Greenberg's conjecture and Leopoldt's conjecture

By Norikazu KUBOTERA

Department of Information and Computer Science, School of Science and Engineering, Waseda University,
3-4-1, Okubo, Shinjuku-ku, Tokyo 169-8555
(Communicated by Shokichi IYANAGA, M. J. A., Sept. 12, 2000)

Abstract: Let p be an odd prime number. We show that the Iwasawa invariants of a certain non-abelian p-extension fields of $\mathbf{Q}$ vanish. And we construct non-abelian p-extensions over some imaginary quadratic fields satisfying Leopoldt's conjecture on the p-adic regulator.

Key words: The Iwasawa invariants; Leopoldt's conjecture; embedding problems.

1. Introduction. Let p be an odd prime number and k a finite algebraic number field. Let k_∞ be the cyclotomic $\mathbf{Z}_p$-extension of k. Greenberg [3] conjectured that if k is a totally real number field, the Iwasawa λ-invariant $\lambda_p(k_\infty/k)$ and the Iwasawa μ-invariant $\mu_p(k_\infty/k)$ always vanish. On this conjecture, there are many results for real abelian number fields by many authors. Recently Komatsu [5] constructed quaternion extensions k over the rational number field $\mathbf{Q}$ with $\lambda_p(k_\infty/k) = \mu_p(k_\infty/k) = 0$.

Let F be a group of order p^3 defined by $\langle a, b, c \mid a^p = b^p = c^p = 1, ba = abc, bc = cb, ca = ac\rangle$. Let $\mathbf{Q}_{(1)}$ be the first layer of the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}$. For any prime number q with $q \equiv 1 \pmod p$, there exists the unique subfield $k(q)$ of $\mathbf{Q}(\zeta_q)$ which is cyclic over $\mathbf{Q}$ of degree p, where ζ_q is a primitive q-th root of unity.

The main purpose of this paper is to prove the following theorems:

Theorem 1. *Let p be a fixed odd prime number. Let l be a prime number satisfying the following conditions. $l \equiv 1 \pmod{p^2}$ and p is not a p-th power residue modulo l. We put $K = \mathbf{Q}_{(1)} \cdot k(l)$. Then there exists a Galois extension $L/\mathbf{Q}$ satisfying the following conditions (1) and (2).*

(1) *The Galois group $\mathrm{Gal}(L/\mathbf{Q})$ is isomorphic to F and $K \subseteq L$.*
(2) *Any prime of L ramified in L/K is lying above p.*

Moreover, for any given odd prime number p there exist infinitely many prime numbers l as above.

Corollary 1. *The Iwasawa invariants $\lambda_p(L_\infty/L)$, $\mu_p(L_\infty/L)$ and $\nu_p(L_\infty/L)$ vanish for the above p-extension L.*

We shall prove that Corollary 1 follows indeed from Theorem 1.

By Iwasawa [4], the class number of K is not divisible by p, and for the Galois extension L over $\mathbf{Q}$ satisfying the conditions (1) and (2) of Theorem 1, the class number of L is not divisible by p. Hence the Iwasawa λ-, μ- and ν-invariants of L vanish.

In the same way as in the proof of Theorem 1, we can costruct the non-abelian p-extensions over some imaginary quadratic fields satisfying Leopoldt's conjecture on the non-vanishing p-adic regulator (cf. [1], [2], [6], [8]).

Theorem 2. *Let k be an imaginary quadratic number field and h_k the class number of k. Let p be a prime number satisfying the one of the following conditions:*

(i) $p > 3$ *and* $p \nmid h_k$.
(ii) $p = 3$, $p \nmid h_k$ *and p is unramified in k.*

Let $k_{(1)}$(resp. $k_{(1)}^{an}$) be the first layer of the cyclotomic(resp. the anti-cyclotomic) $\mathbf{Z}_p$-extension of k. We put $K = k_{(1)} \cdot k_{(1)}^{an}$. Then there exists a Galois extension M/k satisfying $(*)$.

$$(*) \qquad \mathrm{Gal}(M/k) \simeq F \text{ and } K \subseteq M.$$

Any prime of M ramified in M/K is lying above p.

