TITLE:
ON THE VANISHING OF IWASAWA INVARIANTS OF ABSOLUTELY ABELIAN $p$-EXTENSIONS (Algebraic Number Theory and Related Topics)

AUTHOR(S):
Yamamoto, Gen

CITATION:

ISSUE DATE:
1999-04

URL:
http://hdl.handle.net/2433/63020

RIGHT:
ON THE VANISHING OF IWASAWA INVARIANTS OF ABSOLUTELY ABELIAN $p$-EXTENSIONS

GEN YAMAMOTO (山本 惠)

ABSTRACT. Let $p$ be any odd prime. We determine all absolutely abelian $p$-extension fields such that Iwasawa $\lambda_p$, $\mu_p$ and $\nu_p$-invariants of the cyclotomic $\mathbb{Z}_p$-extension are zero, in terms of congruent conditions, $p$-th power residues, and genus fields.

1. INTRODUCTION

Let $p$ be a prime and $\mathbb{Z}_p$ the ring of $p$-adic integers. Let $k$ be a finite extension of the rational number field $\mathbb{Q}$, $k_\infty$ a $\mathbb{Z}_p$-extension of $k$, $k_n$ the $n$-th layer of $k_\infty/k$, and $A_n$ the $p$-Sylow subgroup of the ideal class group of $k_n$. Iwasawa proved the well-known theorem about the order $\#A_n$ of $A_n$ that there exist integers $\lambda = \lambda(k_\infty/k) \geq 0$, $\mu = \mu(k_\infty/k) \geq 0$, $\nu = \nu(k_\infty/k)$, and $n_0 \geq 0$ such that

$$\#A_n = p^{\lambda n + \mu p^n + \nu}$$

for all $n \geq n_0$. These integers $\lambda = \lambda(k_\infty/k)$, $\mu = \mu(k_\infty/k)$ and $\nu = \nu(k_\infty/k)$ are called Iwasawa invariants of $k_\infty/k$ for $p$. If $k_\infty$ is the cyclotomic $\mathbb{Z}_p$-extension of $k$, we write $\lambda_p(k)$, $\mu_p(k)$ and $\nu_p(k)$ for the above invariants, respectively.

In [7], Greenberg conjectured that if $k$ is a totally real, $\lambda_p(k) = \mu_p(k) = 0$. We call this conjecture Greenberg conjecture. For Iwasawa $\lambda_p$, $\mu_p$-invariants of abelian $p$-extension fields of $\mathbb{Q}$, there are results by Greenberg ([7], V), Iwasawa([9]), Fukuda, Komatsu, Ozaki and Taya([6]), Fukuda([4]), and the author([12]), etc. On the other hand, Ferrero and Washington have shown that $\mu_p(k) = 0$ for any abelian extension field $k$ of $\mathbb{Q}$.

In this paper, we will consider a stronger condition than Greenberg conjecture that $\lambda_p(k) = \mu_p(k) = \nu_p(k) = 0$ and determine all absolutely abelian $p$-extensions $k$, i.e. $k$ is an abelian extension of the rational number field $\mathbb{Q}$, with $\lambda_p(k) = \mu_p(k) = \nu_p(k) = 0$ for an odd prime $p$, using the results of G. Cornell and M. Rosen([1]).

2. MAIN THEOREM

Throughout this section, we fix an odd prime $p$. For an absolutely abelian $p$-extension field $k$, let $f_k$ be its conductor, i.e. $f_k$ is the minimum positive integer with $k \subseteq \mathbb{Q}(\zeta_{f_k})$. Then, it follows easily that $f_k = p^a p_1 \cdots p_t$, where $a$ is a non-negative integer and $p_1, \cdots, p_t$ are distinct primes which are congruent to 1 modulo $p$. We denote $k_G$ by the genus field of $k$. So $k_G$ is the maximal unramified abelian extension of $k$ such that $k_G/\mathbb{Q}$ is an abelian extension. In general, if $k/\mathbb{Q}$ is an abelian extension of odd degree, then
it has shown by Leopoldt that

$$[k_G : k] = \prod_{i=1}^{e_t} e_i$$

where \(e_1, \ldots, e_t\) are ramification indices of primes which ramify in \(k/\mathbb{Q}\). Hence in our case, \(k_G\) is also an abelian \(p\)-extension of \(\mathbb{Q}\). For instance we denote by \((\cdot)_{p}\) the \(p\)-th power residue symbol, i.e., for integers \(x, y\), \((\frac{x}{y})_{p} = 1\) if and only if \(x\) is the \(p\)-th power modulo \(y\).

