Iwasawa invariants and linking numbers of primes

Yasushi Mizusawa and Gen Yamamoto

Dedicated to Professor Keiichi Komatsu

Abstract.

For an odd prime number $p$ and a number field $k$ which is an elementary abelian $p$-extension of the rationals, we prove the equivalence between the vanishing of all Iwasawa invariants of the cyclotomic $\mathbb{Z}_p$-extension of $k$ and an arithmetical condition described by the linking numbers of primes from a viewpoint of analogies between pro-$p$ Galois groups and link groups. A criterion of Greenberg’s conjecture for $k$ of degree $p$ is also described in terms of linking matrices.

§1. Introduction

Let $p$ be a fixed prime number. For a number field $k$, we denote by $k'^{\text{cyc}}$ the cyclotomic $\mathbb{Z}_p$-extension of $k$, where $\mathbb{Z}_p$ denotes (the additive group of) the ring of $p$-adic integers. Then $k'^{\text{cyc}}/k$ has a unique cyclic subextension $k_n/k$ of degree $p^n$ for each integer $n \geq 0$. Let $A(k_n)$ be the Sylow $p$-subgroup of the ideal class group of $k_n$, and let $e_n$ be the exponent of the order $|A(k_n)| = p^{e_n}$. The Iwasawa invariants $\lambda(k) \geq 0$, $\mu(k) \geq 0$, and $\nu(k)$ of $k'^{\text{cyc}}/k$ are defined as integers satisfying Iwasawa’s class number formula

$$e_n = \lambda(k)n + \mu(k)p^n + \nu(k)$$

for all sufficiently large $n$ (cf. e.g. [21]). In case of cyclotomic $\mathbb{Z}_p$-extensions, Iwasawa conjectured that $\mu(k) = 0$, and Ferrero and Washington [3] proved that $\mu(k) = 0$ if $k/\mathbb{Q}$ is an abelian extension. It was also conjectured by Greenberg [5] that $\lambda(k) = \mu(k) = 0$ if $k$ is a totally real number field. Greenberg’s conjecture has been studied in various situations, in particular when $k/\mathbb{Q}$ is an abelian extension. Criteria of
Greenberg’s conjecture for real abelian $p$-extensions $k/\mathbb{Q}$ are often described by $p$th power residue symbols of ramified prime numbers (e.g. [4, 22]).

In arithmetic topology (analogies between knot theory and number theory, cf. [16]), $p$th power residue symbols are often translated into analogues of mod $p$ linking numbers of knots. For a pair $(\ell, \ell')$ of distinct prime numbers, the (pro-$p$) linking number $\text{lk}(\ell, \ell')$ is defined as the discrete logarithm of $\ell$ modulo $\ell'$ if $\ell' \equiv 1 \pmod{p}$, and defined as the $p$-adic logarithm of $\ell$ to base $\alpha_p$ if $\ell \equiv 1 \pmod{p}$ and $\ell' = p$, where $\alpha_p$ is a generator of $1 + 2p\mathbb{Z}_p$. Based on analogies in linking numbers, Morishita [15] developed analogies between $p$-extensions of number fields and branched Galois coverings of 3-manifolds. In the origin of arithmetic topology, Mazur [12] pointed out an analogy between Alexander-Fox theory and Iwasawa theory. The Iwasawa invariants of links are also defined and studied, regarding a tower of cyclic $p$-coverings branched along a link as an analogue of a $\mathbb{Z}_p$-extension (cf. [6, 8, 9, 19, 20]).

The purpose of this paper is to study Iwasawa invariants for real abelian $p$-extensions $k/\mathbb{Q}$ from a viewpoint of arithmetic topology. The first result is the following theorem.

**Theorem 1.1.** Assume that $p$ is odd, and put $\ell_0 = p$. Let $S = \{\ell_1, \ldots, \ell_d\} \neq \emptyset$ be a finite set of $d$ prime numbers $\ell_i \equiv 1 \pmod{p}$, and let $k/\mathbb{Q}$ be the maximal elementary abelian $p$-extension unramified outside $S$. Then $\lambda(k) = \mu(k) = \nu(k) = 0$ if and only if $S$ satisfies one of the following two conditions on linking numbers of primes:

1. $d = 1$, and either $\text{lk}(\ell_0, \ell_1) \not\equiv 0 \pmod{p}$ or $\text{lk}(\ell_1, \ell_0) \not\equiv 0 \pmod{p}$.
2. $d = 2$, and $\text{lk}(\ell_0, \ell_1)\text{lk}(\ell_1, \ell_2)\text{lk}(\ell_2, \ell_0) \not\equiv \text{lk}(\ell_0, \ell_2)\text{lk}(\ell_2, \ell_1)\text{lk}(\ell_1, \ell_0) \pmod{p}$.

In particular, $d \leq 2$ if $\lambda(k) = \mu(k) = \nu(k) = 0$.

We prove Theorem 1.1 in §3 via the structure of a certain pro-$p$ Galois group $\tilde{G}_S(\mathbb{Q})$ analogous to a link group, which we recall in §2.

The condition (1) is similar to a condition of ‘circular set of primes’ (cf. e.g. [11]). There is also another generalization of (1) for larger $d$, which is described by linking matrices $C_k$ of cyclic extensions $k/\mathbb{Q}$ of degree $p$ (cf. Proposition 5.3). The matrix $C_k$ is a modification of the linking matrix $C' = (c'_{ij} \pmod{p})_{1 \leq i, j \leq d}$ of $S = \{\ell_1, \ldots, \ell_d\}$ with entries satisfying that $c'_{ij} = \text{lk}(\ell_i, \ell_j)$ if $i \neq j$, and that $\sum_{j=1}^d c'_{ij} \equiv 0 \pmod{p}$. The matrix $C'$ was defined in [16, Example 10.15] as an analogue of the linking matrix of a link. (See §4 for the definition of $C_k$.) Using also
an associated matrix $B_k$, we obtain the following sufficient condition of
Greenberg's conjecture as a partial generalization of Theorem 1.1. (See
§5 for the definition of $B_k$.)

**Theorem 1.2 (Theorem 5.1).** Suppose $\ell_0 = p \neq 2$. Let $k/\mathbb{Q}$ be a
cyclic extension of degree $p$ unramified at $p$, and let $S = \{\ell_1, \ldots, \ell_d\}$ be
the set of ramified primes in $k/\mathbb{Q}$. If $\text{rank} C_k = d - 1$ and $\text{rank} B_k = d$,
and if $p$ is inert in $k/\mathbb{Q}$, then $\lambda(k) = \mu(k) = 0$.

