# 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 $k^{\mathrm{cyc}}$ the cyclotomic $\mathbb{Z}_p$-extension of $k$, where $\mathbb{Z}_p$ denotes (the additive group of) the ring of $p$-adic integers. Then $k^{\mathrm{cyc}}/k$ 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 $\lambda(k) \geq 0$, $\mu(k) \geq 0$, $\nu(k)$ of $k^{\mathrm{cyc}}/k$ 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

Received December 24, 2017.

Revised August 16, 2018.

2010 *Mathematics Subject Classification.* 11R23 (11R18).

*Key words and phrases.* Iwasawa invariants, arithmetic topology, linking numbers.

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 $\mathrm{lk}(\ell, \ell')$ 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 $S = \{\ell_1, \dots, \ell_d\} \neq \emptyset$ 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 $\mathrm{lk}(\ell_0, \ell_1) \not\equiv 0 \pmod{p}$ or $\mathrm{lk}(\ell_1, \ell_0) \not\equiv 0 \pmod{p}$.*
2. *$d = 2$, and*

$$\mathrm{lk}(\ell_0,\ell_1)\mathrm{lk}(\ell_1,\ell_2)\mathrm{lk}(\ell_2,\ell_0) \not\equiv \mathrm{lk}(\ell_0,\ell_2)\mathrm{lk}(\ell_2,\ell_1)\mathrm{lk}(\ell_1,\ell_0) \pmod{p}. \tag{1}$$

*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 $\widetilde{G}_S(\mathbb{Q})$ 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 $C' = (c'_{ij} \bmod p)_{1 \leq i,j \leq d}$ of $S = \{\ell_1, \dots, \ell_d\}$ with entries satisfying that $c'_{ij} = \mathrm{lk}(\ell_i, \ell_j)$ 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 $S = \{\ell_1, \dots, \ell_d\}$ be the set of ramified primes in $k/\mathbb{Q}$. If $\operatorname{rank} C_k = d-1$ and $\operatorname{rank} B_k = d$, 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 $k^{\mathrm{cyc}}/k$. 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 $\overline{\alpha_{\ell'}} = \alpha_{\ell'} + \ell'\mathbb{Z}$ 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 procyclic group $1 + p\mathbb{Z}_p = \alpha_p^{\mathbb{Z}_p}$. Let $\ell$ be a prime number. Put $\operatorname{lk}(\ell, \ell) = 0$. If $\ell \neq \ell' \equiv 1 \pmod{p}$, then $\operatorname{lk}(\ell, \ell')$ is defined as an integer such that

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

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

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

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

For a pro-$p$ group $G$ and the closed subgroup $H$, we denote by $[H, G]$ (resp. $H^p$) the minimal closed subgroup containing $\{[h, g] = h^{-1}g^{-1}hg \mid g \in G, h \in H\}$ (resp. $\{h^p \mid h \in H\}$), 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 $S = \{\ell_1, \dots, \ell_d\} \neq \emptyset$ be a finite set of $d$ prime numbers $\ell_i \equiv 1 \pmod{p}$. Let $(\mathbb{Q}^{\mathrm{cyc}})_S$ be the maximal pro-$p$-extension of $\mathbb{Q}^{\mathrm{cyc}}$ which is unramified* *at every primes not lying over any $\ell_i \in S$. Then the Galois group $\widetilde{G}_S(\mathbb{Q}) = \mathrm{Gal}((\mathbb{Q}^{\mathrm{cyc}})_S/\mathbb{Q})$ over $\mathbb{Q}$ has a minimal presentation*

$$1 \longrightarrow R \longrightarrow F \xrightarrow{\pi} \widetilde{G}_S(\mathbb{Q}) \longrightarrow 1$$

*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 $\widetilde{\ell}_i$ of $(\mathbb{Q}^{\mathrm{cyc}})_S$ 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*

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

*with $y_i \in F$ such that $\pi(y_i)$ is a Frobenius automorphism of $\widetilde{\ell}_i$ in $\widetilde{G}_S(\mathbb{Q})$, and*