Our main theorem gives a necessary and sufficient condition for \(\lambda_p(k) = \mu_p(k) = \nu_p(k) = 0\) in terms of \(p\)-th power residue symbol, congruent conditions and genus fields:

**Theorem 1.** Let \(k\) be an abelian \(p\)-extension of \(\mathbb{Q}\), and \(f_k = p^ap_1 \cdots p_t\) the prime decomposition of its conductor, where primes \(p_1, \ldots, p_t\) are distinct. If

\[
\lambda_p(k) = \mu_p(k) = \nu_p(k) = 0,
\]

then \(t \leq 2\). Conversely, in each case of \(t = 0\) or \(1\) or \(2\), the followings are a necessary and sufficient condition of (1):

In case of \(t = 0\) : (1) holds.

In case of \(t = 1\) : (1) is equivalent to \(k = k_{1,G}\) and,

\[
\left( \frac{p}{p_1} \right) \neq 1 \text{ or } p_1 \neq 1 \pmod{p^2}.
\]

In case of \(t = 2\) : (1) is equivalent to \(k = k_{1,G}\), and for \((i, j) = (1, 2)\) or \((2, 1)\),

\[
\left( \frac{p}{p_i} \right) \neq 1, \left( \frac{p_j}{p_i} \right) \neq 1, p_j \neq 1 \pmod{p^2},
\]

and, there exist \(x, y, z \in \mathbb{F}_p\) such that

\[
\left( \frac{p_ip_j^y}{p_i} \right) = 1, \left( \frac{p_i^y}{p_j} \right) = 1, p_ip_j^y \equiv 1 \pmod{p^2}, \text{ and } xyz \neq -1 \text{ in } \mathbb{F}_p.
\]

In case of \(t = 2\), the conditions in Theorem 1 are complicated. So we will give an example. We consider the case \(p = 3, p_1 = 7\) and \(p_2 = 19\). We denote \(k_7\) (resp. \(k_{19}\)) by the subfield of \(\mathbb{Q}(\zeta_7)\) (resp. \(\mathbb{Q}(\zeta_{19})\)) with degree 3 over \(\mathbb{Q}\). As for the condition \(k_1 = k_{1,G}\), there exists a field \(F\) such that \(k_7 \subset F \subset k_7k_{19}\mathbb{Q}_1\) and \(F \neq k_7k_{19}, k_7\mathbb{Q}_1\), where \(\mathbb{Q}_1\) is the first layer of cyclotomic \(\mathbb{Z}_3\)-extension of \(\mathbb{Q}\). Then \(k_7k_{19}\mathbb{Q}_1/F\) is a nontrivial unramified extension and \(k_7k_{19}\mathbb{Q}_1\) is abelian, hence \(F \subset k_7k_{19}\mathbb{Q}_1 \subset F_G\). But, for \(F_1 = k_7k_{19}\mathbb{Q}_1\), it follows easily that \(F_1 = F_{1,G}\). If we restrict the case \(p\) is unramified in \(k\), i.e. \(a = 0\), then the statement \(k_1 = k_{1,G}\) can be simplified to \(k = k_G\) because \(k_1 = k\mathbb{Q}_1\). This restriction is not so strong: In general, for an absolutely abelian \(p\)-extension field \(k\), there exists an absolutely abelian extension field \(k'\) such that \(p\) is unramified in \(k'\) and \(k_{\infty} = k'_{\infty}\). Note that if \(k\) is the maximal subfield of \(\mathbb{Q}(\zeta_m)\) (\(m = p^ap_1 \cdots p_t\) as above) which is abelian \(p\)-extension of \(\mathbb{Q}\), then \(k = k_G\).

