数理解析研究所講究録
第886巻 1994年 29-38

Some relations between invariants of cyclotomic $\mathbf{Z}_p$-fields

Takashi ICHIKAWA (市川尚志)
Department of Mathematics
Faculty of Science and Engineering
Saga University, Saga 840, Japan

Abstract

In this paper, we show a basic inequality of Riemann-Hurwitz type for certain invariants (connected with the λ-invariants) of cyclotomic $\mathbf{Z}_p$-fields. As its application, if the Vandiver conjecture holds for p, then we have an upper bound of the λ-invariants of some cyclotomic $\mathbf{Z}_p$-fields containing $\exp(2\pi\sqrt{-1}/p)$.

Introduction

For a cyclotomic $\mathbf{Z}_p$-extension K of a number field K_0 with μ-invariant 0, let X_K (resp. $\overline{X}_K$) be the Galois group over K of its maximal abelian p-extension which is unramified (resp. unramified outside places dividing p) over K. We introduce some invariants of K/K_0 : let λ_K (resp. $\overline{\lambda}_K$) be the $\mathbf{Z}_p$-rank of X_K (resp. of the $\mathbf{Z}_p[[\mathrm{Gal}(K/K_0)]]$-torsion submodule of $\overline{X}_K$), and put $\lambda_K^- = \lambda_K - \lambda_{K\cap\mathbf{R}}$. In [5], Kida proved a Riemann-Hurwitz formula for λ^- of cyclotomic $\mathbf{Z}_p$-extensions of CM type, and this follows from a similar formula for $\overline{\lambda}$ of totally real cyclotomic $\mathbf{Z}_p$-extensions which is shown in [8]. Recently, in [6] and [9], Nguyen Quang Do and Wingberg proved a Riemann-Hurwitz formula for $\overline{\lambda}$ of general cyclotomic $\mathbf{Z}_p$-extensions under some assumptions which seemed to cannot be checked easily. We note that the results of [6] and [9] do not deduce immediately a formula for λ because the relation between λ and $\overline{\lambda}$ is not clear. The aim of this paper is to show a basic inequality of Riemann-Hurwitz type for certain invariants of cyclotomic $\mathbf{Z}_p$-extensions which deduces an inequality for λ.

Under the influence of genus theory, we consider an invariant

$$\lambda'_K = \dim_{\mathbf{F}_p}(X_K/pX_K).$$

Then it is easy to see that $\lambda'_K \geq \lambda_K$ and that $\lambda'_K = \lambda_K$ if and only if X_K is a free $\mathbf{Z}_p$-module. We will show that if K contains $\zeta_p = \exp(2\pi\sqrt{-1}/p)$ and L/K is a Galois p-extension unramified at all infinite places such that there is no unramified extensions between their intermediate fields, then

$$\lambda'_L - 1 \leq [L:K](\lambda'_K - 1) + \sum_v (e(v/K) - 1), \tag{1}$$

where v runs through all finite places of L, and $e(v/K)$ denotes the ramification index of v over K which will be well-defined and is equal to the local degree of v over K. In particular, if p does not divide the class number of $\mathbf{Q}(\cos(2\pi/p))$ and K is the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}(\zeta_p)$, then we have

$$\lambda_L - 1 \leq [L:K](\lambda_K - 1) + \sum_v (e(v/K) - 1). \tag{2}$$

When p is odd and $L = K(p^{1/p^k})$, we show that X_L is a cyclic $A_q = \mathbf{Z}_p[[\mathrm{Gal}(L/\mathbf{Q})]]$-module annihilated by an element Φ of A_q which is a deformation of the sum of the p-adic L-functions, and that if (2) is an equality, then $X_L \cong A_q/(A_q\Phi)$. When $p = 2$, we give examples of real quadratic extensions L/K such that (1) is an equality (on the other hand, if the Greenberg conjecture [2] holds for L, then λ_L is always equal to 0).

