infty} = X_{(Fk)_\infty}^- \), we deduce that \( X_{(Fk)_\infty} = X_{(Fk)_\infty}^- \) is a free \( \mathbb{Z}_p \)-module of rank \( p\lambda(k_\infty/k) + s(p - 1) \) from (5) and the fact that \( X_{(Fk)_\infty}^- \) has no nontrivial finite \( \Lambda(Fk)_\infty/Fk \)-submodules (see [9, Proposition 13.28], for example). Thus we have completed the proof of Theorem 3.

References