Int. J. Open Problems Compt. Math., Vol. 2, No. 3, September 2009
ISSN 1998-6262; Copyright ©ICSRS Publication, 2009
www.i-csrs.org

Construction of Real Abelian Fields of Degree p With $\lambda_p = \mu_p = 0$

Manabu Ozaki

Department of Mathematics,
School of Science and Engineering,
Kinki University,
Kowakae 3-4-1, Higashi-Osaka, 577-8502, JAPAN
e-mail: ozaki@math.kindai.ac.jp

Abstract

For any prime number p, we shall construct a real abelian extension k over $\mathbb{Q}$ of degree p such that the Iwasawa module associated with the cyclotomic $\mathbb{Z}_p$-extension k_∞/k is finite and has arbitrarily large p-rank.

Keywords: *Iwasawa theory, $\mathbb{Z}_p$-extension, Greenberg's conjecture*
2000 Mathematics Subject Classification: *11R23, 11R29*

1 Introduction

In the theory of $\mathbb{Z}_p$-extensions, Greenberg's conjecture is one of the most fascinating open problem:

Greenberg's conjecture. For any totally real number field k and prime number p, the both of Iwasawa λ-invariant $\lambda_p(k)$ and μ-invariant $\mu_p(k)$ of the cyclotomic $\mathbb{Z}_p$-extension k_∞/k are vanished. In other words, the Galois group X_{k_∞} of the maximal unramified abelian p-extension over k_∞, which is called the Iwasawa module associated with k_∞/k, is finite.

In connection with this conjecture, many research papers, as Greenberg [3], Iwasawa [4], Ozaki-Taya [8], Yamamoto [10], Fukuda [1], [2], Komatsu [5], deal with the construction of families of totally real p-extension fields k over $\mathbb{Q}$ with $\lambda_p(k) = \mu_p(k) = 0$.

We are interested in not only constructing various families of totally real p-extension $k/\mathbb{Q}$ with $\lambda_p(k) = \mu_p(k) = 0$ but also what kind of finite $\mathbb{Z}_p$-modules appear as X_{k_∞}.

In the present paper, we shall construct real abelian extensions k over $\mathbb{Q}$ of degree p such that $\lambda_p(k) = \mu_p(k) = 0$ and the Iwasawa module associated with the cyclotomic $\mathbb{Z}_p$-extension k_∞/k has arbitrarily large p-rank. Our main result is;

Theorem 1. *Let p be any prime number. For any $M \geq 0$, there is a real abelian field k of degree p such that $\lambda_p(k) = \mu_p(k) = 0$, $p\text{-rank}\, X_{k_\infty} := \dim_{\mathbb{F}_p} X_{k_\infty}/pX_{k_\infty} \geq M$, and the prime p is inert in k, where X_{k_∞} is the Iwasawa module associated with the cyclotomic $\mathbb{Z}_p$-extension k_∞/k.*

We shall also give some applications of our construction.

2 Proof of Theorem 1.

We first introduce some notations, which we shall use below; In what follows, We fix a prime number p once for all. For any number field F, we denote by E_F, I_F and $\mathrm{Cl}(F)$ the unit group, the ideal group and the ideal class group of F, respectively, and we write $A(F)$ for the p-part of $\mathrm{Cl}(F)$. Let F_n denote the n-th layer of the cyclotomic $\mathbb{Z}_p$-extension F_∞/F for any number field F of finite degree and $n \geq 0$. For any module M, $r \in \mathbb{Z}$, and a prime number p, we put $M[r] = \{m \in M |\ rm = 0\}$ and $p\text{-rank}\, M = \dim_{\mathbb{F}_p} M/pM$. Also we define $M[p^\infty]$ to be $\bigcup_{n\geq 1} M[p^n]$.

Since $X_{k_\infty} \simeq \varprojlim A(k_n)$, the projective limit being taken with respect to the norm maps, and the norm map $A(k_m) \longrightarrow A(k_n)$ is surjective if k_∞/k_n is totally ramified at some prime, $p\text{-rank}\, X_{k_\infty} \geq M$ is equivalent to that $p\text{-rank}\, A(k_n) \geq M$ for such $n \geq 0$.