1

Throughout this paper, we put $\zeta_n = \exp(2\pi\sqrt{-1}/n)$ $(n \in \mathbf{N})$, and we consider any field as a subfield of $\mathbf{C}$. For a prime number p, we call K a *cyclotomic $\mathbf{Z}_p$-field* if K is a finite extension of the unique $\mathbf{Z}_p$-extension of $\mathbf{Q}$. Then any finite place of $\mathbf{Q}$ has finitely many extensions in K, and K becomes a $\mathbf{Z}_p$-extension of a number field finite over $\mathbf{Q}$ which we denote by $K = \bigcup_{n\geq 0} K_n$. For a cyclotomic $\mathbf{Z}_p$-field $K = \bigcup_{n\geq 0} K_n$, let X_K be a $\mathbf{Z}_p$-module which is the projective limit of the p-ideal class groups of K_n $(n \geq 0)$ with respect to the norm maps, and let $\widetilde{K}$ (resp. $\widetilde{K}_n$) be the maximal unramified abelian p-extension of K (resp. K_n). Then $\widetilde{K} = \bigcup_{n\geq 0} \widetilde{K}_n$, and hence by class field theory, $X_K \cong \mathrm{Gal}(\widetilde{K}/K)$. We define $\mu_K = 0$ if X_K is a finitely generated $\mathbf{Z}_p$-module.

Let K be a cyclotomic $\mathbf{Z}_p$-field, and let L be a finite extension of K. Then we can take $K = \bigcup_{n\geq 0} K_n$ and $L = \bigcup_{n\geq 0} L_n$ such that $[L_n : K_n] = [L : K]$ for any n.

For a place v of L, we denote by $e(v|L_n/K_n)$ (resp. $f(v|L_n/K_n)$) the ramification index (resp. the relative degree) of $v|L_n$ over K_n, and let $g(v|L_n/K_n)$ be the number of places v' of L_n satisfying $v'|K_n = v|K_n$. If L is Galois over K, then for sufficiently large n, L_n is Galois over K_n and hence

$$e(v|L_n/K_n) \cdot f(v|L_n/K_n) \cdot g(v|L_n/K_n) \;=\; [L_n : K_n].$$

Proposition 1. *Assume that $K \ni \zeta_p$ and that L/K is a Galois p-extension. Then for any place v of L, $\lim_{n\to\infty} e(v|L_n/K_n)$ and $\lim_{n\to\infty} g(v|L_n/K_n)$ exist, and $\lim_{n\to\infty} f(v|L_n/K_n) = 1$.*

Proof. It is enough to show this proposition for finite places. From the assumption, there exists a sequence of field extensions:

$$K = M^0 \subset M^1 \subset \cdots \subset M^k = L$$

such that M^{i+1}/M^i $(i = 0, ..., k-1)$ is a cyclic extension of degree p. Then for each i, $M^{i+1} = M^i(\sqrt[p]{\alpha_i})$ for some $\alpha_i \in (M^i)^\times$. Put $M_n^0 = K_n$ and $M_n^{i+1} = K_n(\sqrt[p]{\alpha_0}, \sqrt[p]{\alpha_1}, ..., \sqrt[p]{\alpha_i})$ for $i = 0, ..., k-1$. Then there exists $N \in \mathbf{N}$ such that for any $n \geq N$, $[L_n : K_n] = [L : K]$ and $\alpha_i \in (M_n^i)^\times$. Hence ($(M_n^i)_v$: the completion of M_n^i by v)

$$\lim_{n\to\infty} g(v|M_n^{i+1}/M_n^i) \;=\; \begin{cases} 1 & \text{if } (M_n^i)_v \not\ni \sqrt[p]{\alpha} \text{ for any } n \\ p & \text{otherwise.} \end{cases}$$

Therefore,

$$\lim_{n\to\infty} g(v|L_n/K_n) \;=\; \prod_{i=0}^{k-1} \lim_{n\to\infty} g(v|M_n^{i+1}/M_n^i)$$

is well-defined.