Corollary 2. *Leopoldt's conjecture for M and p is valid.*

2. Some lemmas for embedding problems. In this section, we quote some lemmas for embedding problems.

Let p be an odd prime number. Let k be a finite algebraic number field and $\mathfrak{G}$ its absolute Galois group. Let K/k be a finite Galois extension, and $(\varepsilon) : 1 \longrightarrow \mathbf{Z}/p\mathbf{Z} \longrightarrow E \xrightarrow{j} \mathrm{Gal}(K/k) \longrightarrow 1$ a cen-

1991 Mathematics Subject Classification. Primary 11R23, 11R27.

tral extension of finite groups. Then an embedding problem $(K/k, \varepsilon)$ is defined by the diagram

$$\begin{array}{ccccccccc} & & & & \mathfrak{G} & & \\ & & & & \downarrow \varphi & & \\ (\varepsilon): 1 \longrightarrow \mathbf{Z}/p\mathbf{Z} \longrightarrow E \xrightarrow{j} & & & & \mathrm{Gal}(K/k) & \longrightarrow 1 \end{array}$$

where φ is the canonical surjection. A solution of the embedding problem $(K/k, \varepsilon)$ is, by definition, a continuous homomorphism ψ of $\mathfrak{G}$ to E with $j \circ \psi = \varphi$. The Galois extension over k corresponding to the kernel of any solution is called a solution field. A solution ψ is called a proper solution if it is surjective.

For each prime $\mathfrak{q}$ of k, we denote by $k_{\mathfrak{q}}$ (resp. $K_{\mathfrak{Q}}$) the completion of k (resp. K) by $\mathfrak{q}$ (resp. prime $\mathfrak{Q}$ of K lying above $\mathfrak{q}$). Then the local problem $(K_{\mathfrak{Q}}/k_{\mathfrak{q}}, \varepsilon_{\mathfrak{q}})$ of $(K/k, \varepsilon)$ is defined by the diagram

$$\begin{array}{ccccccccc} & & & & \mathfrak{G}_{\mathfrak{q}} & & \\ & & & & \downarrow \varphi|_{\mathfrak{G}_{\mathfrak{q}}} & & \\ (\varepsilon_{\mathfrak{q}}): 1 \longrightarrow \mathbf{Z}/p\mathbf{Z} \longrightarrow E_{\mathfrak{q}} \xrightarrow{j|_{E_{\mathfrak{q}}}} & & & & \mathrm{Gal}(K_{\mathfrak{Q}}/k_{\mathfrak{q}}) & \longrightarrow 1 \end{array}$$

where $\mathrm{Gal}(K_{\mathfrak{Q}}/k_{\mathfrak{q}})$ is isomorphic to the decomposition group of $\mathfrak{Q}$ in K/k, $\mathfrak{G}_{\mathfrak{q}}$ is the absolute Galois group of $k_{\mathfrak{q}}$, and $E_{\mathfrak{q}}$ is the inverse image of $\mathrm{Gal}(K_{\mathfrak{Q}}/k_{\mathfrak{q}})$ by j.

In the same manner as the case of $(K/k, \varepsilon)$, solutions, solution fields etc. are defined for $(K_{\mathfrak{Q}}/k_{\mathfrak{q}}, \varepsilon_{\mathfrak{q}})$.