Assume that prime numbers q and r satisfy

(C1) $q \equiv 1 \pmod{2p^{N+1}},\ r \equiv 1 \pmod{2p},\ r \not\equiv 1 \pmod{2p^2}$,
(C2) $q^{\frac{r-1}{p}} \not\equiv 1 \pmod{r}$,
(C3) $p^{\frac{r-1}{p}} \not\equiv 1 \pmod{r}$,

for a given integer $N \geq 1$. Denote by $\mathbb{Q}^{(p)}(q)$ and $\mathbb{Q}^{(p)}(r)$ the real abelian fields of degree p with conductors q and r, respectively. Such abelian fields certainly exist by conditions (C1). Let k be a subfield of $\mathbb{Q}^{(p)}(q)\mathbb{Q}^{(p)}(r)$ with conductor qr such that $[k : \mathbb{Q}] = p$ and the prime p remains prime in k. Such k certainly exists because p remains prime in $\mathbb{Q}^{(p)}(r)$ by condition (C3), and, in the case where $p = 2$, the prime 2 splits in $\mathbb{Q}^{(p)}(q)$ by condition (C1). Then $\mathbb{Q}^{(p)}(q)\mathbb{Q}^{(p)}(r)$ is the genus p-class field of $k/\mathbb{Q}$, that is, the maximal abelian p-extension field over $\mathbb{Q}$ which is unramified over k, and we have

$\mathrm{Gal}(\mathbb{Q}^{(p)}(q)\mathbb{Q}^{(p)}(r)/k) \simeq A(k)/(\sigma-1)A(k)$ by class field theory, where σ is a generator of $\mathrm{Gal}(k/\mathbb{Q})$. Since the prime $\mathfrak{q}$ of k lying above q does not split in $\mathbb{Q}^{(p)}(q)\mathbb{Q}^{(p)}(r)/k$ by (C2), the ideal class containing the prime $\mathfrak{q}$ generates $A(k)/(\sigma-1)A(k)$, which implies that it generates $A(k)$ itself and that $A(k)$ is cyclic by Nakayama's lemma. We shall show that the prime $\mathfrak{q}$ capitulates in k_∞, which is equivalent to $\lambda_p(k)=\mu_p(k)=0$ by [3, Theorem 1], and that p-rank $A(k_N) \geq M$ under some additional conditions on q and N.

Lemma 1. *Let p be a prime number and F'/F a degree p cyclic extension of number fields of finite degree. We assume that $\lambda_p(F)=\mu_p(F)=0$. Let $\mathfrak{l}'$ be a prime ideal of F' which ramifies in F'/F. If $\mathfrak{l}'$ splits completely in F'_n and p-rank $A(F'_n) < p^n$ for some $n \geq 0$, then we have $\pi_{F'_\infty}(\mathfrak{l}')=0$ for the natural projection map $\pi_{F'_\infty} : I_{F'_\infty} \longrightarrow A(F'_\infty)$.*

Proof. Let $H_n = \mathrm{Ker}(j_{n,\infty} : A(F'_n) \longrightarrow A(F'_\infty))$, where $j_{n,\infty}$ is the natural map induced by the inclusion $I_{F'_n} \subseteq I_{F'_\infty}$. We write $\mathfrak{L}'$ for a prime of F'_n lying above $\mathfrak{l}'$. Since $\mathfrak{L}'^p \in I_{F_n}$ and $A(F_\infty)=0$ by our assumption $\lambda_p(F)=\mu_p(F)=0$, we have $\pi_{F'_n}(\mathfrak{L}')^p \in H_n$ for the natural projection map $\pi_{F'_n} : I_{F'_n} \longrightarrow A(F'_n)$. We consider the homomorphism $\psi : \mathbb{F}_p[\mathrm{Gal}(F'_n/F')] \longrightarrow (A(F'_n)/H_n)[p]$, $\alpha \mapsto \alpha\pi_{F'_n}(\mathfrak{L}') \mod H_n$. It follows from the assumption that

$$\#(A(F'_n)/H_n)[p] < p^{p^n} = \#\mathbb{F}_p[\mathrm{Gal}(F'_n/F')].$$

Hence $\mathrm{Ker}(\psi) \neq 0$, which implies $\mathrm{Ker}(\psi)^{\mathrm{Gal}(F'_n/F')} \neq 0$. Because