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

*Proof.* We give a short proof for the convenience of the reader. For each $i$, we fix an embedding of the algebraic closure of $\mathbb{Q}$ into that of the $\ell_i$-adic field $\mathbb{Q}_{\ell_i}$, corresponding to a prime lying over $\widetilde{\ell}_i$. Let $\mathcal{G}_i \simeq \mathbb{Z}_p \rtimes \mathbb{Z}_p$ be the Galois group of the maximal pro-$p$-extension of $\mathbb{Q}_{\ell_i}$ for $i \neq 0$, and put $\mathcal{G}_0 = \mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc}}\mathbb{Q}_p^{\mathrm{ur},p}/\mathbb{Q}_p) \simeq \mathbb{Z}_p \times \mathbb{Z}_p$, where $\mathbb{Q}_p^{\mathrm{ur},p}/\mathbb{Q}_p$ is the unramified $\mathbb{Z}_p$-extension. Then the image of $\mathcal{G}_i$ in $\widetilde{G}_S(\mathbb{Q})$ is the decomposition group of $\widetilde{\ell}_i$. By [17, §4] (or [2, Lemma 3.7]), the natural homomorphism

$$H^2(\widetilde{G}_S(\mathbb{Q}), \mathbb{Z}/p\mathbb{Z}) \hookrightarrow \bigoplus_{i=0}^{d} H^2(\mathcal{G}_i, \mathbb{Z}/p\mathbb{Z})$$

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 $\pi(x_i) \bmod (\widetilde{G}_S(\mathbb{Q}))_2$ corresponds to the idèle class of $\alpha_{\ell_i}$. □

The Galois group $\widetilde{G}_S(\mathbb{Q})$ 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 $\widetilde{G}_S(\mathbb{Q})$ 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, $\mathcal{G}_i \simeq \mathbb{Z}_p \rtimes \mathbb{Z}_p$ 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 $G_S(\mathbb{Q}^{\mathrm{cyc}}) = \mathrm{Gal}((\mathbb{Q}^{\mathrm{cyc}})_S/\mathbb{Q}^{\mathrm{cyc}})$ of $\widetilde{G}_S(\mathbb{Q}) \simeq G_S(\mathbb{Q}^{\mathrm{cyc}}) \rtimes \mathbb{Z}_p$ is a prometacyclic pro-$p$ group (cf. [7, 14]).

One can find infinitely many $S = \{\ell_1, \dots, \ell_d\}$ 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 $a_{ij}$ $(0 \leq i, j \leq d,\ i \neq j)$, there exist infinitely many sets $\{(\ell_i, \overline{\alpha_{\ell_i}}) \,|\, 1 \leq i \leq d\}$ of pairs $(\ell, \overline{\alpha_\ell})$ of prime numbers $\ell \equiv 1 \pmod p$ and the primitive elements $\overline{\alpha_\ell} \in (\mathbb{Z}/\ell\mathbb{Z})^\times$ such that $\mathrm{lk}(\ell_i, \ell_j) \equiv a_{ij} \pmod p$ 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 $L_i = \mathbb{Q}(\zeta_{p^2}, \zeta_{\ell_j}, \sqrt[p]{\ell_j} \,|\, 0 \leq j \leq i-1)$. Choose a prime $\mathfrak{L}_i$ of $\mathbb{Q}(\zeta_p)$ such that the Frobenius automorphism $\sigma_i \in \mathrm{Gal}(L_i/\mathbb{Q}(\zeta_p))$ of $\mathfrak{L}_i$ satisfies

$$\begin{aligned} &\sigma_i(\zeta_{p^2}) = \zeta_{p^2}^{(1+p)^{a_{i0}}},\ \sigma_i(\zeta_{\ell_j}) = \zeta_{\ell_j}^{\alpha_{\ell_j}^{-a_{ij}}} \quad (1 \leq j < i), \\ &\sigma_i(\sqrt[p]{\ell_j}) = \zeta_p^{-a_{ji}} \sqrt[p]{\ell_j} \quad (0 \leq j < i). \end{aligned}$$

Take $\ell_i \in \mathfrak{L}_i$, and choose $\alpha_{\ell_i} \in \mathbb{Z}$ such that $\zeta_{\ell_i - 1} \equiv \alpha_{\ell_i} \pmod{\widetilde{\mathfrak{L}}_i}$, i.e., $\zeta_p \equiv \alpha_{\ell_i}^{\frac{\ell_i - 1}{p}} \pmod{\mathfrak{L}_i}$, where $\widetilde{\mathfrak{L}}_i$ is a prime of $\mathbb{Q}(\zeta_{\ell_i - 1})$ lying over $\mathfrak{L}_i$.