We continue to examine the above example. If we put \((i, j) = (1, 2)\), then \(p_1 = 19 \equiv 1 \pmod{3^2}\), so the condition (3) is not satisfied. But if we put \((i, j) = (2, 1)\), then we can
verify that \( p_i = 19 \) and \( p_j = 7 \) satisfy the conditions (3) and (4). Hence, for example, if \( K \) is the maximal subfield of \( \mathbb{Q}(\zeta_{7\cdot 19}) \) which is 3-extension of \( \mathbb{Q} \), then \( K \) satisfies the conditions of Theorem 1. Therefore we get

\[
\lambda_p(K) = \mu_p(K) = \nu_p(K) = 0.
\]

As for Greenberg conjecture, we can also get the following: In general, it is known that if \( L \subseteq M \) then \( \lambda_p(L) \leq \lambda_p(M) \) and \( \mu_p(L) \leq \mu_p(M) \) for number fields \( L, M \). Hence for any subfield \( k \) of \( \mathbb{Q}(\zeta_{7\cdot 19}) \) which is 3-extension of \( \mathbb{Q} \), i.e. \( k \subseteq K \), then \( \lambda_p(k) = \mu_p(k) = 0 \). This consideration is generalized as follows:

**Corollary 2.** Let \( m = p^a p_1 \cdots p_i \) satisfy the condition (2) or (3), (4). Then for any subfield \( k \) of \( \mathbb{Q}(\zeta_m) \) which is \( p \)-extension of \( \mathbb{Q} \), Greenberg conjecture for \( k \) and \( p \) is valid.

### 3. The results of G. Cornell and M. Rosen

In this section, we review briefly part of [1]. Let \( K/\mathbb{Q} \) be an abelian \( p \)-extension, \( p \) a prime. In the 1950’s, A. Fröhlich determined all such fields with class number prime to \( p \) (cf. [2]). In [1], G. Cornell and M. Rosen reconsidered this problem in the case where \( p \) is an odd prime, and reduced the problem to the case when \( \text{Gal}(K/\mathbb{Q}) \) is an elementary abelian \( p \)-group, i.e. \( \text{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^m \) for some integer \( m \).

We suppose that \( p \) is an odd prime and \( \text{Gal}(K/\mathbb{Q}) \) is an abelian \( p \)-group. Then the genus field \( K_G \) of \( K \) is also abelian \( p \)-extension. If \( p \) does not divide the class number \( h_K \) of \( K \), then \( K \) does not have any non-trivial unramified abelian \( p \)-extension by class field theory, hence \( K_G = K \). In the following we will assume \( K_G = K \). Further, we consider the central \( p \)-class field \( K_C \) of \( K \), i.e. \( K_C \) is the maximal \( p \)-extension of \( K \) such that \( K_C/K \) is abelian and unramified, \( K_C/\mathbb{Q} \) is Galois and \( \text{Gal}(K_C/K) \) is in the center of \( \text{Gal}(K_C/\mathbb{Q}) \). Since a \( p \)-group must have a lower central series that terminates in the identity, one sees that \( p \nmid h_K \) if and only if \( K_C = K \). So we are interested in which case \( K_C = K \). This can be reduced the case when \( \text{Gal}(K/\mathbb{Q}) \) is an elementary abelian \( p \)-group by the following result:

**Lemma 3 ([1] Theorem 1).** Let \( K/\mathbb{Q} \) be an abelian \( p \)-extension with \( K_G = K \). Let \( k \) be the maximal intermediate extension between \( \mathbb{Q} \) and \( K \) such that \( \text{Gal}(k/\mathbb{Q}) \) is an elementary abelian \( p \)-group. Then \( p \)-rank of \( \text{Gal}(K_C/K) \) is equal to the \( p \)-rank of \( \text{Gal}(k_C/k) \).