$$\mathbb{F}_p[\mathrm{Gal}(F'_n/F')]^{\mathrm{Gal}(F'_n/F')} = \mathbb{F}_p \sum_{\gamma \in \mathrm{Gal}(F'_n/F')} \gamma,$$

we have $\sum_{\gamma \in \mathrm{Gal}(F'_n/F')} \gamma \in \mathrm{Ker}(\psi)$. Therefore

$$\pi_{F'_n}(\mathfrak{l}') = \sum_{\gamma \in \mathrm{Gal}(F'_n/F')} \gamma\pi_{F'_n}(\mathfrak{L}') \in H_n,$$

which implies $\pi_{F'_\infty}(\mathfrak{l}')=0$. □

Since $\lambda_p(\mathbb{Q})=\mu_p(\mathbb{Q})=0$, and the prime $\mathfrak{q}$ splits completely in k_N by (C1), if p-rank $A(k_N) < p^N$ then $\mathfrak{q}$ capitulates in k_∞ and $\lambda_p(k)=\mu_p(k)=0$ by Lemma 1. Hence we shall control the p-rank of $A(k_N)$ in what follows.

Lemma 2. *We have*

$$\begin{aligned} p^N - p\text{-rank}\,(E_{\mathbb{Q}_N}/(E_{\mathbb{Q}_N} \cap N_{k_N/\mathbb{Q}_N}k_N^\times)) &\leq p\text{-rank}\,A(k_N) \\ &\leq p(p^N - p\text{-rank}\,(E_{\mathbb{Q}_N}/(E_{\mathbb{Q}_N} \cap N_{k_N/\mathbb{Q}_N}k_N^\times))). \end{aligned}$$

Proof. Since $A(\mathbb{Q}_N)$ is trivial, $A(k_N)/(\sigma-1)A(k_N)$ is an elementary abelian p-group. The number of primes of $\mathbb{Q}_N$ which ramify in k_N is p^N+1 because the prime q splits completely and the prime r remains prime in $\mathbb{Q}_N/\mathbb{Q}$ by (C1). Hence it follows from genus formula for $k_N/\mathbb{Q}_N$ that

$$p\text{-rank}\,A(k_N) \geq p\text{-rank}\,(A(k_N)/(\sigma-1)A(k_N)) \\ = p^N - p\text{-rank}\,(E_{\mathbb{Q}_N}/(E_{\mathbb{Q}_N}\cap N_{k_N/\mathbb{Q}_N}k_N^{\times})),$$

It follows from the filtration of submodules of $A(k_N)$

$$A(k_N) \supseteq (\sigma-1)A(k_N) \supseteq (\sigma-1)^2A(k_N)\cdots \supseteq (\sigma-1)^pA(k_N),$$

and $(\sigma-1)^pA(k_n)\subseteq pA(k_n)$ that

$$p\text{-rank}\,A(k_N) \leq p(p\text{-rank}\,(A(k_N)/(\sigma-1)A(k_N))).$$

Thus we have the lemma. □

Let γ be a fixed generator of $\mathrm{Gal}(k_N/k)$ and $(k_N)_{\overline{\mathfrak{Q}}_0}$ the completion of k_N at the unique prime $\overline{\mathfrak{Q}}_0$ above a fixed prime $\mathfrak{Q}_0$ of $\mathbb{Q}_N$ lying over q.

By virtue of Lemma 2, we can control the p-rank of $A(k_N)$ by controlling $E_{\mathbb{Q}_N}/E_{\mathbb{Q}_N}\cap N_{k_N/\mathbb{Q}_N}k_N^{\times}$. Hence we shall investigate the map

$$\rho : E_{\mathbb{Q}_N} \longrightarrow \mathrm{Gal}(k_N/\mathbb{Q}_N)^{\oplus p^N}, \rho(\varepsilon) = ((\gamma^{-i}(\varepsilon),(k_N)_{\overline{\mathfrak{Q}}_0}/\mathbb{Q}_q))_{i=0}^{p^N-1},$$

where $(*,(k_N)_{\overline{\mathfrak{Q}}_0}/\mathbb{Q}_q)$ denotes the local Artin symbol for $(k_N)_{\overline{\mathfrak{Q}}_0}/\mathbb{Q}_q$. Then it follows from the Hasse norm theorem and the product formula of the local Artin symbols that

$$\mathrm{Ker}(\rho) = E_{\mathbb{Q}_N}\cap N_{k_N/\mathbb{Q}_N}k_N^{\times},$$

since the ramified primes of $k_N/\mathbb{Q}_N$ are exactly the primes lying above q and the unique prime lying above r,