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

## §3. Proof of Theorem 1.1 via Theorem 2.2

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

$$F \xrightarrow{\pi} \widetilde{G}_S(\mathbb{Q}) \xrightarrow{|_K} \mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/p\mathbb{Z},$$

where $\pi$ is the homomorphism obtained in Theorem 2.2. Recall that the inertia subgroup $T_i$ of $\widetilde{G}_S(\mathbb{Q})$ for $\widetilde{\ell}_i$ is a procyclic pro-$p$ group generated by $\pi(x_i)$. Since $K/\mathbb{Q}$ is not unramified at $\ell_i \in S$, $T_i \not\subset \mathrm{Gal}((\mathbb{Q}^{\mathrm{cyc}})_S/K)$, i.e., $\pi(x_i)|_K \neq 1 \in \mathrm{Gal}(K/\mathbb{Q})$ for $i \neq 0$. Hence the inertia subgroup

$T_i \cap \mathrm{Ker}(|_K)$ of $\mathrm{Gal}((\mathbb{Q}^{\mathrm{cyc}})_S/K)$ for $\widetilde{\ell}_i$ is generated by $\pi(x_i^p)$ if $1 \le i \le d$. Then $\pi$ induces an exact sequence

$$1 \longrightarrow NR \longrightarrow H \longrightarrow \mathrm{Gal}((K^{\mathrm{cyc}})_\emptyset/K) \longrightarrow 1 ,$$

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

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

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

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

of

$$G = \mathrm{Gal}((K^{\mathrm{cyc}})_\emptyset/\mathbb{Q}) = \mathrm{Gal}((k^{\mathrm{cyc}})_\emptyset/\mathbb{Q}),$$

where $\varpi = |_{(K^{\mathrm{cyc}})_\emptyset} \circ \pi$. Let

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

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

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

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

The restriction mapping $G \xrightarrow{|_{k^{\mathrm{cyc}}}} \mathrm{Gal}(k^{\mathrm{cyc}}/\mathbb{Q})$ induces a surjective homomorphism

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

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 $\mathrm{Gal}(k^{\mathrm{cyc}}/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^d \oplus \mathbb{Z}_p$, $\psi$ must be an isomorphism. This implies that

$$G_2 = \mathrm{Gal}((k^{\mathrm{cyc}})_\emptyset/k^{\mathrm{cyc}}).$$

Recall that

$$G_2/[G_2, G_2] \simeq \varprojlim A(k_n),$$

where $\varprojlim$ is the projective limit with respect to the norm mappings. Then we obtain the following equivalences:

$$
\begin{aligned}
\lambda(k) = \mu(k) = \nu(k) = 0 \ &\Leftrightarrow \ G_2 \simeq 1 \\
&\Leftrightarrow \ G_2 = (G_2)^p G_3 \\
&\Leftrightarrow \ F_2N/(F_2)^pF_3N = R'(F_2)^pF_3N/(F_2)^pF_3N. \qquad (2)
\end{aligned}
$$

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

**Lemma 3.1.** $\{\overline{[x_i, x_j]} \,|\, 0 \leq i < j \leq d\}$ *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

$$[g_1^{-1}x_i^p g_1, g_2^{-1}x_j^p g_2] \equiv [x_i, x_j]^{p^2} \equiv 1 \mod (F_2)^pF_3,$$

$(F_2)^pF_3N/(F_2)^pF_3$ 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 $\prod_{i=1}^d x_i^{z_i p} \equiv 1 \pmod{F_2}$ and $F/F_2$ is a free $\mathbb{Z}_p$-module generated by $\{x_jF_2 \,|\, 0 \leq j \leq d\}$, 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

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

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 $g = \prod_{0 \leq i < j \leq d}[x_i, x_j]^{z_{i,j}} \equiv 1 \pmod{(F_2)^pF_3}$ with some $z_{i,j} \in \mathbb{Z}_p$, then $[a, b]^{z_{i,j}} = \varphi_{i,j}(g) \in (F_2')^pF_3'$, and hence $z_{i,j} \equiv 0 \pmod{p}$ 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. $\square$

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

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

i.e., $d \leq 2$, by Lemma 3.1 and (2).