Theorem 1.2 is proved in §5 by extending an idea of Fukuda [4]
which is based on the capitulation of ideal classes in $k^{\text{cyc}}/k$. In §6, we
also give an infinite family of examples of Theorem 1.2 such that the
$p$-rank of $A(k)$ is $p - 1$.

§2. Linking numbers and pro-$p$ Galois groups

First we recall the definition of linking numbers of primes. Suppose
that $p \neq 2$. For each prime number $\ell' \equiv 1 \pmod{p}$, we fix an integer
$\alpha_{\ell'}$ such that $\alpha_{\ell'} \ell' \mathbb{Z}$ generates the cyclic group $(\mathbb{Z}/\ell'\mathbb{Z})^\times$. As in
[13], we also choose $\alpha_p = (1 + p)^{-1} \in \mathbb{Z}_p$ as a generator of the pro-cyclic
group $1 + p\mathbb{Z}_p = \alpha_p^{\mathbb{Z}_p}$. Let $\ell$ be a prime number. Put $\text{lk}(\ell, \ell') = 0$.
If $\ell \neq \ell' \equiv 1 \pmod{p}$, then $\text{lk}(\ell, \ell')$ is defined as an integer such that

$$\ell^{-1} \equiv \alpha_{\ell'}^{\text{lk}(\ell, \ell')} \pmod{\ell'}$$

and $0 \leq \text{lk}(\ell, \ell') < \ell' - 1$. If $\ell \equiv 1 \pmod{p}$, then $\text{lk}(\ell, p)$ is defined as a
$p$-adic integer satisfying

$$\ell^{-1} = \alpha_p^{\text{lk}(\ell, p)}.$$

**Remark 2.1.** While the definition of $\text{lk}(\ell, \ell')$ depends on the choice
of $\alpha_{\ell'}$, the divisibility by $p$ and the validity of (1) are independent of the
choices of $\alpha_{\ell'}$.

For a pro-$p$ group $G$ and the closed subgroup $H$, we denote by
$[H, G]$ (resp. $H^p$) the minimal closed subgroup containing $\{[h, g] = h^{-1} g h^{-1} g, h, g \in H\}$ (resp. $\{h^p | h \in H\}$), and put $G_2 = [G, G]$,
$G_3 = [G_2, G]$. Based on the theory of [10], the following theorem has
been obtained in [13] as a partial refinement of Salle's result [17] (cf. also
[2]).

**Theorem 2.2.** Assume that $p \neq 2$, and put $\ell_0 = p$. Let $S = \{\ell_1, \ldots, \ell_d\} \neq \emptyset$ be a finite set of $d$ prime numbers $\ell_i \equiv 1 \pmod{p}$. Let $(\mathbb{Q}^{\text{cyc}})_S$ be the maximal pro-$p$-extension of $\mathbb{Q}^{\text{cyc}}$ which is unramified
at every primes not lying over any $\ell_i \in S$. Then the Galois group $\tilde{G}_S(Q) = \text{Gal}(Q^{cyc}_S/Q)$ over $Q$ has a minimal presentation

$$1 \longrightarrow R \longrightarrow F \longrightarrow \tilde{G}_S(Q) \longrightarrow 1$$

where $F = \langle x_0, x_1, \cdots, x_d \rangle$ is a free pro-$p$ group with $d+1$ generators $x_i$ such that $\pi(x_i)$ generates the inertia group of a prime $\ell_i$ of $(Q^{cyc})_S$ lying over $\ell_i$, and $R = \langle r_0, r_1, \cdots, r_d \rangle_F$ is a normal subgroup of $F$ normally generated by $d+1$ relations $r_i$ of the form

$$r_i = \begin{cases} 
[x_0^{-1}, y_0^{-1}] & \text{if } i = 0, \\
[x_i^{-1}, y_i^{-1}] & \text{if } 1 \leq i \leq d
\end{cases}$$

with $y_i \in F$ such that $\pi(y_i)$ is a Frobenius automorphism of $\ell_i$ in $\tilde{G}_S(Q)$, and

$$y_i \equiv \prod_{j=0}^{d} x_j^{\text{lk}(\ell_i, \ell_j)} \mod [F,F].$$

Proof. We give a short proof for the convenience of the reader. For each $i$, we fix an embedding of the algebraic closure of $Q$ into that of the $\ell_i$-adic field $Q_{\ell_i}$, corresponding to a prime lying over $\ell_i$. Let $G_i \simeq \mathbb{Z}_p \rtimes \mathbb{Z}_p$ be the Galois group of the maximal pro-$p$-extension of $Q_{\ell_i}$ for $i \neq 0$, and put $G_0 = \text{Gal}(Q^{cyc}_{Q_{\ell_i}}/Q) \simeq \mathbb{Z}_p \times \mathbb{Z}_p$, where $Q^{cyc}_{Q_{\ell_i}}/Q$ is the unramified $\mathbb{Z}_p$-extension. Then the image of $G_i$ in $\tilde{G}_S(Q)$ is the decomposition group of $\ell_i$. By [17, §4] (or [2, Lemma 3.7]), the natural homomorphism

$$H^2(\tilde{G}_S(Q), \mathbb{Z}/p\mathbb{Z}) \hookrightarrow \bigoplus_{i=0}^{d} H^2(G_i, \mathbb{Z}/p\mathbb{Z}).$$

on the second cohomology groups is injective. By the same argument as in the proof of [10, Theorem 11.10 and Example 11.11], we obtain the presentation $\pi$ such that $\pi(x_i) \mod (\tilde{G}_S(Q))^2$ corresponds to the idèle class of $\alpha_{\ell_i}$. \qed

The Galois group $\tilde{G}_S(Q)$ is considered in [13] (including the case of $p = 2$) as an analogue of a link group, which is the fundamental group of the complement of a link in the 3-sphere. The ‘Koch type’ presentation of $\tilde{G}_S(Q)$ in Theorem 2.2 is an analogue of the Milnor presentation of a link group, where $\pi(x_i)$ (resp. $\pi(y_i)$) is analogous to the meridian (resp. longitude) of the tubular neighbourhood $V$ of a component of the link. In fact, $G_i \simeq \mathbb{Z}_p \rtimes \mathbb{Z}_p$ above is an analogue of the fundamental group $\pi_1(\partial V) \simeq \mathbb{Z} \times \mathbb{Z}$ of the boundary of $V$. Hence the linking numbers of primes are certainly analogous to the linking numbers of knots.
Remark 2.3. When \( d = 2 \), the condition (1) is satisfied if and only if the closed subgroup \( G_S(Q^{cyc}) = \text{Gal}((Q^{cyc})_S/Q^{cyc}) \) of \( \tilde{G}_S(Q) \simeq G_S(Q^{cyc}) \rtimes \mathbb{Z}_p \) is a pro-metacyclic pro-\( p \) group (cf. [7, 14]).