Hence we have

$$E_{\mathbb{Q}_N}/E_{\mathbb{Q}_N}\cap N_{k_N/\mathbb{Q}_N}k_N^{\times} \simeq \mathrm{Im}(\rho). \tag{2.1}$$

Let $\eta = N_{\mathbb{Q}(\zeta_{p^{N+1}})/\mathbb{Q}_N}(\zeta_{p^{N+1}}-1)^{\gamma-1}$ (when $p\neq 2$), or $\eta = \zeta_{2^{N+2}}^{-2}\dfrac{\zeta_{2^{N+2}}^5-1}{\zeta_{2^{N+2}}-1}$ (when $p=2$), where ζ_m denotes a primitive m-th root of unity for $m\geq 1$. Then $C_{\mathbb{Q}_N} = \langle -1, \gamma^i\eta | 0\leq i\leq p^N-2\rangle$ is the cyclotomic unit group of $\mathbb{Q}_N$ and $p\nmid [E_{\mathbb{Q}_N} : C_{\mathbb{Q}_N}]$ as well known. Hence we have $\mathrm{Im}(\rho) = \rho(C_{\mathbb{Q}_N}) = \rho(\mathbb{Z}[\mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q})]\eta)$ since $\rho(-1)=1$.

Lemma 3. *Let σ be a fixed generator of* $\mathrm{Gal}(k_N/\mathbb{Q}_N)$. *If we assume that*

$$(\gamma^{-j}\eta, (k_N)_{\overline{\mathfrak{Q}}_0}/\mathbb{Q}_q) = \begin{cases} \sigma\ (0 \le j \le p^{N-1}-1), \\ 1\ (p^{N-1} \le j \le p^N - 1). \end{cases} \tag{2.2}$$

Then we have p-rank$\,(E_{\mathbb{Q}_N}/E_{\mathbb{Q}_N} \cap N_{k_N/\mathbb{Q}_N} k_N^\times) = p^N - p^{N-1} + 1$.

Proof. It follows from the definition of the map ρ and (2.2) that

$$\rho(\gamma^i\eta) = \begin{cases} (1, \cdots, 1, \overset{i+1}{\check{\sigma}}, \cdots, \overset{i+p^{N-1}}{\check{\sigma}}, 1 \cdots, 1) \quad \text{if } 0 \le i \le p^N - p^{N-1}, \\ (\sigma, \cdots, \overset{i-(p^N-p^{N-1})}{\check{\sigma}}, 1, \cdots, \overset{i}{\check{1}}, \sigma, \cdots, \sigma) \\ \qquad\qquad\qquad\qquad \text{if } p^N - p^{N-1} + 1 \le i \le p^N - 1. \end{cases}$$

Clearly $\rho(\gamma^i\eta)$ $(0 \le i \le p^N - p^{N-1})$ are independent in $\mathrm{Gal}(k_N/\mathbb{Q}_N)^{\oplus p^N} \simeq (\mathbb{F}_p)^{\oplus p^N}$. For $p^N - p^{N-1} + 1 \le i \le p^N - 1$, we have

$$\rho(\gamma^i\eta) = \rho(\eta) \prod_{j=0}^{p-2} \left(\rho(\gamma^{(j+1)p^{N-1}}\eta)\rho(\gamma^{i-(p^N-p^{N-1})+jp^{N-1}}\eta)^{-1} \right).$$

Therefore $\mathrm{Im}(\rho)$ is generated by $\{\rho(\gamma^i\eta) |\ 0 \le i \le p^N - p^{N-1}\}$, from which we conclude that

$$\begin{aligned} p\text{-rank}\, E_{\mathbb{Q}_N}/E_{\mathbb{Q}_N} \cap N_{k_N/\mathbb{Q}_N} k_N^\times &= p\text{-rank Im}(\rho) \\ &= p\text{-rank } \rho(\mathbb{Z}[\mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q})]\eta) = p^N - p^{N-1} + 1 \end{aligned}$$

by using (2.1) □

If assumption (2.2) of Lemma 3 holds, then we have

$$p^{N-1} - 1 \le p\text{-rank}\, A(k_N) \le p^N - p < p^N$$

by Lemma 2. Hence it follows that $\lambda_p(k) = \mu_p(k) = 0$ and p-rank$\,X_{k_\infty} \ge p$-rank$\,A(k_N) \ge p^{N-1} - 1$. If we take an integer N so that $p^{N-1} - 1 \ge M$, the field k certainly satisfies the requirement of the statement of Theorem 1.