We will show the rest of the statement. First we assume that v does not divide p. Then the completion L_v of L by v is a discrete valuation field, and hence $\lim_{n\to\infty} e(v|L_n/K_n)$ (resp. $\lim_{n\to\infty} f(v|L_n/K_n)$) is equal to the ramification index (resp. the relative degree) of L_v/K_v. Moreover, the latter is equal to 1 because the residue field of K_v is the unique $\mathbf{Z}_p$-extension of a finite field. Second we assume that v divides p. Then the p-power degree of $e(v|K_n/K_0)$ tends to infinity as $n \to \infty$, and hence there exists $N' \geq N$ such that one can take v-units $\beta_i \in M_n^i$ satisfying $M_n^{i+1} = M_n^i(\sqrt[p]{\beta_i})$ for any $n \geq N'$ and $i = 0, ..., k-1$. Let k_n^i be the residue field of M_n^i at v, and put $\overline{\beta_i} = \beta_i \bmod(v)$. Then for any $n \geq N'$ and $i = 0, ..., k-1$, $k_n^{i+1} = k_n^i(\sqrt[p]{\overline{\beta_i}}) = k_n^i$ because k_n^i is a finite field of p-power order. Therefore,

$$\lim_{n\to\infty} f(v|L_n/K_n) \;=\; \prod_{i=0}^{k-1} \lim_{n\to\infty} f(v|M_n^{i+1}/M_n^i) \;=\; 1,$$

and hence

$$\lim_{n\to\infty} e(v|L_n/K_n) = \frac{[L:K]}{\lim_{n\to\infty} g(v|L_n/K_n)}.$$

2

Let K, L, and v be as in Proposition 1. Then we call $\lim_{n\to\infty} e(v|L_n/K_n)$ the *ramification index* of v over K, and denote this by $e(v/K)$. If $e(v/K) > 1$, then we call L/K is *ramified* at v. Let $P_f(L)$ (resp. $P_f(L_n)$) be the set of finite places of L (resp. L_n), and let $R(L/K)$ (resp. $R(L_n/K_n)$) be the set of places of L (resp. L_n) ramified over K (resp. K_n). By Proposition 1, for sufficiently large n, the restriction $v \mapsto v|L_n$ of places of L induces a bijection

$$R(L/K) \cap P_f(L) \xrightarrow{\sim} R(L_n/K_n) \cap P_f(L_n),$$

and hence $R(L/K) \cap P_f(L)$ is a finite set. It is shown by Iwasawa [3, Theorem 3] that if L is a p-extension of a $\mathbf{Z}_p$-field K with $\mu_K = 0$, then $\mu_L = 0$. As for the λ'-invariant, we have the following results.

Theorem 1. *Let K be a cyclotomic $\mathbf{Z}_p$-field such that $K \ni \zeta_p$ and $\mu_K = 0$, and let L/K be a cyclic extension of degree p such that $R(L/K) \neq \emptyset$ and $R(L/K) \subset P_f(L)$. Then*

$$\lambda'_L - 1 \leq p(\lambda'_K - 1) + \sum_{v\in P_f(L)} (e(v/K) - 1).$$

Proof. Put $\Gamma = \mathrm{Gal}(L/K)$, and let γ be a generator of Γ. Let $\tilde{L}$ (resp. $\tilde{L}_n$) be the maximal unramified abelian p-extension of L (resp. L_n), and put $G = \mathrm{Gal}(\tilde{L}/K)$, $X_L = \mathrm{Gal}(\tilde{L}/L)$. Let $R(L/K) = \{v_0, v_1, ..., v_s\}$, and for each $i = 0, ..., s$, let $\tilde{v}_i$ be a place of $\tilde{L}$ dividing v_i with inertia subgroup I_i of G. Put $G_n = \mathrm{Gal}(\tilde{L}_n/K_n)$ and $X_{L,n} = \mathrm{Gal}(\tilde{L}_n/L_n)$, and let $I_{i,n}$ be the inertia subgroup of G_n at $\tilde{v}_i$. Since for sufficiently large n, $[L_n : K_n] = p$ and L_n/K_n is totally ramified at v_i, the injection $I_{i,n} \hookrightarrow G_n$ induces an isomorphism $I_{i,n} \xrightarrow{\sim} G_n/X_{L,n}$. Therefore,

$$I_i = \varprojlim I_{i,n} \xrightarrow{\sim} \varprojlim G_n/X_{L,n} = G/X_L = \Gamma,$$