If $d = 1$, $R'(F_2)^p F_3 N/(F_2)^p F_3 N = \langle \overline{[x_0, x_1]}^{\mathrm{lk}(\ell_0,\ell_1)}, \overline{[x_0, x_1]}^{\mathrm{lk}(\ell_1,\ell_0)} \rangle$ is a subspace of

$$F_2 N/(F_2)^p F_3 N = \langle \overline{[x_0, x_1]} \rangle \simeq \mathbb{F}_p$$

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

If $d = 2$, $R'(F_2)^p F_3 N/(F_2)^p F_3 N = \langle \overline{\rho_0}, \overline{\rho_1}, \overline{\rho_2} \rangle$ is a subspace of

$$F_2 N/(F_2)^p F_3 N = \langle \overline{[x_0, x_1]}, \overline{[x_1, x_2]}, \overline{[x_2, x_0]} \rangle \simeq \mathbb{F}_p^3$$

(cf. Lemma 3.1). Then $(\overline{\rho_0}, \overline{\rho_1}, \overline{\rho_2}) = (\overline{[x_0, x_1]}, \overline{[x_1, x_2]}, \overline{[x_2, x_0]})A$ with a matrix

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

having the determinant

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

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

$$F \xrightarrow{\pi} \widetilde{G}_S(\mathbb{Q}) \xrightarrow{|_{K^g}} \mathrm{Gal}(K^g/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^{d+1-\delta}$$

induces a homomorphism

$$\begin{aligned}&F/F^p[F,F]\langle x_0^\delta\rangle \xrightarrow{\simeq} \mathrm{Gal}(K^g/\mathbb{Q}) \xrightarrow{|_K} \mathrm{Gal}(K/\mathbb{Q})\\ &: \overline{x_i} \mapsto \pi(x_i)|_{K^g} \mapsto \pi(x_d^{m_i})|_K\end{aligned}$$

with some integers $m_i = m_{K,i} \not\equiv 0 \pmod p$ for $\delta \leq i \leq d$. Note that $m_d = 1$.

Remark 4.1. The presentation in Theorem 2.2 is constructed to satisfy $\pi(x_i)|_{K^g} = \tau_i|_{K^g}$ for $\tau_i \in \mathrm{Gal}(\mathbb{Q}(\zeta_{p^2\ell_1\cdots\ell_d})/\mathbb{Q}(\zeta_{p^2\ell_1\cdots\ell_d/\ell_i}))$ such that $\tau_0(\zeta_{p^2}) = \zeta_{p^2}^{1+p}$ and $\tau_j(\zeta_{\ell_j}^{\alpha_{\ell_j}}) = \zeta_{\ell_j}$ if $j \neq 0$. Then $K$ is identified as the fixed field of $\langle \tau_0^\delta, \tau_d^p, \tau_i\tau_d^{-m_i} \mid \delta \leq i < d\rangle$ in $\mathbb{Q}(\zeta_{p^2\ell_1\cdots\ell_d})/\mathbb{Q}$.

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

$$\mathrm{Gal}(K^g/K) \cap \langle \pi(x_i)|_{K^g}, \pi(y_i)|_{K^g}\rangle = \langle \pi(y_i x_i^{c_{ii}})|_{K^g}\rangle$$

of $\mathfrak{l}_{K,i}$ in $\mathrm{Gal}(K^g/K)$ is generated by the Frobenius automorphism $\left(\frac{K^g/K}{\mathfrak{l}_{K,i}}\right) = \pi(y_i x_i^{c_{ii}})|_{K^g}$ with some integer $c_{ii}$. Since

$$1 = \pi(y_i x_i^{c_{ii}})|_K = \pi(x_i^{c_{ii}} \textstyle\prod_{j=\delta}^d x_j^{\mathrm{lk}(\ell_i,\ell_j)})|_K = \pi(x_d)|_K^{m_i c_{ii} + \sum_{j=\delta}^d m_j \mathrm{lk}(\ell_i,\ell_j)},$$

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

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

with entries in $\mathbb{F}_p$, which satisfies

$$\begin{pmatrix} \left(\frac{K^g/K}{\mathfrak{l}_{K,\delta}}\right) \\ \vdots \\ \left(\frac{K^g/K}{\mathfrak{l}_{K,d}}\right)\end{pmatrix} = C_K \begin{pmatrix} \pi(x_\delta)|_{K^g} \\ \vdots \\ \pi(x_d)|_{K^g}\end{pmatrix}, \tag{3}$$