Now we choose primes q and r such that conditions (C1), (C2), (C3), and (2.2) hold.

Since $\gamma^{-i}\eta$ $(0 \le i \le p^N - 2)$ (and -1 if $p = 2$) are independent in $\mathbb{Q}_N(\zeta_p)^\times$ as well known, $\gamma^{-i}\eta \mod (\mathbb{Q}_N^\times)^p$ $(0 \le i \le p^N - 2)$ (and $-1 \mod (\mathbb{Q}_N^\times)^2$ if $p = 2$) are independent in $\mathbb{Q}_N^\times/(\mathbb{Q}_N^\times)^p$. Hence, by taking the norm $N_{\mathbb{Q}_N(\zeta_p)/\mathbb{Q}_N}$, we can see that $\gamma^{-i}\eta \mod (\mathbb{Q}_N(\zeta_p)^\times)^p$ $(0 \le i \le p^N - 2)$ (and $-1 \mod (\mathbb{Q}_N^\times)^2$ if $p = 2$) are independent also in $\mathbb{Q}_N(\zeta_p)^\times/(\mathbb{Q}_N(\zeta_p)^\times)^p$. Therefore there exists a degree one prime $\tilde{\mathfrak{Q}}$ of $\mathbb{Q}_N(\zeta_p)(=\mathbb{Q}(\zeta_{p^{N+1}})$ (if $p \neq 2$), $=\mathbb{Q}_N=\mathbb{Q}(\zeta_{2^{N+2}}+\zeta_{2^{N+2}}^{-1})$ (if $p=2$)) such that

$$\sqrt[p]{\gamma^{-i}\eta}^{\left(\frac{\mathbb{Q}_N\left(\sqrt[p]{\gamma^{-i}\eta},\zeta_p\right)/\mathbb{Q}_N(\zeta_p)}{\tilde{\mathfrak{Q}}}\right)-1}=\begin{cases}\zeta_p\ (0\le i\le p^{N-1}-1),\\ 1\ (p^{N-1}\le i\le p^N-2),\end{cases} \tag{2.3}$$

by Čebotarev density theorem, where $\left(\frac{*/*}{*}\right)$ denotes the Artin symbol. Note that $N(\tilde{\mathfrak{Q}})$ is a prime number with $N(\tilde{\mathfrak{Q}})\equiv 1 \pmod{p^{N+1}}$ (if $p\neq 2$), or $N(\tilde{\mathfrak{Q}})\equiv \pm 1 \pmod{2^{N+2}}$ (if $p=2$).

Furthermore, in the case where $p=2$, we can choose the prime $\tilde{\mathfrak{Q}}$ so that

$$\left(\frac{\mathbb{Q}_N(\sqrt{-1})/\mathbb{Q}_N}{\tilde{\mathfrak{Q}}}\right)=1, \tag{2.4}$$

which is equivalent to $N(\tilde{\mathfrak{Q}})\equiv 1 \pmod{2^{N+2}}$. We note that if $\tilde{\mathfrak{Q}}$ satisfies (2.3), then

$$\sqrt[p]{\gamma^{-(p^N-1)}\eta}^{\left(\frac{\mathbb{Q}_N\left(\sqrt[p]{\gamma^{-(p^N-1)}\eta},\zeta_p\right)/\mathbb{Q}_N(\zeta_p)}{\tilde{\mathfrak{Q}}}\right)-1}=1, \tag{2.5}$$

because $\prod_{i=0}^{p^N-1}\gamma^{-i}\eta=\pm 1$. We take the prime number $N(\tilde{\mathfrak{Q}})$ as a prime number q. Then $q\equiv 1 \pmod{2p^{N+1}}$. We choose a degree one prime $\mathfrak{r}$ of $\mathbb{Q}(\zeta_p)$ (degree one implies that $N(\mathfrak{r})$ is a prime number with $N(\mathfrak{r})\equiv 1 \pmod{p}$) such that