One can find infinitely many \( S = \{\ell_1, \ldots, \ell_d\} \) with prescribed mod \( p \) linking numbers as follows. In particular, there exist infinitely many sets \( S = \{\ell_1, \ell_2\} \) satisfying (1).

Proposition 2.4. Suppose \( \ell_0 = p \neq 2 \) and \( d \geq 1 \). For arbitrary integers \( a_{ij} \quad (0 \leq i, j \leq d, i \neq j) \), there exist infinitely many sets \( \{(\ell_i, \alpha_{ij}) \mid 1 \leq i \leq d\} \) of pairs \((\ell, \alpha)\) of prime numbers \( \ell \equiv 1 \pmod{p} \) and the primitive elements \( \alpha \in (\mathbb{Z}/\ell\mathbb{Z})^{\times} \) such that \( \text{lk}((\ell_i, \ell_j)) \equiv a_{ij} \pmod{p} \) for all \( 0 \leq i, j \leq d \) \((i \neq j)\).

Proof. Put \( \zeta_n = \exp \frac{2\pi \sqrt{-1}}{n} \) for each \( 1 \leq n \in \mathbb{Z} \). We choose \( \ell_i \) and \( \alpha_{\ell_i} \) \((1 \leq i \leq d)\) by the following recursive step: Put \( L_i = \mathbb{Q}(\zeta_p^p, \zeta_{\ell_i}, \sqrt[p]{\ell_j} \mid 0 \leq j \leq i - 1) \). Choose a prime \( \mathfrak{S}_i \) of \( \mathbb{Q}(\zeta_p) \) such that the Frobenius automorphism \( \sigma_i \in \text{Gal}(L_i/\mathbb{Q}(\zeta_p)) \) of \( \mathfrak{S}_i \) satisfies

\[
\begin{align*}
\sigma_i(\zeta_p^p) &= \zeta_p^{(1+p)^{\alpha_{\ell_i}}}, \\
\sigma_i(\zeta_{\ell_j}) &= \zeta_{\ell_j}^{a_{ij}} \quad (1 \leq j < i), \\
\sigma_i(\sqrt[p]{\ell_j}) &= \zeta_p^{-a_{ij}} \sqrt[p]{\ell_j} \quad (0 \leq j < i).
\end{align*}
\]

Take \( \ell_i \in \mathfrak{S}_i \), and choose \( \alpha_{\ell_i} \in \mathbb{Z} \) such that \( \zeta_{\ell_i - 1} \equiv \alpha_{\ell_i} \pmod{\mathfrak{S}_i} \), i.e.,

\( \zeta_p \equiv \alpha_{\ell_i}^{\frac{1}{p-1}} \pmod{\mathfrak{S}_i} \), where \( \tilde{\mathfrak{S}}_i \) is a prime of \( \mathbb{Q}(\zeta_{\ell_i - 1}) \) lying over \( \mathfrak{S}_i \).

Then we have \( \text{lk}(\ell_i, \ell_j) \equiv a_{ij} \pmod{p} \) for all \( 0 \leq i, j \leq d \) \((i \neq j)\). By the Chebotarev density theorem, there exist infinitely many such sets \( S = \{\ell_1, \ldots, \ell_d\} \). \( \square \)

§3. Proof of Theorem 1.1 via Theorem 2.2

Recall that \( \ell_0 = p \neq 2 \), \( S = \{\ell_1, \ldots, \ell_d\}, d \geq 1 \), \( \text{Gal}(k/Q) \simeq (\mathbb{Z}/p\mathbb{Z})^d \) and that \( k/Q \) is unramified outside \( S \). Let \( K/Q \) be a cyclic extension of degree \( p \) which is unramified outside \( S \) and ramified at any \( \ell_i \in S \). Then \( K \subset k \subset (Q^{cyc})_S \), and \( k/K \) is unramified. Let \( H = \text{Ker}(|_K \circ \pi) \) be the kernel of the surjective homomorphism

\[
F \to \tilde{G}_S(Q) \to \text{Gal}(K/Q) \simeq \mathbb{Z}/p\mathbb{Z},
\]

where \( \pi \) is the homomorphism obtained in Theorem 2.2. Recall that the inertia subgroup \( T_{\ell_i} \) of \( \tilde{G}_S(Q) \) for \( \ell_i \) is a procyclic pro-\( p \) group generated by \( \pi(x_i) \). Since \( K/Q \) is not unramified at \( \ell_i \in S \), \( T_{\ell_i} \not\subset \text{Gal}((Q^{cyc})_S/K) \), i.e., \( \pi(x_i)|_K \neq 1 \in \text{Gal}(K/Q) \) for \( i \neq 0 \). Hence the inertia subgroup
$T_i \cap \text{Ker}(|_{\ell_i})$ of $\text{Gal}(\mathbb{Q}^{\text{cyc}}_S/K)$ for $\ell_i$ is generated by $\pi(x_i^p)$ if $1 \leq i \leq d$. Then $\pi$ induces an exact sequence

$$1 \longrightarrow NR \longrightarrow H \longrightarrow \text{Gal}((K^{\text{cyc}})_0/K) \longrightarrow 1,$$

where $(K^{\text{cyc}})_0$ is the maximal unramified pro-$p$-extension of $K^{\text{cyc}}$, and $N = \langle x_1^p, \ldots, x_d^p \rangle_H$ is the closed normal subgroup of $H$ which is normally generated by $x_1^p, \ldots, x_d^p$. Since $(K^{\text{cyc}})_0/Q$ is a Galois extension, $NR$ is a normal subgroup of $F$. Actually, since $g^{-1}x_i^pg \in N$ for any $i \neq 0$ and any $g \in F = \bigcup_{j=0}^{p^d - 1} x_1^jH$, $N$ is also a normal subgroup of $F$, and normally generated by $x_1^p, \ldots, x_d^p$, i.e.,

$$N = \langle x_1^p, \ldots, x_d^p \rangle_F.$$

Since $k^{\text{cyc}}/K^{\text{cyc}}$ is unramified, $(K^{\text{cyc}})_0 = (k^{\text{cyc}})_0$ is also the maximal unramified pro-$p$-extension of $k^{\text{cyc}}$. Then $\pi$ also induces a presentation

$$1 \longrightarrow NR \longrightarrow F \overset{\varpi}{\longrightarrow} G \longrightarrow 1$$

of

$$G = \text{Gal}((K^{\text{cyc}})_0/Q) = \text{Gal}((k^{\text{cyc}})_0/Q),$$

where $\varpi = |(K^{\text{cyc}})_0 \circ \pi$. Let

$$R' = \langle \rho_0, \ldots, \rho_d \rangle_F$$

be the normal subgroup of $F$ normally generated by $d + 1$ elements

$$\rho_i = [x_i^{-1}, y_i^{-1}] \equiv \prod_{j=0}^d [x_i, x_j]^{\text{lk}(\ell_i, \ell_j)} \mod F_3.$$

Then $R' \subset F_2$, $NR = NR'$, and $G \cong F/NR'$.