In the case \( \text{Gal}(K/\mathbb{Q}) \) is an elementary abelian \( p \)-group, by the results of Furuta and Tate, we have the following lemma:

**Lemma 4 ([1] Section 1).** Let \( K \) be an absolutely abelian \( p \)-extension such that \( \text{Gal}(K/\mathbb{Q}) \) is an elementary abelian \( p \)-group and \( K_G = K \). Then, we have

\[
\text{Gal}(K_C/K) \cong \text{Coker}(\bigoplus_{i=1}^a \wedge^2(G_i) \longrightarrow \wedge^2(G)),
\]

where \( G_i \)'s are the decomposition groups of primes ramified in \( K/\mathbb{Q} \) and \( G = \text{Gal}(K/\mathbb{Q}) \).
We will assume $\text{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^m$. Let $p_1, \cdots, p_t$ be the primes ramified in $K$ and $h_K$ the class number of $K$. From genus theory, it follows that if $h_K$ is not divisible by $p$, then $t = m$. Also it follows that if $m \geq 4$ then $p$ divides $h_K$ by Lemma 4. So, we assume $t = m$ and $m = 2$ or 3. (In case of $t = m = 1$, $p \not| h_K$. cf. [8].)

**Lemma 5 ([1] Proposition 2).** Suppose $m = 2$ and $p_i \neq p$ for $i = 1, 2$. Then $p|h_K$ if and only if $(\mathbb{Q}_p/p_1^2)_p = 1$ and $(\mathbb{Q}_p/p_2)_p = 1$.

Next, we consider the case where one of the ramified primes is $p$. Suppose $m = 2$ and $p$ and $p_1$ are the only primes ramified in $K$. Then we can get easily $K = k(p_1)\mathbb{Q}_1$ and $p_1 \equiv 1 \pmod{p}$, where $k(p_1)$ is the unique subfield of $\mathbb{Q}(\zeta_{p_1})$ which is cyclic over $\mathbb{Q}$ of degree $p$, $\zeta_{p_1}$ is a primitive $p_1$-th root of unity, and $\mathbb{Q}_1$ is the first layer of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$.

**Lemma 6 ([1] Proposition 3).** Suppose $m = 2$ and $p$ and $p_1$ are the only primes ramified in $K$. Then $p|h_K$ if and only if $(\mathbb{Q}_p/p_1)_p = 1$ and $p_1 \equiv 1 \pmod{p^2}$.

Suppose $t = m = 3$ and $p_1, p_2$ and $p_3$ all the primes ramified in $K$. We put $D_{p_i}$, the decomposition field of $p_i$ ($i = 1, 2, 3$) in $K$. In [1], the following simple result is given:

**Lemma 7 ([1] Theorem 2).** Suppose $t = m = 3$. Following statements (a) and (b) are equivalent:

(a) $h_K$ is not divisible by $p$,

(b) $[D_{p_1} : \mathbb{Q}] = [D_{p_2} : \mathbb{Q}] = [D_{p_3} : \mathbb{Q}] = p$ and $D_{p_1}D_{p_2}D_{p_3} = K$.

In the next section, we shall prove Theorem 1, using these results.

4. **Proof of Theorem 1**

Notations are as in previous section.

Firstly, we suppose $\lambda_p(k) = \mu_p(k) = \nu_p(k) = 0$. Clearly, this condition is equivalent to $A(k_n) = 0$ for any sufficiently large $n$. Then, $k_n$ satisfies $k_n = k_{n,G}$ and $k_1 = k_{1,G}$, because all ramified primes are totally ramified in $k_n/k_1$. Since $k_n$ is also an abelian $p$-extension of $\mathbb{Q}$, we can apply the results of Cornell-Rosen:

Let $L$ be the maximal subfield of $k_n$ such that $\text{Gal}(L/\mathbb{Q})$ is an elementary abelian extension of $\mathbb{Q}$. Since $k_n = k_{n,G}$, $\text{Gal}(k_n/\mathbb{Q})$ is the direct sum of the inertia groups of primes ramified in $k_n/\mathbb{Q}$, hence it follows that $L = k(p_1) \cdots k(p_t)\mathbb{Q}_1$. By Lemma 3, $A(k_n) = 0$ is equivalent to $p|\parallel h_L$. Note that if $t \geq 3$ then we always have $p|\parallel h_L$ as in the previous section. Hence we may examine in each case of $t = 0$ or 1 or 2.

If $t = 0$ then $L = \mathbb{Q}_1$, hence it is well known that $A(L) = A(\mathbb{Q}_1) = 0$ (cf. [8]).