and hence $G = X_L I_i$ $(i = 0, ..., s)$. For each i, let $\sigma_i \in I_i$ maps to γ, and $a_i \in X_L$ satisfying $\sigma_i = a_i\sigma_0$. Put $S = \gamma - 1$ and

$$\nu = 1 + \gamma + \gamma^2 + \cdots + \gamma^{p-1} = \{(1+S)^p - 1\}/S$$

which act on X_L. Since $\sigma_i{}^p = 1$ and $\sigma_i{}^p = \nu(a_i)\sigma_0{}^p$, $\nu(a_i) = 0$. Let M be the sub $\mathbf{Z}_p$-module of X_L generated by $a_1, ..., a_s$. Since $\widetilde{K}/K$ is the maximal unramified

abelian subextension of $\tilde{L}/K$, $\mathrm{Gal}(\tilde{L}/\widetilde{K})$ is the closed subgroup of X_L generated by SX_L, I_0, and $a_1, ..., a_s$. Therefore,

$$X_K = G/\mathrm{Gal}(\tilde{L}/\widetilde{K}) \xrightarrow{\sim} X_L/(M + SX_L),$$

and hence

$$0 \longrightarrow M/(M \cap SX_L) \longrightarrow X_L/SX_L \longrightarrow X_K \longrightarrow 0$$

is exact. Let $b_j \in X_L$ $(j = 1, ..., \lambda'_K)$ satisfying

$$X_K = \sum_{j=1}^{\lambda'_K} \mathbf{Z}_p \bar{b}_j \quad (\bar{b}_j = b_j \bmod (M + SX_L)).$$

Then

$$X_L/SX_L = \sum_{i=1}^{s} \mathbf{Z}_p a_i + \sum_{j=1}^{\lambda'_K} \mathbf{Z}_p b_j.$$

Since $S\nu = 0$ on X_L and $\nu(a_i) = 0$,

$$X_L = \sum_{k=0}^{p-2} \sum_{i=1}^{s} \mathbf{Z}_p S^k(a_i) + \sum_{l=0}^{p-1} \sum_{j=1}^{\lambda'_K} \mathbf{Z}_p S^l(b_j).$$

Therefore,

$$\lambda'_L - 1 \leq (p-1)s + p\lambda'_K - 1 = p(\lambda'_K - 1) + (s+1)(p-1).$$

Theorem 2. *Let K be a cyclotomic $\mathbf{Z}_p$-field such that $K \ni \zeta_p$ and $\mu_K = 0$, and let $K = M^0 \subset M^1 \subset \cdots \subset M^k = L$ be a sequence of cyclic extensions of degree p such that $R(M^{i+1}/M^i) \neq \emptyset$ and $R(M^{i+1}/M^i) \subset P_f(M^{i+1})$ for any $i = 0, ..., k-1$. Then*

$$\lambda'_L - 1 \leq [L : K](\lambda'_K - 1) + \sum_{v \in P_f(L)} (e(v/K) - 1).$$

Proof. We will show this theorem by the induction on k. Assume that there exist cyclotomic $\mathbf{Z}_p$-fields $K \subset M \subset L$ such that

$$\lambda'_M - 1 \leq [M : K](\lambda'_K - 1) + \sum_{v' \in P_f(M)} (e(v'/K) - 1),$$

and that L/M is a cyclic extension of degree p with $\emptyset \neq R(L/K) \subset P_f(L)$. Then by Theorem 1 and the above inequality,

$$\lambda'_L - 1 \leq [L : K](\lambda'_K - 1) + p \sum_{v' \in P_f(M)} (e(v'/K) - 1) + \sum_{v \in P_f(L)} (e(v/M) - 1).$$