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

**Lemma 4.2.** *Under the settings above, the following two conditions are equivalent, where* $(0,\cdots,0) \neq (b_\delta,\cdots,b_d) \in \mathbb{F}_p^{d+1-\delta}$*:*

1. $A(K) = \langle [\mathfrak{l}_{K,\delta}], \cdots, [\mathfrak{l}_{K,d}] \rangle \simeq (\mathbb{Z}/p\mathbb{Z})^{d-\delta}$ *and* $\prod_{i=\delta}^{d} [\mathfrak{l}_{K,i}]^{b_i} = 1$.
2. $\operatorname{rank} C_K = d - \delta$ *and* $(b_\delta, \cdots, b_d) C_K = (0, \cdots, 0)$.

*Proof.* The equation (3) implies that $\mathrm{Gal}(K^g/K) = \langle \left(\frac{K^g/K}{\mathfrak{l}_{K,\delta}}\right), \cdots, \left(\frac{K^g/K}{\mathfrak{l}_{K,d}}\right) \rangle$ if and only if $\operatorname{rank} C_K = d - \delta$. By [4, Lemma 1.1], $A(K) = \langle [\mathfrak{l}_{K,\delta}], \cdots, [\mathfrak{l}_{K,d}] \rangle \simeq \mathbb{F}_p^{d-\delta}$ if and only if $\operatorname{rank} C_K = d - \delta$. Then, since $A(K) \to \mathrm{Gal}(K^g/K) : [\mathfrak{l}_{K,i}] \mapsto \left(\frac{K^g/K}{\mathfrak{l}_{K,i}}\right)$ becomes a $\mathbb{F}_p$-linear isomorphism, we obtain the equivalence. □

If $\delta = 1$ and $m_i = 1$ 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 $S = \{\ell_1, \cdots, \ell_d\}$ 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 $k^{(1)}, \cdots, k^{(p-1)}$ of degree $p$ except for $k$ and $\mathbb{Q}_1$. Put $k^{(0)} = k$, and put

$$J = \{ j \mid \operatorname{rank} C_K = d - \delta_K \text{ for } K = k^{(j)} \} \subset \{0, 1, \cdots, p-1\}$$

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

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

Now we shall recall and prove Theorem 1.2.

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

*Proof.* Suppose that $\operatorname{rank} C_k = d - 1$ and $\operatorname{rank} B_k = d$. Then $A(k) = \langle [\mathfrak{l}_{k,1}], \cdots, [\mathfrak{l}_{k,d}] \rangle$ by Lemma 4.2, and there is $J' \subset J$ such that $B'_k = (b_{ij})_{1 \leq i \leq d, j \in J'}$ is a regular $d \times d$ matrix. Let $O_{k_1}$ denote the ring of algebraic integers in $k_1$, and let $\mathfrak{p}$ be the prime ideal of $\mathbb{Q}_1$ lying over $p$. For any $1 \leq j \leq p-1$, since $[\mathfrak{p}] \in A(\mathbb{Q}_1) \simeq 1$ and $\mathfrak{p} O_{k_1} = \mathfrak{l}_{k^{(j)},0} O_{k_1}$, we have $[\mathfrak{l}_{k^{(j)},0} O_{k_1}] = [\mathfrak{p} O_{k_1}] = 1 \in A(k_1)$. Moreover, $\mathfrak{l}_{k^{(j)},i} O_{k_1} = \mathfrak{l}_{k,i} O_{k_1}$ for any $1 \leq j \leq p-1$ and $1 \leq i \leq d$. Hence $\prod_{i=1}^{d} [\mathfrak{l}_{k,i} O_{k_1}]^{b_{ij}} = \prod_{i=1}^{d} [\mathfrak{l}_{k^{(j)},i} O_{k_1}]^{b_{ij}} = 1$ for any $j \in J'$ by Lemma 4.2.