If $t = 1$ then $L = k(p_1)\mathbb{Q}_1$. By lemma 6, we get the statement in Theorem 1.

In the following we assume that $t = 2$. In this case, $L = k(p_1)k(p_2)\mathbb{Q}_1$. Let $G_p, G_{p_i}$ ($i = 1, 2$) be the decomposition groups for $p, p_i$ in $\text{Gal}(L/\mathbb{Q})$ and let $D_p, D_{p_i}$ be the fixed field of $G_p, G_{p_i}$, respectively. We note that $D_p \subset k(p_1)k(p_2)\mathbb{Q}_1$ and $D_{p_i} \subset k(p_1)k(p_2)\mathbb{Q}_1$.

Now, from our assumption $p|\parallel h_L$, we have $[D_p : \mathbb{Q}] = [D_{p_1} : \mathbb{Q}] = [D_{p_2} : \mathbb{Q}] = p$ and $D_pD_{p_1}D_{p_2} = L$ by Lemma 7. Here, we assume that either $(\mathbb{Q}_p/p_1)_p = 1$ or $(\mathbb{Q}_p/p_2)_p = 1$ or
\(p_2 \equiv 1 \pmod{p^2}\) holds, and either \((\frac{p_2}{p_1})_p = 1\) or \((\frac{p_1}{p_2})_p = 1\) or \(p_1 \equiv 1 \pmod{p^2}\). This is equivalent to

\[D_p = k(p_1) \text{ or } D_{p_1} = k(p_2) \text{ or } D_{p_2} = \mathbb{Q}_1\]  
for \((i, j) = (1, 2)\) and \((2, 1)\),

(5)

because \([D_p : \mathbb{Q}] = [D_{p_1} : \mathbb{Q}] = [D_{p_2} : \mathbb{Q}] = p\).

If \(D_p = k(p_1)\), then \(D_{p_2} \neq k(p_1)\) because \(D_p D_{p_1} D_{p_2} = L\). Hence by (5) (put \((i, j) = (2, 1)\)), we have \(D_{p_1} = \mathbb{Q}_1\). Then \(D_{p_2} \subseteq k(p_1)\mathbb{Q}_1 = D_p D_{p_1}\), which contradicts \(D_p D_{p_1} D_{p_2} = L\). In the same way, if \(D_p = k(p_2)\), then \(D_{p_1} \neq k(p_2)\) and we have \(D_{p_2} = \mathbb{Q}_1\) by (5), which contradicts. Thus, it follows that the assumption (5) cause contradiction. Therefore, for \((i, j) = (1, 2)\) or \((2, 1)\), \((\frac{p}{p_1})_p \neq 1\), \(p \neq 1\), and \(p_j \not\equiv 1 \pmod{p^2}\).

Without loss of generality, we may assume \((i, j) = (1, 2)\). Since \((\frac{p}{p_1})_p \neq 1\), \(p\) is inert in \(k(p_1)\). Hence \(\sigma = (\frac{k(p_1)/\mathbb{Q}}{p}) \neq 1\), where \((\frac{k(p_1)/\mathbb{Q}}{p})\) is the Artin symbol, and \(\sigma\) generates \(\text{Gal}(k(p_1)/\mathbb{Q})\). We often regard \(\sigma >\) \(\text{Gal}(k(p_1)/k(p_2))\) or \(\text{Gal}(L/k(p_2)\mathbb{Q}_1)\) in the natural way. Similarly, we put \(\tau = (\frac{k(p_2)/\mathbb{Q}}{p_1})\) and \(\eta = (\frac{\mathbb{Q}_1/\mathbb{Q}}{p_2})\), then \(\sigma >\) \(\text{Gal}(k(p_2)/\mathbb{Q})\) and \(\eta >\) \(\text{Gal}(\mathbb{Q}_1/\mathbb{Q})\).