By Proposition 1, $P_f(M)$ is a disjoint union of its subsets $P_1(M)$ and $P_2(M)$ consisting of finite places of M ramified in L and splitting in L respectively. Hence

$$\sum_{v\in P_f(L)}(e(v/K)-1)=\sum_{v'\in P_1(M)}(pe(v'/K)-1)+p\sum_{v'\in P_2(M)}(e(v'/K)-1),$$

and

$$\begin{aligned}&\sum_{v'\in P_1(M)}(pe(v'/K)-1)\\ &=p\sum_{v'\in P_1(M)}(e(v'/K)-1)+(p-1)|P_1(M)|\\ &=p\sum_{v'\in P_1(M)}(e(v'/K)-1)+\sum_{v\in P_f(L)}(e(v/M)-1).\end{aligned}$$

Therefore,

$$\lambda'_L-1\ \le\ [L:K](\lambda'_K-1)+\sum_{v\in P_f(L)}(e(v/K)-1).$$

3

In what follows, let K be the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}(\zeta_p)$. Then by a result of Ferrero-Washington [1], $\mu_K=0$. Let h_p^+ denote the class number of $\mathbf{Q}(\cos(2\pi/p))$.

Theorem 3. *Assume that p does not divide h_p^+, and let $K=M^0\subset\cdots\subset M^k=L$ be a sequence of cyclic extensions of degree p such that $R(M^{i+1}/M^i)\neq\emptyset$ and $R(M^{i+1}/M^i)\subset P_f(M^{i+1})$ for any $i=0,\ldots,k-1$. Then*

$$\lambda_L-1\ \le\ [L:K](\lambda_K-1)+\sum_{v\in P_f(L)}(e(v/K)-1).$$

Proof. This follows from Theorem 2 and the result of Iwasawa which says that X_K is a free $\mathbf{Z}_p$-module (cf. [7, Theorem 10.16]).

Corollary 1. *Assume that p does not divide h_p^+, and let v_p be the unique place of K dividing p. Let L/K a cyclic extension of degree p such that $R(L/K)\neq\emptyset$ and $R(L/K)\subset P_f(L)$, and let N and I be the endomorphisms of the unit group U_L of L defined by $N(a)=a^{1+\gamma+\cdots+\gamma^{p-1}}$ and $I(a)=a^{\gamma-1}$ $(a\in U_L)$ respectively, where γ is a generator of* $\mathrm{Gal}(L/K)$. *Then*

$$\frac{|\mathrm{Ker}(N)/\mathrm{Im}(I)|}{|\mathrm{Ker}(I)/\mathrm{Im}(N)|}\ \ge\ \begin{cases}p & \text{if } v_p \text{ is unramified in } L\\ 1 & \text{if } v_p \text{ is ramified in } L.\end{cases}$$

Proof. Put

$$p^m = \frac{|\mathrm{Ker}(I)/\mathrm{Im}(N)|}{|\mathrm{Ker}(N)/\mathrm{Im}(I)|}.$$

Then by a result of Iwasawa [4, Theorem 6],

$$\lambda_L - 1 = p(\lambda_K - 1) + (m+1)(p-1) + \sum_{v \in P_f'(L)} (e(v/K) - 1),$$

where $P_f'(L)$ is the set of finite places of L not dividing p. Hence

$$m \leq \begin{cases} -1 & \text{if } v_p \text{ is unramified in } L \\ 0 & \text{if } v_p \text{ is ramified in } L. \end{cases}$$

4

In this section, assume that $p > 2$, and put $L = K(p^{1/p^k})$ for $k \in \mathbf{N}$.

Proposition 2. *The Galois extension L/K is of degree p^k, and there exists a unique place of L dividing p which is totally ramified over K.*

Proof. For $n \geq 0$, let C be the completion of $\mathbf{Q}(\zeta_{p^n})$ by the unique place of K dividing p. Then by Proposition 1, to prove this proposition, it is enough to show that $C(p^{1/p^i}) \neq C(p^{1/p^{i+1}})$ for any $i = 0, \ldots, k-1$. On the contrary, assume that $C(\sqrt[p]{\alpha}) = C(\alpha)$ $(\alpha := p^{1/p^i})$ for some i. Then $\mathbf{Q}_p(\sqrt[p]{\alpha})/\mathbf{Q}_p(\alpha)$ is an abelian extension because $C(\alpha)/\mathbf{Q}_p(\alpha)$ is an abelian extension. Since $\sqrt[p]{\alpha} \notin \mathbf{Q}_p(\alpha)$, $\zeta_p \in \mathbf{Q}_p(\alpha)$, and hence $p^i = [\mathbf{Q}_p(\alpha) : \mathbf{Q}_p]$ is divisible by $p-1 = [\mathbf{Q}_p(\zeta_p) : \mathbf{Q}_p]$, which is a contradiction.