$$\left(\frac{\mathbb{Q}(\zeta_p,\sqrt[p]{p})/\mathbb{Q}(\zeta_p)}{\mathfrak{r}}\right)\neq 1, \left(\frac{\mathbb{Q}(\zeta_p,\sqrt[p]{q})/\mathbb{Q}(\zeta_p)}{\mathfrak{r}}\right)\neq 1,$$

which is equivalent to $p^{\frac{N(\mathfrak{r})-1}{p}}\not\equiv 1 \pmod{N(\mathfrak{r})}$ and $q^{\frac{N(\mathfrak{r})-1}{p}}\not\equiv 1 \pmod{N(\mathfrak{r})}$, respectively, and that

$$\left(\frac{\mathbb{Q}(\zeta_{p^2})/\mathbb{Q}(\zeta_p)}{\mathfrak{r}}\right)\neq 1 \text{ (if } p\neq 2) , \left(\frac{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}{\mathfrak{r}}\right)=1 \text{ (if } p=2),$$

which is equivalent to $N(\mathfrak{r})\not\equiv 1 \pmod{p^2}$ (when $p\neq 2$) and $N(\mathfrak{r})\equiv 1 \pmod{4}$ (when $p=2$), respectively. This is possible by the Čebotarev density theorem because $p \mod (\mathbb{Q}(\zeta_p)^\times)^p$, $q \mod (\mathbb{Q}(\zeta_p)^\times)^p$, and $\zeta_p \mod (\mathbb{Q}(\zeta_p)^\times)^p$ are independent in $\mathbb{Q}(\zeta_p)^\times/(\mathbb{Q}(\zeta_p)^\times)^p$ as one can see easily by taking the norm to $\mathbb{Q}$. We take the prime number $N(\mathfrak{r})$ as a prime number r. Then prime numbers q and r satisfy conditions (C1), (C2) and (C3) (In the case where $p=2$, it follows from $2^{\frac{N(\mathfrak{r})-1}{2}}\not\equiv 1 \pmod{N(\mathfrak{r})}$ that $N(\mathfrak{r})\not\equiv 1 \pmod{8}$). And let k be a real abelian field of degree p with conductor qr in which the prime p does not split. We shall verify the field k and a certain prime $\mathfrak{Q}_0$ of $\mathbb{Q}_N$ lying above q satisfy the assumption (2.2) of Lemma 3 in the following.

Let us take the prime of $\mathbb{Q}_N$ below $\tilde{\mathfrak{Q}}$ as $\mathfrak{Q}_0$, and let $\delta \in \mathbb{Q}_q$ be a uniformizer such that $\mathbb{Q}_q(\sqrt[p]{\delta}) = (k_N)_{\overline{\mathfrak{Q}}_0}$. Then we can see

$$\sqrt[p]{\delta}^{(\gamma^{-i}\eta,\,(k_N)_{\overline{\mathfrak{Q}}_0}/\mathbb{Q}_q)-1} = \sqrt[p]{\gamma^{-i}\eta}^{\,1-\left(\frac{\mathbb{Q}_N(\sqrt[p]{\gamma^{-i}\eta},\zeta_p)/\mathbb{Q}_N(\zeta_p)}{\tilde{\mathfrak{Q}}}\right)}$$

by a property of local and global Artin symbols. Therefore we see that

$$(\gamma^{-i}\eta, (k_N)_{\overline{\mathfrak{Q}}_0}/\mathbb{Q}_q) = (\eta, (k_N)_{\overline{\mathfrak{Q}}_0}/\mathbb{Q}_q) \neq 1$$

for $1 \leq i \leq p^{N-1} - 1$, and $(\gamma^{-i}\eta, (k_N)_{\overline{\mathfrak{Q}}_0}/\mathbb{Q}_q) = 1$ for $p^{N-1} \leq i \leq p^N - 1$ by (2.3) and (2.5). Therefore condition (2.2) holds. Thus the above abelian field k satisfies $\lambda_p(k) = \mu_p(k) = 0$ and p-rank $X_{k_\infty} \geq p$-rank $A(k_N) \geq p^{N-1} - 1 \geq M$. We have completed the proof of Theorem 1.