The restriction mapping $G \overset{\text{lk}_{k^{\text{cyc}}}}{\longrightarrow} \text{Gal}(k^{\text{cyc}}/Q)$ induces a surjective homomorphism

$$\psi : G/G_2 \longrightarrow \text{Gal}(k^{\text{cyc}}/Q).$$

Since $NR \subset NF_2$, we have $G/G_2 \simeq F/NF_2 \simeq (\mathbb{Z}/p\mathbb{Z})^d \oplus \mathbb{Z}_p$. Since moreover $\text{Gal}(k^{\text{cyc}}/Q) \simeq (\mathbb{Z}/p\mathbb{Z})^d \oplus \mathbb{Z}_p$, $\psi$ must be an isomorphism. This implies that

$$G_2 = \text{Gal}((k^{\text{cyc}})_0/k^{\text{cyc}}).$$

Recall that

$$G_2/[G_2, G_2] \simeq \lim_{\leftarrow n} A(k_n),$$
where $\lim$ is the projective limit with respect to the norm mappings.
Then we obtain the following equivalences:

$$
\lambda(k) = \mu(k) = \nu(k) = 0 \iff G_2 \simeq 1 \\
\iff G_2 = (G_2)^pG_3 \\
(2) \iff F_2N/(F_2)^pF_3N = \mathcal{R}(F_2)^pF_3N/(F_2)^pF_3N.
$$

Put $\bar{g} = g(F_2)^pF_3N$ for $g \in F$.

**Lemma 3.1.** \{\{x_i, x_j\} | 0 \leq i < j \leq d\} forms a basis of the vector space $F_2N/(F_2)^pF_3N$ over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

**Proof.** Note that the map

$$
F/F_2 \times F/F_2 \to F_2/F_3 : (g_1F_2, g_2F_2) \mapsto [g_1, g_2]F_3
$$

is a surjective $\mathbb{Z}_p$-bilinear homomorphism. Since

$$(g_1^{-1}x_i^p, g_2^{-1}x_j^p) \equiv [x_i, x_j]^{\bar{p}} \equiv 1 \mod (F_2)^pF_3,$$

$$(F_2)^pF_3N/(F_2)^pF_3$$

is an abelian group. Suppose that $g \in (F_2)^pF_3N \cap F_2$. Then $g \in (F_2)^pF_3N$ is written in the form $g = g' \prod_{i=1}^d x_i^{z_i p}$ with some $g' \in (F_2)^pF_3$ and $z_i \in \mathbb{Z}_p$. Since $\prod_{i=1}^d x_i^{z_i p} \equiv 1 \mod (F_2)$ and $F/F_2$ is a free $\mathbb{Z}_p$-module generated by $\{x_iF_2 | 0 \leq j \leq d\}$, we have $z_i = 0$ for all $1 \leq i \leq d$, i.e., $g = g' \in (F_2)^pF_3$. Hence $(F_2)^pF_3N \cap F_2 = (F_2)^pF_3$, which induces an isomorphism

$$
F_2/(F_2)^pF_3 \simeq F_2N/(F_2)^pF_3N : g(F_2)^pF_3 \mapsto \bar{g}.
$$

For each pair $(i, j)$ such that $0 \leq i < j \leq d$, there is a surjective homomorphism $\varphi_{i,j} : F \to F' : x_i \mapsto a, x_j \mapsto b, x_l \mapsto 1 (l \notin \{i, j\})$, where $F'$ is the free pro-$p$ group with two generators $a, b$. If $g = \prod_{0 \leq i < j \leq d} [x_i, x_j]^{z_{i,j}} \equiv 1 \mod (F_2)^pF_3)$ with some $z_{i,j} \in \mathbb{Z}_p$, then $[a, b]^{z_{i,j}} = \varphi_{i,j}(g) \in (F_2)^pF_3^2$, and hence $z_{i,j} \equiv 0 \mod p$ for any $(i, j)$. Therefore $\{[x_i, x_j] | 0 \leq i < j \leq d\}$ is a basis of the $\mathbb{F}_p$-vector space $F_2/(F_2)^pF_3$. This yields the claim of Lemma 3.1. \qed

If $\lambda(k) = \mu(k) = \nu(k) = 0$, then

$$
\frac{d(d + 1)}{2} = \dim_{\mathbb{F}_p}(F_2N/(F_2)^pF_3N) = \dim_{\mathbb{F}_p}(\mathcal{R}(F_2)^pF_3N/(F_2)^pF_3N) \leq d + 1,
$$

i.e., $d \leq 2$, by Lemma 3.1 and (2).
If $d = 1$, $R'(F_2)^p F_3 N/(F_2)^p F_3 N = \langle \ell_0, \ell_1 \rangle_{\ell_0, \ell_1} \langle x_0, x_1 \rangle_{x_0, x_1}$ is a subspace of $F_2 N/(F_2)^p F_3 N = \langle x_0, x_1 \rangle \simeq \mathbb{F}_p$

(cf. Lemma 3.1). By (2), $\lambda(k) = \mu(k) = \nu(k) = 0$ if and only if $\text{lk}(\ell_0, \ell_1) \in \mathbb{Z}_p^\times$ or $\text{lk}(\ell_1, \ell_0) \in \mathbb{Z}_p^\times$.