Lemma 1 (Neukirch [9])**.** *$(K/k, \varepsilon)$ has a solution if and only if $(K_{\mathfrak{Q}}/k_{\mathfrak{q}}, \varepsilon_{\mathfrak{q}})$ has a solution for any prime $\mathfrak{q}$ of k.*

Lemma 2 (Shafarevich [11])**.** *Let $k_{\mathfrak{p}}$ be a finite extension over $\mathbf{Q}_p$ with degree N. If $k_{\mathfrak{p}}$ does not contain a primitive p-th root of unity, the Galois group of the maximal p-extension over $k_{\mathfrak{p}}$ is a free pro-p-group, of rank $N + 1$.*

3. Proof of Theorem 1. Let F be a group of order p^3 defined by $\langle a, b, c \mid a^p = b^p = c^p = 1, ba = abc, bc = cb, ca = ac \rangle$. Let $(\varepsilon): 1 \longrightarrow \mathbf{Z}/p\mathbf{Z} \longrightarrow F \xrightarrow{j} \mathrm{Gal}(K/\mathbf{Q}) \longrightarrow 1$ be a non-split central extension. First, we see that the embedding problem $(K/\mathbf{Q}, \varepsilon)$ is solvable. By Lemma 1 we have only to consider the local problem $(K_{\mathfrak{q}}/\mathbf{Q}_q, \varepsilon_q)$ for any prime number q, where $\mathfrak{q}$ is a prime of k lying above q.

Let $\mathfrak{p}$ and $\mathfrak{l}$ be primes of K above p and l, respectively.

Since $F_p = j^{-1}(\mathrm{Gal}(K_{\mathfrak{p}}/\mathbf{Q}_p)) = F$ and since the Galois group of the maximal p-extension over $\mathbf{Q}_p$ is a free pro-p-group of rank 2by Lemma 2, the local problem $(K_{\mathfrak{p}}/\mathbf{Q}_p, \varepsilon_p)$ has a solution. Since (ε_p) is a non-split central extension, it is a proper solution. By local class field theory, $L(p)/K_{\mathfrak{p}}$ is a ramified extension, where $L(p)$ is a solution field of $(K_{\mathfrak{p}}/\mathbf{Q}_p, \varepsilon_p)$.

Since $F_l = j^{-1}(\mathrm{Gal}(K_{\mathfrak{l}}/\mathbf{Q}_l)) \simeq \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$, there exists a solution of the local problem $(K_{\mathfrak{l}}/\mathbf{Q}_l, \varepsilon_l)$.

It is clear that for any prime $\mathfrak{q}$ of K which is unramified in $K/\mathbf{Q}$, the local problem $(K_{\mathfrak{q}}/\mathbf{Q}_q, \varepsilon_q)$ has a solution, where $q = \mathfrak{q} \cap \mathbf{Q}$.

Thus there exists a proper solution of $(K/\mathbf{Q}, \varepsilon)$, since (ε) is a non-split central extension. Let L be a solution field of $(K/\mathbf{Q}, \varepsilon)$. Let $\mathfrak{L}$ be a prime of L lying above l. $\mathfrak{L}$ is unramified in L/K, because the ramification group of $\mathfrak{L}$ over $\mathbf{Q}$ is not isomorphic to $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$.

Assume that a prime $\mathfrak{Q} \nmid p$ of L is ramified in L/K. We put $q = \mathfrak{Q} \cap \mathbf{Q}$. Then q is a prime number. By local class field theory, $N(\mathfrak{Q}) = q^{p^s} \equiv 1 \pmod p$ for some integer s, where $N(\mathfrak{Q})$ is the absolute norm of $\mathfrak{Q}$. Hence $q \equiv 1 \pmod p$. Then there exists a cyclic subextension $k(q)/\mathbf{Q}$ of $\mathbf{Q}(\zeta_q)/\mathbf{Q}$ with $[k(q) : \mathbf{Q}] = p$. Let $\widetilde{\mathfrak{Q}}$ be a prime of $L \cdot k(q)$ above $\mathfrak{Q}$ and let L' be the inertia field of $\widetilde{\mathfrak{Q}}$ in $L \cdot k(q)/K$. Then we see that L' is neither K, L nor $L \cdot k(q)$ by considering the ramification group. Since $\mathrm{Gal}(L \cdot k(q)/K)$ is the center of $\mathrm{Gal}(L \cdot k(q)/\mathbf{Q})$, $L'/\mathbf{Q}$ is a Galois extension. Furthermore, $\mathrm{Gal}(L'/\mathbf{Q})$ is isomorphic to $\mathrm{Gal}(L/\mathbf{Q})$ and $L'/\mathbf{Q}$ gives a proper solution of $(K/\mathbf{Q}, \varepsilon)$. By the choice of L', any prime of L which is unramified in L/K is also unramified in L'/K, and a prime of L' above q is unramified in L'/K. By continuing this procedure, we can find a required extension over $\mathbf{Q}$.