If we write additively as '$\sum_{i=1}^{d} b_{ij}[\mathfrak{l}_{k,i}O_{k_1}] = 0$', then

$$([\mathfrak{l}_{k,1}O_{k_1}], \cdots, [\mathfrak{l}_{k,d}O_{k_1}]) = (0, \cdots, 0){B'_k}^{-1} = (0, \cdots, 0).$$

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

Remark 5.2. Note that the extensions $k^{(1)}, \cdots, k^{(p-1)}$ have the common genus class field which contains $k_1$. For $1 \leq i \leq d$, since $\pi_1(x_i)|_k = \pi_1(x_d^{m_{k,i}})|_k$ and $\langle \pi_1(x_i)|_{k_1} \rangle = \mathrm{Gal}(k_1/\mathbb{Q}_1) = \langle \pi_1(x_d)|_{k_1} \rangle$, we have $\pi_1(x_i)|_{k_1} = \pi_1(x_d^{m_{k,i}})|_{k_1}$, and hence $m_{k^{(j)},i} \equiv m_{k,i} \pmod p$ 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 $\mathrm{Gal}(k_1/k^{(j)}) = \langle \pi(x_0^{-j}x_d)|_{k_1} \rangle$, i.e., $m_0 = m_{k^{(j)},0} \equiv j^{-1} \pmod p$ 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,* $\mathrm{rank}\, B_k = 2$ *(and* $\mathrm{rank}\, C_k = 1$*) if and only if (1) is satisfied.*

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

$$C_k \in \begin{pmatrix} l_{12} & 0 \\ -l_{21} & 0 \end{pmatrix} GL_2(\mathbb{F}_p)$$

and

$$C_K \in \begin{pmatrix} 0 & -l_{01} & -l_{02} \\ 0 & l_{K,10} + l_{12} & -l_{12} \\ 0 & -l_{21} & l_{K,20} + l_{21} \end{pmatrix} GL_3(\mathbb{F}_p)$$

for $K \neq k$, we have $(l_{21}, l_{12})C_k = (0, 0)$ and $(b_{0,K}, b_{1,K}, b_{2,K})C_K = (0, 0, 0)$ with

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

where $\times$ denotes the cross product of vectors. For each $K = k^{(j)}$ with $1 \leq j \leq p-1$, $\mathrm{rank}\, C_K \leq 1$ (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 $\operatorname{rank} C_k = 0$ (i.e., $0 \notin J$). Since

$$\begin{vmatrix} l_{21} & b_{1,K} \\ l_{12} & b_{2,K} \end{vmatrix} = -l_{01}l_{12}l_{K,20} + l_{02}l_{21}l_{K,10}, \tag{4}$$

we have $J = \{0, 1, \cdots, p-1\}$ (in particular $\operatorname{rank} C_k = 1$) if (1) is satisfied. If $0 \in J$, then $(b_{10}, b_{20}) = (l_{21}, l_{12})$. If $0 \neq j \in J$, then $(b_{0j}, b_{1j}, b_{2j}) = (b_{0,K}, b_{1,K}, b_{2,K})$. Since the $2 \times 2$ minors of $B_k$ are either (4) or

$$\begin{vmatrix} b_{1,K} & b_{1,K'} \\ b_{2,K} & b_{2,K'} \end{vmatrix} = (-l_{01}l_{12}l_{K,20} + l_{02}l_{21}l_{K,10})(l_{01} + l_{02})(m_{K',0}m_{K,0}^{-1} - 1)$$

with some $K$ and $K'$, we have (1) if and only if $\operatorname{rank} B_k = 2$. $\square$

## §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

$$(\operatorname{lk}(\ell_i, \ell_j))_{0 \le i,j \le 3} = \begin{pmatrix} 0 & 5 & 8 & 5 \\ 2 + z_1 & 0 & 1 & 12 \\ 1 + z_2 & 3 & 0 & 13 \\ 0 + z_3 & 1 & 7 & 0 \end{pmatrix} \equiv \begin{pmatrix} 0 & 2 & 2 & 2 \\ 2 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \bmod 3,$$

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

$$C_k = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \quad \operatorname{rank} C_k = 2, \quad (1, 0, 2)C_k = (0, 0, 0),$$

and $A(k) \simeq (\mathbb{Z}/3\mathbb{Z})^2$ by Lemma 4.2. For $j \in \{1, 2\}$, assuming $m_{k^{(j)},0} = j \equiv j^{-1} \pmod 3$, we have

$$C_{k^{(j)}} = \begin{pmatrix} j & 2 & 2 & 2 \\ 2 & j+1 & 1 & 0 \\ 1 & 0 & j+1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \quad \operatorname{rank} C_{k^{(j)}} = 3,$$