If $d = 2$, $R'(F_2)^p F_3 N/(F_2)^p F_3 N = \langle \rho_0, \rho_1, \rho_2 \rangle$ is a subspace of $F_2 N/(F_2)^p F_3 N = \langle x_0, x_1, x_2, x_2, x_0 \rangle \simeq \mathbb{F}_p^3$

(cf. Lemma 3.1). Then $(\rho_0, \rho_1, \rho_2) = \langle x_0, x_1, x_2, x_2, x_0 \rangle A$ with a matrix

$$A = \begin{pmatrix}
\text{lk}(\ell_0, \ell_1) & -\text{lk}(\ell_1, \ell_0) & 0 \\
0 & \text{lk}(\ell_1, \ell_2) & -\text{lk}(\ell_2, \ell_1) \\
-\text{lk}(\ell_0, \ell_2) & 0 & \text{lk}(\ell_2, \ell_0)
\end{pmatrix}$$

having the determinant

$$\det A = \text{lk}(\ell_0, \ell_1)\text{lk}(\ell_1, \ell_2)\text{lk}(\ell_2, \ell_0) - \text{lk}(\ell_0, \ell_2)\text{lk}(\ell_2, \ell_1)\text{lk}(\ell_1, \ell_0).$$

By (2), $\lambda(k) = \mu(k) = \nu(k) = 0$ if and only if $\det A \in \mathbb{Z}_p^\times$.

Thus the proof of Theorem 1.1 is completed.

**Remark 3.2.** All real abelian $p$-extensions $k/Q$ such that $\lambda(k) = \mu(k) = \nu(k) = 0$ have been determined by some conditions on $p$th power residue symbols (cf. [18, 22, 23]). One can also obtain Theorem 1.1 by translating the condition of [22, Theorem 1] into the words of linking numbers (cf. [24, 25]). Moreover, there is an analogous condition of (1) in the function field analogue [1, Theorem] of [22, Theorem 1].

§4. **Linking matrices of number fields**

We define a linking matrix $C_K$ for a cyclic extension $K/Q$ of degree $p$. Suppose that $p \neq 2$. We use the same notation as in Theorem 2.2. Suppose that $K/Q$ is unramified outside $\{\ell_2, \cdots, \ell_d\}$ and ramified at $\ell_i$ for any $\delta \leq i \leq d$, where $\delta = \delta_K$ is either 0 or 1 according to whether $K/Q$ is ramified at $\ell_0 = p$ or not. Let $K^g$ be the genus class field of $K/Q$, i.e., $K^g$ is the maximal unramified abelian extension of $K$ which is abelian over $Q$. Then $K^g/Q$ coincides with the maximal elementary abelian $p$-extension of $Q$ unramified outside $\{\ell_2, \cdots, \ell_d\}$, and hence the homomorphism

$$F \rightarrow \tilde{G}_S(Q) \xrightarrow{|K^g|} \text{Gal}(K^g/Q) \simeq (\mathbb{Z}/p\mathbb{Z})^{d+1-\delta}$$
induces a homomorphism

$$F/K^p[F,F][x_0^\delta] \xrightarrow{\sim} \text{Gal}(K^\delta/Q) \xrightarrow{|K|} \text{Gal}(K/Q)$$

$$: \pi_i \mapsto \pi(x_i)|_{K^\delta} \mapsto \pi(x_d^m)|_K$$

with some integers $m_i = m_{K,i} \neq 0 \pmod{p}$ for $\delta \leq i \leq d$. Note that $m_d = 1$.

**Remark 4.1.** The presentation in Theorem 2.2 is constructed to satisfy $\pi(x_i)|_{K^\delta} = \tau_i|_{K^\delta}$ for $\tau_i \in \text{Gal}(Q(\zeta_{p^2\ell_i}, \ldots, \ell_d)/Q(\zeta_{p^2\ell_i}, \ldots, \ell_d))$ such that $\tau_0(\zeta_{p^2}) = \zeta_{p^2+p}$ and $\tau_0(\zeta_{p^2+\ell_i}) = \zeta_{\ell_i}$ if $j \neq 0$. Then $K$ is identified as the fixed field of $\langle \tau_0, \tau_d^i, \tau_d^j \mid \delta \leq i < d \rangle$ in $Q(\zeta_{p^2\ell_i}, \ldots, \ell_d)/Q$.

Let $I_{K,i}$ be the prime ideal of $K$ lying over $\ell_i$ for each $\delta \leq i \leq d$. The decomposition group

$$\text{Gal}(K^\delta/K) \cap \langle \pi(x_i)|_{K^\delta}, \pi(y_i)|_{K^\delta} \rangle = \langle \pi(y_i x_i^{c_i})|_{K^\delta} \rangle$$

of $I_{K,i}$ in $\text{Gal}(K^\delta/K)$ is generated by the Frobenius automorphism $(K^\delta/K)_{I_{K,i}} = \langle \pi(y_i x_i^{c_i})|_{K^\delta} \rangle$ with some integer $c_i$. Since

$$1 = \pi(y_i x_i^{c_i})|_K = \pi(x_i^{c_i} \prod_{j=\delta}^d x_j^{\text{lk}(\ell_i, \ell_j)})|_K = \pi(x_d)^{m_i c_i + \sum_{j=\delta}^d m_{j \text{lk}(\ell_i, \ell_j)}} I_{K,i},$$

we have $c_{i i} \equiv -m_{i}^{-1} \sum_{j=\delta}^d m_{j \text{lk}(\ell_i, \ell_j)} \pmod{p}$. Put $c_{i j} = \text{lk}(\ell_i, \ell_j)$ if $i \neq j$. Then the linking matrix of $K$ is defined as a $(d + 1 - \delta) \times (d + 1 - \delta)$ matrix

$$C_K = (c_{i j} \pmod{p})_{\delta \leq i, j \leq d}$$

with entries in $F_p$, which satisfies

$$\left( \begin{array}{c} (K^\delta/K)_{I_{K,i}} \\ \vdots \\ (K^\delta/K)_{I_{K,i}} \end{array} \right) = C_K \left( \begin{array}{c} \pi(x_d)|_{K^\delta} \\ \vdots \\ \pi(x_d)|_{K^\delta} \end{array} \right),$$

i.e., $(K^\delta/K)_{I_{K,i}} = \prod_{j=\delta}^d \pi(x_j)^{c_{i j}}$ for $\delta \leq i \leq d$. Note that $\{\pi(x_j)|_{K^\delta}\}_{\delta \leq j \leq d}$ forms a basis of the $F_p$-vector space $\text{Gal}(K^\delta/Q) \simeq F_p^{d+1-\delta}$. Since $\text{Gal}(K^\delta/K) \simeq F_p^{d+1-\delta}$, we have rank $C_K \leq d - \delta$. The following lemma is a translation of [4, Lemma 1.1] into the words of a linking matrix. We denote by $[\alpha]$ the ideal class of an ideal $\alpha$.

**Lemma 4.2.** Under the settings above, the following two conditions are equivalent, where $$(0, \ldots, 0) \neq (b_8, \ldots, b_d) \in \mathbb{F}_p^{d+1-\delta}:$$. 
1. \( A(K) = ([K_d], \ldots, [K_d]) \simeq (\mathbb{Z}/p\mathbb{Z})^{d-\delta} \text{ and } \prod_{i=0}^{d} [l_i, k]^h_i = 1 \).