Corollary 2. *Assume that p does not divide h_p^+. Then $\lambda_L \leq p^k \lambda_K$.*

Proof. This follows from Theorem 3 and Proposition 2.

Put $\Delta = \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$, and regard Δ as a subgroup of $\mathrm{Gal}(K/\mathbf{Q})$ by the Teichmüller character $\omega : \mathbf{F}_p^\times \to \mathbf{Z}_p^\times$ and the isomorphisms $\Delta \cong \mathbf{F}_p^\times$, $\mathrm{Gal}(K/\mathbf{Q}) \cong \mathbf{Z}_p^\times$ induced from the Galois action on $\{\zeta_{p^n}\}_{n \in \mathbf{N}}$. For each $i = 0, 1, \ldots, p-2$, put

$$\varepsilon_i = \frac{1}{|\Delta|} \sum_{\delta \in \Delta} \omega^{-i}(\delta) \cdot \delta \in \mathbf{Z}_p[[\mathrm{Gal}(K/\mathbf{Q})]],$$

and for each $i = 3, 5, \ldots, p-2$, let $L_p(s, \omega^{1-i})$ denote the p-adic L-function with character ω^{1-i}. Let γ and q be the elements of $\mathrm{Gal}(L/\mathbf{Q}(\zeta_p))$ given by $\gamma(\zeta_{p^n}) =$

$\zeta_{p^n}{}^{p+1}$, $\gamma(p^{1/p^k}) = p^{1/p^k}$ and $q(\zeta_{p^n}) = \zeta_{p^n}$, $q(p^{1/p^k}) = \zeta_{p^k}p^{1/p^k}$ $(n \geq 0)$ respectively. Then under the correspondences $\gamma \leftrightarrow 1+T$ and $q \leftrightarrow 1+S$, $\mathbf{Z}_p[[\mathrm{Gal}(L/\mathbf{Q}(\zeta_p))]]$ is isomorphic to the quotient ring Λ_q of $\mathbf{Z}_p[[T,S]]_{\mathrm{n.c}}$ (: the non-commutative power series ring over $\mathbf{Z}_p$ with variables T and S) by the relations $(1+T)(1+S) = (1+S)^{p+1}(1+T)$ and $(1+S)^{p^k} = 1$. Therefore, $A_q = \mathbf{Z}_p[[\mathrm{Gal}(L/\mathbf{Q})]]$ satisfies

$$A_q = \bigoplus_{i=0}^{p-2} \varepsilon_i \mathbf{Z}_p[[\mathrm{Gal}(L/\mathbf{Q}(\zeta_p))]] \cong \bigoplus_{i=0}^{p-2} \varepsilon_i \Lambda_q. \tag{3}$$

From the injection $\iota : \mathrm{Gal}(K/\mathbf{Q}) \to \mathrm{Gal}(L/\mathbf{Q})$ given by $\iota(\sigma)(p^{1/p^k}) = p^{1/p^k}$ $(\sigma \in \mathrm{Gal}(K/\mathbf{Q}))$, we can regard $\mathbf{Z}_p[[\mathrm{Gal}(K/\mathbf{Q})]]$ as a sub $\mathbf{Z}_p$-algebra of A_q. Let $\tilde{L}$ be the maximal unramified abelian p-extension of L, and let $\tau \in \mathrm{Gal}(L/\mathbf{Q})$ act on $X_L = \mathrm{Gal}(\tilde{L}/L)$ as $\tau(x) = \tilde{\tau}x\tilde{\tau}^{-1}$ $(\tau \in \mathrm{Gal}(L/\mathbf{Q}), x \in X_L)$ where $\tilde{\tau} \in \mathrm{Gal}(\tilde{L}/\mathbf{Q})$ is a lifting of τ. Then this action is well-defined, and hence we can regard X_L as a left A_q-module.