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

$$B_k = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 1 \\ 2 & 0 & 1 \end{pmatrix}, \quad \operatorname{rank} B_k = 3.$$

Hence $A(k)$ capitulates in $k_1$ by Theorem 1.2. Since

$$\pi(y_0)|_k = \textstyle\prod_{j=1}^3 \pi(x_j)|_k^{\mathrm{lk}(\ell_0,\ell_j)} = \pi(x_3)|_k^{\sum_{j=1}^3 m_j \mathrm{lk}(\ell_0,\ell_j)} = \pi(x_3)|_k^2 \neq 1$$

by Theorem 2.2, $p$ is inert in $k/\mathbb{Q}$. 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 $k/\mathbb{Q}$ of degree $p$ such that; $p$ is inert in $k/\mathbb{Q}$, $A(k) \simeq (\mathbb{Z}/p\mathbb{Z})^{d-1}$, 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

$$(\mathrm{lk}(\ell_i,\ell_j))_{0\leq i,j\leq d} \equiv \begin{pmatrix} 0 & 0 & 1 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \\ 2 & -1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ d & -1 & 0 & \cdots & 0 \end{pmatrix} \mod p.$$

Let $k/\mathbb{Q}$ 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

$$\pi(y_0)|_k = \textstyle\prod_{j=1}^d \pi(x_j)|_k^{\mathrm{lk}(\ell_0,\ell_j)} = \prod_{j=2}^d \pi(x_j)|_k = \pi(x_d)|_k^{d-1} \neq 1$$

by Theorem 2.2, $p$ is inert in $k/\mathbb{Q}$. (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

$$C_k = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ -1 & 1 & & \\ \vdots & & \ddots & \\ -1 & & & 1 \end{pmatrix}$$

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 $m_{k^{(j)},0} \equiv$

$j^{-1} \pmod p$ as in Remark 5.2. Then

$$C_{k(j)} = \left(\begin{array}{cc|cccc} -(d-1)j & 0 & 1 & \cdots & & 1 \\ 1 & -j^{-1} & 0 & \cdots & & 0 \\ \hline 2 & -1 & 1-2j^{-1} & & & \\ \vdots & \vdots & & & \ddots & \\ d & -1 & & & & 1-dj^{-1} \end{array}\right)$$

for $1 \leq j \leq p-1$. Put $J' = \{0, 2, \cdots, d\}$ if $d < p$, and $J' = \{0, 1, 2, \cdots, p-1\}$ if $d = p$. One can easily see that $J' \subset J$, i.e., $\operatorname{rank} C_{k(j)} = d$ if $0 \neq j \in J'$. If $d < p$,

$$B'_k = (b_{ij})_{1 \leq i \leq d, j \in J'} = \begin{pmatrix} 1 & -1 & \cdots & -1 \\ 0 & 2^{-1} & & \\ \vdots & & \ddots & \\ 0 & & & d^{-1} \end{pmatrix}$$

and $b_{0j} = 0$ for any $2 \leq j \leq d$. If $d = p$,

$$B'_k = (b_{ij})_{1 \leq i \leq d, j \in J'} = \left(\begin{array}{cc|ccc} 1 & 0 & -1 & \cdots & -1 \\ \hline 0 & 1^{-1} & 2^{-1} & & \\ 0 & 2^{-1} & & \ddots & \\ \vdots & \vdots & & & (p-1)^{-1} \\ \hline 0 & (p-1)^{-1} & 0 & \cdots & 0 \end{array}\right),$$

$b_{01} = 1$, and $b_{0j} = 0$ for all $2 \leq j \leq p-1$. Since $\det B'_k \neq 0$, we have $\operatorname{rank} B_k = d$, and hence $\lambda(k) = \mu(k) = 0$ by Theorem 1.2. $\square$

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

$$(\mathrm{lk}(\ell_i, \ell_j))_{0 \leq i,j \leq 2} = \begin{pmatrix} 0 & 57 & 1 \\ 1+z_1 & 0 & 48 \\ 2+z_2 & 65 & 0 \end{pmatrix} \equiv \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 2 & -1 & 0 \end{pmatrix} \mod 3$$

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 $\lambda(k^g) = \mu(k^g) = \nu(k^g) = 0$ 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


[ 1 ] A. Aiba, On the vanishing of Iwasawa invariants of geometric cyclotomic $\mathbb{Z}_p$-extensions, Acta Arith. **108** (2003), no. 2, 113–122.