2. \( \text{rank } C_K = d - \delta \text{ and } (b_d, \ldots, b_d) C_K = (0, \ldots, 0). \)

**Proof.** The equation (3) implies that \( \text{Gal}(K^\delta/K) = \langle (K^\delta/K, \ldots, (K^\delta/K) \rangle \text{ if and only if } \text{rank } C_K = d - \delta \text{. By [4, Lemma 1.1], } A(K) = \langle [K_d], \ldots, [K_d] \rangle \simeq \mathbb{F}_p^{d-\delta} \text{ if and only if } \text{rank } C_K = d - \delta \text{. Then, since } A(K) \rightarrow \text{Gal}(K^\delta/K) : [K_d] \mapsto \langle (K^\delta/K) \rangle \text{ becomes a } \mathbb{F}_p\text{-linear isomorphism, we obtain the equivalence.} \)

If \( \delta = 1 \) and \( \mu_i = 1 \) for all \( 1 \leq i \leq d \), the \( d \times d \) matrix \( C_K \) coincides with the linking matrix \( C' \) of \( S \) (cf. [16, Example 10.15]).

§5. A criterion of Greenberg's conjecture via capitulation

Using the linking matrices \( C_K \), we obtain a criterion of Greenberg's conjecture as follows. Recall that \( \ell_0 = p \neq 2 \) and \( \ell_i \equiv 1 \pmod{p} \) for \( 1 \leq i \leq d \). Let \( k/\mathbb{Q} \) be a cyclic extension of degree \( p \) which is unramified outside the set \( S = \{ \ell_1, \ldots, \ell_d \} \) and ramified at any \( \ell_i \in S \). Then the \( (\mathbb{Z}/p\mathbb{Z})^{2} \)-extension \( k_1/\mathbb{Q} \) contains \( p - 1 \) cyclic subextensions \( k^{(1)}, \ldots, k^{(p-1)} \) of degree \( p \) except for \( k \) and \( \mathbb{Q}_p \). Put \( k^{(0)} = k \), and put

\[
J = \{ j \mid \text{rank } C_K = d - \delta \text{ for } K = k^{(j)} \} \subset \{0, 1, \ldots, p - 1\}
\]

with the cardinality \( |J| \). For each \( j \in J \), let \( (b_{d,j}, \ldots, b_{d,j}) \in \mathbb{F}_p^{d+1-\delta} \) be a nonzero vector satisfying \( (b_{d,j}, \ldots, b_{d,j}) C_{k^{(j)}} = (0, \ldots, 0) \), where \( \delta = 1 \) if \( j = 0 \), and \( \delta = 0 \) otherwise. Omitting \( b_{d,j} \), we define a \( d \times |J| \) matrix

\[
B_k = (b_{i,j})_{1 \leq i \leq d, j \in J}.
\]

Now we shall recall and prove Theorem 1.2.

**Theorem 5.1** (Theorem 1.2). Under the settings above, if \( \text{rank } C_k = d - 1 \) and \( \text{rank } B_k = d \), then \( A(k) \) capitulates in \( k_1 \). If moreover \( p \) is \( \text{inert } in k/\mathbb{Q}, \) we have \( \lambda(k) = \mu(k) = 0 \).

**Proof.** Suppose that \( \text{rank } C_k = d - 1 \) and \( \text{rank } B_k = d \). Then \( \text{A}(k) = ([k_1], \ldots, [k_1]) \) by Lemma 4.2, and there is \( J' \subset J \) such that \( B_k' = (b_{i,j})_{1 \leq i \leq d, j \in J'} \) is a regular \( d \times d \) matrix. Let \( O_{k_1} \) denote the ring of algebraic integers in \( k_1 \), and let \( p \) be the prime ideal of \( \mathbb{Q}_1 \) lying over \( p \). For any \( 1 \leq j \leq p - 1 \), since \( [p] \in A(k_1) \simeq 1 \) and \( pO_{k_1} = [k_1]_O O_{k_1} \), we have \([k_1, O_{k_1}] = [pO_{k_1}] = 1 \in A(k_1) \). Moreover, \( I_{p, j} O_{k_1} = [k_1, O_{k_1}] \) for any \( 1 \leq j \leq p - 1 \) and \( 1 \leq i \leq d \). Hence

\[
\prod_{i=1}^{d} [k_i, O_{k_1}]^{b_{i,j}} = 1 \text{ for any } j \in J' \text{ by Lemma 4.2.}
\]
Iwasawa invariants and linking numbers

If we write additively as \( \sum_{i=1}^{d} b_{ij}[l_{k,i}O_{k_1}] = 0 \), then

\[
([l_{k,1}O_{k_1}], \ldots, [l_{k,d}O_{k_1}]) = (0, \ldots, 0)B_k^{-1} = (0, \ldots, 0).
\]

This implies that the lift mapping \( A(k) \rightarrow A(k_1) : [a] \mapsto [aO_{k_1}] \) is a zero mapping, i.e., \( A(k) \) capitulates in \( k_1 \). Then, moreover if \( p \) is inert in \( k/Q \), we have \( \lambda(k) = \mu(k) = 0 \) by [5, Theorem 1].

**Remark 5.2.** Note that the extensions \( k^{(1)}, \ldots, k^{(p-1)} \) have the common genus class field which contains \( k_1 \). For \( 1 \leq i \leq d \), since \( \pi_1(x_i)|_k = \pi_1(x_i|m_{k,i})|_k \) and \( \pi_1(x_i) = \text{Gal}(k_1/Q_1) = \langle \pi_1(x_d)|_{k_1} \rangle \), we have \( \pi_1(x_i)|_{k_1} = \pi_1(x_d|m_{k,i})|_{k_1} \), and hence \( m_{k,(i)} \equiv m_{k,i} \pmod{p} \) for any \( 0 \leq j \leq p-1 \), i.e., \( m_{i} (1 \leq i \leq d) \) is common for all \( K = k^{(j)} \). On the other hand, we may assume that \( \text{Gal}(k_1/k^{(j)}) = \langle \pi(x_0^{(j)}x_d)|_{k_1} \rangle \), i.e.,

\[
m_0 = m_{k,(i)} \equiv j^{-1} \pmod{p}
\]

for each \( K = k^{(j)} \) \((1 \leq j \leq p-1)\).

Theorem 1.2 is a partial generalization of Theorem 1.1 in the following sense.