Theorem 4. *Assume that p does not divide h_p^+. Then there exist $\Phi \in A_q$ and $z \in X_L$ which satisfy the following:*

(a) *$A_q \ni \alpha \mapsto \alpha z \in X_L$ induces a surjective A_q-homomorphism $A_q/(A_q\Phi) \to X_L$.*

(b) *If we put $\Phi = \sum_{i=0}^{p-2} \varepsilon_i F_i$ $(F_i \in \Lambda_q)$ under the isomorphism (3), then*

$$F_i|_{S=0,T=(1+p)^s-1} = \begin{cases} 1 & (i = 0,1,2,4,\ldots,p-3) \\ L_p(s,\omega^{1-i}) & (i = 3,5,\ldots,p-2). \end{cases}$$

Moreover, if $\lambda_L = p^k\lambda_K$, then the above homomorphism $A_q/(A_q\Phi) \to X_L$ is an isomorphism.

Proof. Put $\Lambda = \mathbf{Z}_p[[T]]$ and $A = \mathbf{Z}_p[[\mathrm{Gal}(K/\mathbf{Q})]]$. Then under the correspondence $\gamma \leftrightarrow 1+T$, $\mathbf{Z}_p[[\mathrm{Gal}(K/\mathbf{Q}(\zeta_p))]]$ is isomorphic to Λ, and hence

$$A = \bigoplus_{i=0}^{p-2} \varepsilon_i \mathbf{Z}_p[[\mathrm{Gal}(K/\mathbf{Q}(\zeta_p))]] \cong \bigoplus_{i=0}^{p-2} \varepsilon_i \Lambda. \tag{4}$$

By Proposition 2 and the proof of Theorem 1, $X_K \cong X_L/SX_L$. Let $\sigma \in \mathrm{Gal}(K/\mathbf{Q})$ act on X_K as $\sigma(x) = \tilde{\sigma}x\tilde{\sigma}^{-1}$ $(\sigma \in \mathrm{Gal}(K/\mathbf{Q}), x \in X_K)$, where $\tilde{\sigma} \in \mathrm{Gal}(\widetilde{K}/\mathbf{Q})$ is a lifting of σ. Then this action induces an action of A on $X_K \cong X_L/SX_L$ compatible with the A_q-module structure of X_L. By a result of Iwasawa (cf. [7, Theorem 10.16]), there exist $\phi \in A$ and $z_0 \in X_K$ such that $A \ni \alpha \mapsto \alpha z_0 \in X_K$ induces an A-isomorphism $A/(A\phi) \xrightarrow{\sim} X_K$, and that if we put $\phi = \sum_{i=0}^{p-2} \varepsilon_i f_i$ $(f_i \in \Lambda)$ under

the isomorphism (4), then $f_i \notin p\Lambda$ and

$$f_i|_{T=(1+p)^s-1} = \begin{cases} 1 & (i = 0, 1, 2, 4, ..., p-3) \\ L_p(s, \omega^{1-i}) & (i = 3, 5, ..., p-2). \end{cases}$$

Let z be an element of X_L such that $z \bmod(SX_L) = z_0$. Then by Nakayama's lemma, $A_q\alpha \mapsto \alpha z \in X_L$ is a surjective A_q-homomorphism. Since $\phi(z) \in SX_L$, there exists $\Phi \in A_q$ such that $\Phi(z) = 0$ and $\Phi \equiv \phi \bmod(SA_q)$, and hence we have a surjective A_q-homomorphism $A_q/(A_q\Phi) \to X_L$. For each i, let F_i be the element of Λ_q such that $\varepsilon_i\Phi = \varepsilon_i F_i$ under (3). Then $\Phi = \sum_{i=0}^{p-2} \varepsilon_i F_i$ and $F_i \equiv f_i \bmod(S\Lambda_q)$. Hence $A_q/(A_q\Phi)$ is a $\mathbf{Z}_p$-module with $p^k\lambda_K$ generators $S^a\varepsilon_i T^b$ $(0 \le a < p^k, 0 \le i < p-1, 0 \le b < \mathrm{rank}_{\mathbf{Z}_p}(\Lambda/\Lambda f_i))$. Therefore, if $\lambda_L = p^k\lambda_K$, then the homomorphism $A_q/(A_q\Phi) \to X_L$ is an isomorphism.