We show now that for a fixed odd prime number p there exist infinitely many prime numbers l satisfying that $l \equiv 1 \pmod{p^2}$ and p is not a p-th power residue modulo l.

Let M and M' denote the cyclotomic fields $\mathbf{Q}(\zeta_p)$ and $\mathbf{Q}(\zeta_{p^2})$, respectively. Then M' and $M(\sqrt[p]{p})$ are independent cyclic extensions of degree p over M. We can choose a prime $\mathfrak{L}$ of M with absolute degree 1 such that $\mathfrak{L}$ is decomposed in M' and undecomposed in $M(\sqrt[p]{p})$. By Tchebotarev density theorem, there exist infinitely many such primes $\mathfrak{L}$. Let l be a prime number with $N(\mathfrak{L}) = l$. Then l satisfies the above conditions. □

4. Proof of Theorem 2 and Corollary 2.

Proof of Theorem 2. If $\mathfrak{q}$ is a prime of k with $N(\mathfrak{q}) \equiv 1 \pmod p$, there exists a cyclic extension over k of degree p which is unramified outside $\mathfrak{q}$ and in which $\mathfrak{q}$ is totally ramified. Hence, in the same way as in the proof of Theorem 1 there exists a number field satisfying $(*)$. □

Proof of Corollary 2. Put $B_{k,p} = \{\alpha \in k^\times \mid (\alpha) = \mathfrak{a}^p$ for some ideal of k, and $\alpha \in k_{\mathfrak{p}}^{\times p}$ for any prime $\mathfrak{p}$ of k lying above $p\}/k^{\times p}$. Then we have clearly $B_{k,p} = 0$ and Leopoldt's conjecture follows from the following lemma:

Lemma 3 (Miki [7])**.** *Let K be a finite algebraic number field and L/K a finite p-extension unramified outside p. If $B_{K,p} = 0$ and $\zeta_p \notin K_{\mathfrak{P}}$ for any prime $\mathfrak{P}|p$ of K, then Leopoldt's conjecture for L and p is valid.* □

References

[1] Ax, J.: On the units of an algebraic number field. Illinois J. Math., **9**, 584–589 (1965).

[2] Brumer, A.: On the units of algebraic number fields. Mathematika, **14**, 121–124 (1967).

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

[4] Iwasawa, K.: A note on class numbers of algebraic number fields. Abh. Math. Sem. Univ. Hamburg, **20**, 257–258 (1956).

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

[6] Leopoldt, H. W.: Zur Arithmetik in abelschen Zahlkörpern. J. Reine. Angew. Math., **209**, 54–71 (1962).

[7] Miki, H.: On the Leopoldt conjecture on the p-adic regulators. J. Number Theory, **26**, 117–128 (1987).

[8] Miyake, K.: On the units of an algebraic number field. J. Math. Soc. Japan, **34**, 515–525 (1982).

[9] Neukirch, J.: Über das Einbettungsproblem der algebraischen Zahlentheorie. Invent. Math., **21**, 59–116 (1973).

[10] Nomura, A.: On the class numbers of certain Hilbert class fields. Manuscripta Math., **79**, 379–390 (1993).

[11] Shafarevich, I. R.: On p-extensions. Mat. Sb. (N.S.), **20(62)**, 351–363 (1947); Amer. Math. Soc. Transl. Ser. 2, **4**, 59–72 (1956) (English transl.).