**Proposition 5.3.** If \( d = 2 \) under the settings above, \( \text{rank} B_k = 2 \) (and rank \( C_k = 1 \)) if and only if (1) is satisfied.

**Proof.** Put \( l_{K,ij} = m_{K,j}l_k(\ell_i, \ell_j) (\delta_K \leq j \leq 2) \) for \( \mathbb{Q}_1 \neq K \subset k_1 \), and put \( b_{ij} = l_{K,ij} \) if \( j \neq 0 \) (cf. Remark 5.2). Since

\[
C_k \in \begin{pmatrix} l_{12} & 0 \\ -l_{21} & 0 \end{pmatrix} \text{GL}_2(\mathbb{F}_p)
\]

and

\[
C_K \in \begin{pmatrix} 0 & -l_{01} & -l_{02} \\ 0 & l_{K,10} + l_{12} & -l_{12} \\ -l_{21} & l_{K,20} + l_{21} \end{pmatrix} \text{GL}_3(\mathbb{F}_p)
\]

for \( K \neq k \), we have \( (l_{12}, l_{12})C_k = (0,0) \) and \( (b_{0,K}, b_{1,K}, b_{2,K})C_K = (0,0,0) \) with

\[
\begin{pmatrix} b_{0,K} \\ b_{1,K} \\ b_{2,K} \end{pmatrix} = \begin{pmatrix} l_{12}l_{K,20} + l_{K,20}l_{K,10} + l_{K,10}l_{21} \\ l_{K,20}l_{01} + l_{01}l_{21} + l_{21}l_{02} \\ l_{K,10}l_{02} + l_{02}l_{12} + l_{12}l_{01} \end{pmatrix} \times \begin{pmatrix} -l_{01} \\ -l_{12} \\ -l_{21} \end{pmatrix} = \begin{pmatrix} l_{K,10} + l_{12} \\ l_{K,20} + l_{21} \end{pmatrix},
\]

where \( \times \) denotes the cross product of vectors. For each \( K = k^{(j)} \) with \( 1 \leq j \leq p-1 \), rank \( C_K \leq 1 \) (i.e., \( j \notin J \)) if and only if \( b_{0,K} = b_{1,K} = \)
$b_{2,K} = 0$. Note that $l_{21} = l_{12} = 0$ if and only if rank $C_k = 0$ (i.e., $0 \not\in J$). Since
\begin{equation}
\begin{vmatrix}
  l_{21} & b_{1,K} \\
  l_{12} & b_{2,K}
\end{vmatrix} = -l_{01}l_{12}l_{K,20} + l_{02}l_{21}l_{K,10},
\end{equation}
we have $J = \{0, 1, \ldots , p-1\}$ (in particular rank $C_k = 1$) if (1) is satisfied. If $0 \in J$, then $(b_{10}, b_{20}) = (l_{21}, l_{12})$. If $0 \not\in j \in J$, then $(b_{1j}, b_{2j}, b_{2j}) = (b_{0,K}, b_{1,K}, b_{2,K})$. Since the $2 \times 2$ minors of $B_k$ are either (4) or
\begin{equation*}
\begin{vmatrix}
  b_{1K} & b_{1,K'} \\
  b_{2K} & b_{2,K'}
\end{vmatrix} = (-l_{01}l_{12}l_{K,20} + l_{02}l_{21}l_{K,10})(l_{01} + l_{02})(m_{K',0}m_{K,0}^{-1} - 1)
\end{equation*}
with some $K$ and $K'$, we have (1) if and only if rank $B_k = 2$. □

§6. Examples

Using Theorem 1.2, one can see the detail of an example by Greenberg [5] as follows.

Example 6.1 ([5, p.283]). If $\ell_0 = p = 3$, $d = 3$, $(\ell_1, \ell_2, \ell_3) = (7, 13, 19)$, $\alpha_{\ell_1} = 3$, $\alpha_{\ell_2} = \alpha_{\ell_3} = 2$, we have
\[
(lk(\ell_i, \ell_j))_{0 \leq i, j \leq 3} = \begin{pmatrix}
0 & 5 & 8 & 5 \\
2 + z_1 & 0 & 1 & 12 \\
1 + z_2 & 3 & 0 & 13 \\
0 + z_3 & 1 & 7 & 0
\end{pmatrix} \equiv \begin{pmatrix}
0 & 2 & 2 & 2 \\
2 & 0 & 1 & 0 \\
1 & 0 & 0 & 1 \\
0 & 1 & 1 & 0
\end{pmatrix} \mod 3,
\]
with some $z_i \in 3\mathbb{Z}_3$, where we note that $(1+p)^p \equiv 1 \pmod{p^2}$. Let $k/\mathbb{Q}$ be the cyclic cubic extension ramified only at $S = \{7, 13, 19\}$ such that $m_{k,1} = m_1 = 1$, $m_{k,2} = m_2 = 2$ (and $m_{k,3} = m_3 = 1$). Then
\[
C_k = \begin{pmatrix}
1 & 1 & 0 \\
0 & 1 & 1 \\
1 & 1 & 0
\end{pmatrix}, \quad \text{rank } C_k = 2, \quad (1, 0, 2)C_k = (0, 0, 0),
\]
and $A(k) \simeq (\mathbb{Z}/3\mathbb{Z})^2$ by Lemma 4.2. For $j \in \{1, 2\}$, assuming $m_{k(\cdot),0} = j \equiv j^{-1} \pmod{3}$, we have
\[
C_{k(j)} = \begin{pmatrix}
j & 2 & 2 & 2 \\
2 & j + 1 & 1 & 0 \\
1 & 0 & j + 1 & 1 \\
0 & 1 & 1 & 0
\end{pmatrix}, \quad \text{rank } C_{k(j)} = 3,
and $(1, 2, 1, 0)C_{k(1)} = (0, 0, 0, 0) = (1, 0, 1, 1)C_{k(2)}$. Then $J = \{0, 1, 2\}$, and
\[
B_k = \begin{pmatrix}
1 & 2 & 0 \\
0 & 1 & 1 \\
2 & 0 & 1
\end{pmatrix}, \quad \text{rank } B_k = 3.
\]
Hence $A(k)$ capitulates in $k_1$ by Theorem 1.2. Since
\[
\pi(y_0)|_k = \prod_{j=1}^{3} \pi(x_j)|^{\text{lk}(\ell_0, \ell_j)}_k = \pi(x_3)|_{k}^{\sum_{j=1}^{3} m_j \text{lk}(\ell_0, \ell_j)} = \pi(x_3)|_{k}^{2} \neq 1
\]
by Theorem 2.2, $p$ is inert in $k/Q$. Therefore $\lambda(k) = \mu(k) = 0$ by [5, Theorem 1].