[ 2 ] J. Blondeau, P. Lebacque and C. Maire, On the cohomological dimension of some pro-$p$-extensions above the cyclotomic $\mathbb{Z}_p$-extension of a number field, Mosc. Math. J. **13** (2013), no. 4, 601–619.

[ 3 ] B. Ferrero and L. C. Washington, The Iwasawa invariant $\mu_p$ vanishes for abelian number fields, Ann. of Math. (2) **109** (1979), no. 2, 377–395.

[ 4 ] T. Fukuda, On the vanishing of Iwasawa invariants of certain cyclic extensions of $\mathbf{Q}$ with prime degree, Proc. Japan Acad. Ser. A Math. Sci. **73** (1997), no. 6, 108–110.

[ 5 ] R. Greenberg, On the Iwasawa invariants of totally real number fields, Amer. J. Math. **98** (1976), no. 1, 263–284.

[ 6 ] J. Hillman, D. Matei and M. Morishita, Pro-$p$ link groups and $p$-homology groups, Primes and knots, 121–136, Contemp. Math. **416**, Amer. Math. Soc., Providence, RI, 2006.

[ 7 ] T. Itoh and Y. Mizusawa, On tamely ramified pro-$p$-extensions over $\mathbb{Z}_p$-extensions of $\mathbb{Q}$, Math. Proc. Cambridge Philos. Soc. **156** (2014), no. 2, 281–294.

[ 8 ] T. Kadokami and Y. Mizusawa, Iwasawa type formula for covers of a link in a rational homology sphere, J. Knot Theory Ramifications **17** (2008), no. 10, 1199–1221.

[ 9 ] T. Kadokami and Y. Mizusawa, On the Iwasawa invariants of a link in the 3-sphere, Kyushu J. Math. **67** (2013), no. 1, 215–226.

[10] H. Koch, Galois theory of $p$-extensions, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002.

[11] J. Labute, Linking numbers and the tame Fontaine-Mazur conjecture, Ann. Math. Qué. **38** (2014), no. 1, 61–71.

[12] B. Mazur, Remarks on the Alexander polynomial, unpublished paper, 1963/1964.

[13] Y. Mizusawa, On pro-$p$ link groups of number fields, Trans. Amer. Math. Soc. **372** (2019), no. 10, 7225–7254.

[14] Y. Mizusawa and M. Ozaki, On tame pro-$p$ Galois groups over basic $\mathbb{Z}_p$-extensions, Math. Z. **273** (2013), no. 3–4, 1161–1173.

[15] M. Morishita, On certain analogies between knots and primes, J. Reine Angew. Math. **550** (2002), 141–167.

[16] M. Morishita, Knots and Primes - An Introduction to Arithmetic Topology, Springer, 2012.

[17] L. Salle, Sur les pro-$p$-extensions à ramification restreinte au-dessus de la $\mathbb{Z}_p$-extension cyclotomique d'un corps de nombres, J. Théor. Nombres Bordeaux **20** (2008), no. 2, 485–523.

[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.

[19] J. Ueki, On the Iwasawa $\mu$-invariants of branched $\mathbf{Z}_p$-covers, Proc. Japan Acad. Ser. A Math. Sci. **92** (2016), no. 6, 67–72.

[20] J. Ueki, On the Iwasawa invariants for links and Kida's formula, Int. J. Math. **28** (2017), no. 6, 1750035.

[21] L. C. Washington, Introduction to cyclotomic fields, Second edition, Graduate Texts in Mathematics **83**, Springer-Verlag, New York, 1997.

[22] G. Yamamoto, On the vanishing of Iwasawa invariants of absolutely abelian $p$-extensions. Acta Arith. **94** (2000), no. 4, 365–371.

[23] G. Yamamoto, Iwasawa invariants of abelian $p$-extension fields, thesis, Waseda Univ., 2001.

[24] G. Yamamoto, Linking numbers for primes and $\mathbf{Z}_p$-extensions of abelian $p$-extension fields, a talk at Muroran Number Theory Conference, Muroran Institute of Technology, March 2004.

[25] G. Yamamoto, On linking numbers of primes and $\mathbf{Z}_p$-extensions (Japanese), Proceedings of the 11th Workshop on Number Theory in Hokuriku, Kanazawa University, December 2012 (2013), 8–20.

*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.*