Since \((\frac{p}{p_1})_p \neq 1\), there exists \(x \in \mathbb{F}_p\) such that \((\frac{p_1 p}{p^2})_p = 1\). Then

\[
\left(\frac{p_2 p^x}{p_1}\right)_p = 1 \iff \left(\frac{k(p_1)/\mathbb{Q}}{p_2 p^x}\right) = \left(\frac{k(p_1)/\mathbb{Q}}{p_2}\right) \left(\frac{k(p_1)/\mathbb{Q}}{p}\right)^x = 1.
\]

Therefore \((\frac{k(p_1)/\mathbb{Q}}{p_2})_p = \sigma^{-x}\). Similarly, we obtain \(y, z \in \mathbb{F}_p\) such that \((\frac{p_2 p^y}{p_1})_p = 1\) and \(p_1 p_2^y \equiv 1 \pmod{p^2}\), and hence \((\frac{k(p_2)/\mathbb{Q}}{p_1})_p = \tau^{-y}\) and \((\frac{\mathbb{Q}_1/\mathbb{Q}}{p_2})_p = \eta^{-z}\).

Since \((\frac{k(p_1)/k(p_2)/\mathbb{Q}}{p})_p = (\frac{k(p_1)/\mathbb{Q}}{p}) (\frac{k(p_2)/\mathbb{Q}}{p}) = \sigma \tau^{-y}\), \(D_p\) is the fix field of \(\sigma \tau^{-y}\) in \(k(p_1)k(p_2)\). Therefore, when we consider \(G_p\) in \(\text{Gal}(L/\mathbb{Q})\),

\[G_p = \langle \eta, \sigma \tau^{-y} \rangle .\]

And similarly,

\[G_{p_1} = \langle \sigma, \tau \eta^{-z} \rangle ,\]

and

\[G_{p_2} = \langle \tau, \eta \sigma^{-x} \rangle ,\]

in \(\text{Gal}(L/\mathbb{Q})\).

By a direct computation, we have,

\[G_p \cap G_{p_1} = \langle \sigma \tau^{-y} \eta^{xz} \rangle .\]

Hence,

\[G_p \cap G_{p_1} \cap G_{p_2} = \langle \sigma \tau^{-y} \eta^{xyz} \rangle \cap \langle \tau, \eta \sigma^{-x} \rangle \]

\[= \begin{cases} 
\{1\} & \text{if } xyz \neq -1, \\
\langle \sigma \tau^{-y} \eta^{xyz} \rangle & \text{if } xyz = -1.
\end{cases}\]

But, our assumption \(D_p D_{p_1} D_{p_2} = L\) implies \(G_p \cap G_{p_1} \cap G_{p_2} = \{1\}\). Hence \(xyz \neq -1\).
Conversely, we assume $k$ satisfies the conditions of Theorem 1 in case of $t = 2$. Since $k_1 = k_{1,G}$, it follows easily that $L = k(p_1)k(p_2)\mathbb{Q}_1$ is the maximal intermediate extension between $\mathbb{Q}$ and $k_n(n \geq 1)$ such that $\text{Gal}(L/\mathbb{Q})$ is an elementary abelian $p$-group. Without loss of generality, we may assume $(i, j) = (1, 2)$. Since $\text{Gal}(k(p_1)k(p_2)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^2$ and $p$ is unramified in $k(p_1)k(p_2)$, $p$ must decompose in $k(p_1)k(p_2)$. But the condition $(\frac{p_2}{p_1})_p \neq 1$ implies $p$ is inert in $k(p_1) \subset k(p_1)k(p_2)$, hence we obtain $[D_p : \mathbb{Q}] = p$. Similarly, $(\frac{p_1}{p_2})_p \neq 1$ and $p_2 \neq 1 \pmod{p^2}$ imply $[D_{p_1} : \mathbb{Q}] = [D_{p_2} : \mathbb{Q}] = p$. Therefore, as in the above computation of $G_p, G_{p_i}$, we have $D_pD_{p_1}D_{p_2} = L$, by $xyz \neq -1$. □

5. REMARKS

The condition of Theorem 1 in [12] means $xyz = 0$ which is a special case of $xyz \neq -1$. Hence, our Corollary 2 contains some known results and there exist infinitely many fields satisfying the conditions of Theorem 1 (cf. [12]).