Moreover, we obtain infinitely many examples of Theorem 1.2 as follows.

**Corollary 6.2.** If $2 \leq d \leq p$, there exist infinitely many cyclic extensions $k/Q$ of degree $p$ such that: $p$ is inert in $k/Q$, $A(k) \simeq (\mathbb{Z}/p\mathbb{Z})^{d-1}$, and $\lambda(k) = \mu(k) = 0$ (and $\nu(k) = 1$ if $d = 2$).

**Proof.** Put $\ell_0 = p$. By Proposition 2.4, there exist infinitely many $S = \{\ell_1, \cdots, \ell_d\}$ such that
\[
(\text{lk}(\ell_i, \ell_j))_{0 \leq i, j \leq d} \equiv \begin{pmatrix}
0 & 0 & 1 & \cdots & 1 \\
1 & 0 & 0 & \cdots & 0 \\
2 & -1 & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
2 \cdots 1 & 0 & \cdots & 0
\end{pmatrix} \mod p.
\]
Let $k/Q$ be the $\mathbb{Z}/p\mathbb{Z}$-extension ramified only at $S$ such that $m_{k,i} = m_i = 1$ for all $1 \leq i \leq d$. Since
\[
\pi(y_0)|_k = \prod_{j=1}^{d} \pi(x_j)|^{\text{lk}(\ell_0, \ell_j)}_k = \prod_{j=2}^{d} \pi(x_j)|_k = \pi(x_3)|_{k}^{d-1} \neq 1
\]
by Theorem 2.2, $p$ is inert in $k/Q$. (If $d = 2$, then (1) is satisfied, and hence Theorem 1.1 yields that $\lambda(k^g) = \mu(k^g) = \nu(k^g) = 0$, which implies $\lambda(k) = \mu(k) = 0$, $\nu(k) = 1$ and $A(k) \simeq \mathbb{Z}/p\mathbb{Z}$.) Since
\[
C_k = \begin{pmatrix}
0 & 0 & \cdots & 0 \\
-1 & 1 & & \\
\vdots & \ddots & \ddots & \\
-1 & & \cdots & 1
\end{pmatrix}
\]
has rank $d - 1$, we have $A(k) \simeq (\mathbb{Z}/p\mathbb{Z})^{d-1}$ by Lemma 4.2. Moreover $0 \in J$ and $(b_{10}, \cdots, b_{d0}) = (1, 0, \cdots, 0) \in \mathbb{F}_p^d$. Suppose that $m_{k(1),0}$
\[ j^{-1} \pmod{p} \] as in Remark 5.2. Then
\[
C_{k(i)} = \begin{pmatrix}
-(d-1)j & 0 & 1 & \cdots & 1 \\
1 & -j^{-1} & 0 & \cdots & 0 \\
2 & -1 & 1 - 2j^{-1} & & \\
\vdots & \vdots & & \ddots & \\
d & -1 & & & 1 - dj^{-1}
\end{pmatrix}
\]
for \( 1 \leq j \leq p-1 \). Put \( J' = \{0, 2, \ldots, d\} \) if \( d < p \), and \( J' = \{0, 1, 2, \ldots, p-1\} \) if \( d = p \). One can easily see that \( J' \subset J \), i.e., rank \( C_{k(i)}(j) = d \) if \( 0 \neq j \in J' \).

If \( d < p \),
\[
B'_k = (b_{ij})_{1 \leq i,j \leq d \in J'} = \begin{pmatrix}
1 & -1 & \cdots & -1 \\
0 & 2^{-1} & & \\
\vdots & \vdots & \ddots & \\
0 & & & d^{-1}
\end{pmatrix}
\]
and \( b_{0j} = 0 \) for any \( 2 \leq j \leq d \). If \( d = p \),
\[
B'_k = (b_{ij})_{1 \leq i,j \leq d \in J'} = \begin{pmatrix}
1 & 0 & -1 & \cdots & -1 \\
0 & 1^{-1} & 2^{-1} & & \\
\vdots & \vdots & \ddots & \ddots & \\
0 & (p-1)^{-1} & 0 & \cdots & 0
\end{pmatrix}
\]
b_{01} = 1, and \( b_{0j} = 0 \) for all \( 2 \leq j \leq p-1 \). Since \( \det B'_k \neq 0 \), we have rank \( B_k = d \) and hence \( \lambda(k) = \mu(k) = 0 \) by Theorem 1.2.

**Example 6.3.** If \( \ell_0 = p = 3 \), \( d = 2 \), \( (\ell_1, \ell_2) = (67, 79) \), \( \alpha_{\ell_1} = 12 \), \( \alpha_{\ell_2} = 53 \), we have
\[
(lk(\ell_i, \ell_j))_{0 \leq i,j \leq 2} = \begin{pmatrix}
0 & 57 & 1 \\
1 + z_1 & 0 & 48 \\
2 + z_2 & 65 & 0
\end{pmatrix} \equiv \begin{pmatrix}
0 & 0 & 1 \\
1 & 0 & 0 \\
2 & -1 & 0
\end{pmatrix} \pmod{3}
\]
with some \( z_i \in 3\mathbb{Z}_3 \). Then \( \lambda(k) = \mu(k) = 0 \) (and \( \nu(k) = 1 \)) for \( k \) with \( m_{k,1} = 1 \) as in the proof of Corollary 6.2. Since \( \lambda(k^3) = \mu(k^3) = \nu(k^3) = 0 \) by Theorem 1.1, we have \( \lambda(k) = \mu(k) = 0 \) (and \( \nu(k) = 1 \)) also for \( k \) with \( m_{k,1} = 2 \).

**Acknowledgements.** The authors thank the referee and Professor Masato Kurihara for helpful comments for the improvement of this paper. A part of this work was supported by JSPS KAKENHI Grant Numbers JP26800010, JP17K05167.
References

[18] H. Taya and G. Yamamoto, Notes on certain real abelian 2-extension fields with $\lambda_2 = \mu_2 = \nu_2 = 0$, Trends in Mathematics, Information Center for Mathematical Sciences 9 (2006), no. 1, 81–89.


Y. Mizusawa
Department of Mathematics, Nagoya Institute of Technology, Gokiso, Showa-ku, Nagoya 466-8555, Japan.
E-mail address: mizusawa.yasushi@nitech.ac.jp

G. Yamamoto
School of Engineering, Tokyo Denki University, 5 Senju-asahi-cho, Adachi-ku, Tokyo 120-8551, Japan.