3 Applications of Theorem 1

We shall give some applications of Theorem 1 in this section.

As a corollary to Theorem 1, we have the following result on the maximal unramified p-extensions of $\mathbb{Z}_p$-extension fields over totally real number fields:

Corollary 1. *For any prime number p, there exists a real abelian fields k with $[k : \mathbb{Q}] = p$ such that the maximal unramified abelian p-extension $L(k_\infty)/k_\infty$ is finite but the maximal unramified p-extension $\tilde{L}(k_\infty)/k_\infty$ is infinite, k_∞ being the cyclotomic $\mathbb{Z}_p$-extension field of k.*

Proof. In the proof of Theorem 1, we have shown that for any given number N, there exists a real abelian field k of degree p such that $\lambda_p(k) = \mu_p(k) = 0$ and p-rank $A(k_N) \geq p^{N-1} - 1$. If we choose N so that $p^{N-1} - 1 \geq 2 + 2\sqrt{r(k_N)}$, $r(k_N) = p^{N+1}$ being the number of archimedean places of k_N, it follows from Golod-Shafarevich criterion (see for example [7, Theorem (10.8.6)]) that the maximal unramified p-extension $\tilde{L}(k_N)$ over k_N is infinite. Therefore the extension $\tilde{L}(k_\infty)/k_\infty$ is infinite since $\tilde{L}(k_N)k_\infty \subseteq \tilde{L}(k_\infty)$. Also, the finiteness of $[L(k_\infty) : k_\infty]$ follows from the condition $\lambda_p(k) = \mu_p(k) = 0$. □

Remark 1. Mizusawa [6] give an different type example of $\mathbb{Z}_p$-extension field k_∞ with $[L(k_\infty) : k_\infty] < \infty$ and $[\tilde{L}(k_\infty) : k_\infty] = \infty$. Let $p = 3$ and $k = \mathbb{Q}(\sqrt{39345017})$. In this case, $\tilde{L}(k)/k$ is an infinite extension. Mizusawa verified $\lambda_3(k) = \mu_3(k) = 0$ by numerical computation. Hence $[L(k_\infty) : k_\infty] < \infty$ and $[\tilde{L}(k_\infty) : k_\infty] = \infty$ for the cyclotomic $\mathbb{Z}_3$-extension k_∞ over k.

We also obtain a result concerning the delay of the stabilization of $\#A(k_n)$ in the Iwasawa class number formula as a corollary to Theorem 1.

For any number field k and prime number p, we let $n_0(k,p)$ be the minimum non-negative integer such that

$$\mathrm{Cl}(k_n)[p^\infty] = p^{\lambda_p(k)n+\mu_p(k)p^n+\nu_p(K)}$$

for all $n \geq n_0(k,p)$, where k_n is the n-th layer of the cyclotomic $\mathbb{Z}_p$-extension k_∞/k, and $\lambda_p(k)$, $\mu_p(k)$ and $\nu_p(k)$ denote Iwasawa invariants of k_∞/k.

Corollary 2. *For any prime number p and integer M, there exists a real abelian field k of degree p such that $\lambda_p(k) = \mu_p(k) = 0$ and $n_0(k,p) \geq M$*

Proof. By the construction in the proof of Theorem 1, for any give $N \geq 1$, there exists a real abelian field k of degree p such that $\lambda_p(k) = \mu_p(k) = 0$, p-rank $A(k_N) \geq p^{N-1} - 1$, $A(k)$ is a cyclic group, and the prime p remains prime in k. Since k_∞ has a unique prime lying over p, we have

$$A(k_n) \simeq X_{k_\infty}/(\gamma^{p^n} - 1)X_{k_\infty},$$

where γ is a fixed generator of $\Gamma := \mathrm{Gal}(k_\infty/k)$. It follows from the above isomorphism and the cyclicity of $A(k)$ that X_{k_∞} is a cyclic $\mathbb{Z}_p[[\Gamma]]$-module by Nakayama's lemma, $\mathbb{Z}_p[[\Gamma]]$ being the completed group ring of Γ over $\mathbb{Z}_p$. Hence, by using the assumption $\# X_{k_\infty} < \infty$, we may assume that