If $K = k(p_1)k(p_2)$ satisfies the conditions of Theorem 1, then $\lambda_p(k) = \mu_p(k) = 0$ for any field $k \subseteq K$ with $[k : \mathbb{Q}] = p$. This is a result of Fukuda [4]. He has shown this result using a technic of capitulation of ideal class group. The case $xyz = -1$ is a difficult case. But we can get some results:

Proposition 8. Notations are as in section 3. Assume that $(\frac{p_1}{p_1})_p \neq 1, (\frac{p_1}{p_2})_p \neq 1$, and $p_2 \neq 1 \pmod{p^2}$. Then $\lambda_p(k) = \mu_p(k) = 0$ for the decomposition field $k$ of $p$ in $k(p_1)k(p_2)$.

Proof. We apply a result of [6]:

Lemma 9 ([6] Corollary 3.6). Let $k$ be a cyclic extension of $\mathbb{Q}$ of degree $p$. Then the following conditions are equivalent:

(a) $\lambda_p(k) = \mu_p(k) = 0$,

(b) For any prime ideal $w$ of $k_\infty$ which is prime to $p$ and ramified in $k_\infty/\mathbb{Q}_\infty$, the order of the ideal class of $w$ is prime to $p$.

If $xyz \neq -1$ then we have $\lambda_p(k) = \mu_p(k) = 0$ by Corollary 2. So we only consider the case $xyz = -1$. In this case we have $k \neq k(p_i)$ ($i = 1, 2$). It follows easily that $A(k)$, the $p$-part of the ideal class group of $k$, is cyclic of order $p$, and it is generated by products of primes of $k$ above $p$. On the other hand, for $i = 1, 2$, the prime $p_i$ of $k$ above $p_i$ generates $A(k)$, and is inert in $k_\infty/k$. Since the primes of $k$ above $p$ is principal for some $k_n$ by the natural mapping $A(k) \to A(k_n)$ (cf. [7]), $p_i$ is principal in $k_\infty$.

Since the primes ramified in $k_\infty/\mathbb{Q}_\infty$ are $p_1$ and $p_2$, which is principal in $k_\infty$, we can apply Lemma 9 and obtain $\lambda_p(k) = \mu_p(k) = 0$. □

Recently, Fukuda verified Greenberg conjecture for various cubic cyclic fields $k$ with $f_k = p_1p_2$ and $p = 3$. He gives an example, which is the case $p_1 = 7$ and $p_2 = 223$. Note that there exist two such fields, and these $p_1$ and $p_2$ do not satisfy condition (3) in Theorem 1. He verified $\lambda_3 = \mu_3 = 0$ for one of such fields by using his result concerning with the unit group of $k$ (cf. [5]).
When $t \geq 3$, i.e., at least 3 primes are ramified in $k/\mathbb{Q}$, there are a few results for Greenberg conjecture. In this case, the $p$-rank of $A(k)$ is greater than 2. Greenberg([7]) gave the following example, but the proof are omitted in his paper: $p = 3$ and $k$ is an cubic cyclic field with conductor $7 \cdot 13 \cdot 19$ and 3 is inert in $k/\mathbb{Q}$. He mentioned that by "delicate" arguments one can show $\lambda_{3}(k) = \mu_{3}(k) = 0$. The author had a chance to contact Prof. Greenberg, and asked him about this example. He kindly taught the author the "delicate" arguments, which is a system to examine relations of the ideal class group of intermediate fields of $k\mathbb{Q}_{1}$. Applying his idea, we can show the following result:

**Theorem 10** ([13]). Let $p$ be any odd prime. For any integer $0 \leq m \leq p-1$, there exist infinitely many cyclic extension fields $k$ of $\mathbb{Q}$ with $[k : \mathbb{Q}] = p$ such that $p$-rank$A(k) = m$ and $\lambda_{p}(k) = \mu_{p}(k) = 0$.

**REFERENCES**


**DEPARTMENT OF MATHEMATICAL SCIENCE, SCHOOL OF SCIENCE AND ENGINEERING, WASEDA UNIVERSITY, 3-4-1, OKUBO SHINJUKU-KU, TOKYO 169-8555, JAPAN  
E-mail address: 697m5068@mse.waseda.ac.jp**