5

In this section, we assume that $p = 2$ and study the λ'-invariants of certain cyclotomic $\mathbf{Z}_2$-fields.

Theorem 5. *Let $p_1, ..., p_t$ be primes such that $p_i \equiv 5 \bmod(8)$ $(i = 1, ..., t)$, and put $m = p_1 \cdots p_t$ and $L = K(\sqrt{m})$. Then $\lambda'_L = t - 1$.*

Proof. Since $K/\mathbf{Q}$ is totally ramified at 2 and $\mathbf{Q}(\sqrt{m})/\mathbf{Q}$ is unramified at 2, $L/\mathbf{Q}(\sqrt{m})$ is totally ramified at any place of $\mathbf{Q}(\sqrt{m})$ dividing 2. Let I_0 be the ideal class group of $\mathbf{Q}(\sqrt{m})$ denoted as an additive group. Then the canonical homomorphism $X_L/2X_L \to I_0/2I_0$ is a surjection. By genus theory, $I_0/2I_0 \cong \mathrm{Gal}(\mathbf{Q}(\sqrt{p_1}, ..., \sqrt{p_t})/K)$, and hence $\lambda'_L \ge t-1$. Since each p_i generates $1+4\mathbf{Z}_2 \cong \mathrm{Gal}(K/\mathbf{Q})$, p_i is unramified and remains prime in K. Hence L/K is only ramified at p_i $(i = 1, ..., t)$. Therefore, by Theorem 2,

$$\lambda'_L - 1 \le [L : K](\lambda'_K - 1) + \sum_{v \in P_f(L)} (e(v/K) - 1) = t - 2,$$

and hence we have $\lambda'_L = t - 1$.

Corollary 3. *For each $n \ge 0$, let $K_n/\mathbf{Q}$ the unique subextension of $K/\mathbf{Q}$ with Galois group $\mathbf{Z}/2^n\mathbf{Z}$. Let m be as above, and let I_n be the ideal class group of $K_n(\sqrt{m})$. Then $|I_n/2I_n| = 2^{t-1}$.*

Proof. Since $K(\sqrt{m})/\mathbf{Q}(\sqrt{m})$ is totally ramified at any place of $\mathbf{Q}(\sqrt{m})$ lying above 2,

$$|I_0/2I_0| \le |I_n/2I_n| \le |X_{K(\sqrt{m})}/2X_{K(\sqrt{m})}|.$$

Therefore, by Theorem 5, we have $|I_n/2I_n| = 2^{t-1}$.

References

1. B. Ferrero and L. Washington, The Iwasawa invariant μ_p vanishes for abelian number fields, *Ann. of Math.* **109** (1979), 377-395.

2. R. Greenberg, On the Iwasawa invariants of totally real number fields, *Amer. J. Math.* **98** (1976), 263-284.

3. K. Iwasawa, On the μ-invariants of $\mathbf{Z}_l$-extensions, *in* "Number theory, algebraic geometry and commutative algebra" pp.1-11, Kinokuniya, Tokyo, 1973.

4. K. Iwasawa, Riemann-Hurwitz formula and p-adic Galois representations for number fields, *Tôhoku Math. J.* **33** (1981), 263-288.

5. Y. Kida, l-extensions of CM-fields and cyclotomic invariants, *J. Number Theory* **12** (1980), 519-528.

6. T. Nguyen Quang Do, K_3 et formules de Riemann-Hurwitz p-adiques, to appear in *K-theory.*

7. L.C. Washington, "Introduction to cyclotomic fields", Graduate Texts in Mathematics 83, Springer-Verlag, 1982.

8. K. Wingberg, Duality theorems for Γ-extensions of algebraic number fields, *Compositio Math.* **55** (1985), 333-381.

9. K. Wingberg, On the maximal unramified extension of an algebraic number field, *J. reine angew. Math.* **440** (1993), 129-156.