$$X_{k_\infty}/pX_{k_\infty} \simeq \mathbb{F}_p[[\Gamma]]/(\gamma - 1)^e,$$

for some $e \geq 0$. Thus we have

$$A(k_n)/pA(k_n) \simeq \mathbb{F}_p[[\Gamma]]/((\gamma-1)^e,\, (\gamma-1)^{p^n}) = \mathbb{F}_p[[\Gamma]]/(\gamma-1)^{\min\{e,p^n\}}$$

for $n \geq 0$, from which we find that

$$e \geq \min\{e, p^N\} = p\text{-rank}\, A(k_N) \geq p^{N-1} - 1. \tag{3.1}$$

On the other hand, we see that

$$p^{n_0(k,p)} \geq e, \tag{3.2}$$

since

$$\begin{aligned}\min\{e, p^{n_0(k,p)}\} &= p\text{-rank}\, A(k_{n_0(k,p)}) \\ &= p\text{-rank}\, A(k_{n_0(k,p)+1}) = \min\{e, p^{n_0(k,p)+1}\}.\end{aligned}$$

Thus we conclude from (3.1) and (3.2) that

$$p^{n_0(k,p)} \geq p^{N-1} - 1.$$

Because N is an arbitrarily given number, the proof have been completed. □

Example 1. Here we give an example of Theorem 1. Let $p = 2$ and $k = \mathbb{Q}(\sqrt{5 \cdot 732678913})$ (732678913 is a prime number). Then we can see that $\lambda_2(k) = \mu_2(k) = 0$ and 2-rank $X_{k_\infty} = 19$, where k_∞/k is the cyclotomic $\mathbb{Z}_2$-extension (cf. Theorem 1).

For this real quadratic field k, we see that $[L(k_\infty) : k_\infty] < \infty$ and $[\tilde{L}(k_\infty) : k_\infty] = \infty$, where $L(k_\infty)/k_\infty$ and $\tilde{L}(k_\infty)/k_\infty$ are the maximal unramified abelian 2-extension and the maximal unramified 2-extension, respectively (cf. Corollary 1).

Also we find that $n_0(k, 2) \geq 5$ (cf. Corollary 2). Specifically, we can see 2-rank $\mathrm{Cl}(k_n) = 2^n$ for $0 \leq n \leq 4$ and 2-rank $\mathrm{Cl}(k_n) = 19$ for $n \geq 5$.

4 Open Question

The paper [9] shows that for any given finite $\mathbb{Z}_p$-module X there exists a totally real number field k of finite degree such that $X_{k_\infty} \simeq X$. The author would like to know whether we can always choose the above k to be a real abelian field of degree p.

ACKNOWLEDGMENTS. The author would like to express thanks to Professor Ralph Greenberg for improving an earlier version of Lemma 1. The proof of Lemma 1 included in this paper was given by him.

References

[1] T. Fukuda, On the vanishing of Iwasawa invariants of certain cyclic extensions of $\mathbb{Q}$ with prime degree, *Proc. Japan Acad.*, **73** (1997), 108–110.

[2] T. Fukuda, On the vanishing of Iwasawa invariants of certain cyclic extensions of $\mathbb{Q}$ with prime degree II, *Proc. Japan Acad.*, **74** (1997), 160–164.

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

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

[5] K. Komatsu, On the Iwasawa λ-invariants of quaternion extensions, *Acta. Arith.*, **87** (1999), 219–221.

[6] Y. Mizusawa, On Greenberg's conjecture on a certain real quadratic field, *Proc. of Japan Acad.*, **76** (2000), 163–164.

[7] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of Number Fields*, Grundlehren der mathematischen Wissenschaften 323, Springer-Verlag, Berlin Heidelberg, 2000. ‘

[8] M. Ozaki and H. Taya, On the Iwasawa λ_2-invariant of certain families of real quadratic fields, *Manuscripta Math.* **94** (1997), 437–444.

[9] M. Ozaki, Construction of $\mathbb{Z}_p$-extensions with prescribed Iwasawa modules, *J. Math. Soc. Japan* **56** (2004), 787–801.

[10] G. Yamamoto, On the vanishing of Iwasawa invariants of certain (p,p)-extensions of $\mathbb{Q}$. *Proc. Japan Acad.*, **73** (1997), 45–47.