On the Vanishing of Iwasawa Invariants of Certain (p, p)-extensions of Q

By Gen YAMAMOTO

Department of Mathematics, School of Science and Engineering, Waseda University

(Communicated by Shokichi IYANAGA, M. J. A., March 12, 1997)

Abstract: Let p be any odd prime. We show that the Iwasawa λ_p and μ_p-invariants of certain (p, p)-extension fields K of $\boldsymbol{Q}$ vanish, and that there are infinitely many such K.

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

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

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

In [4], Greenberg conjectured that if k is a totally real, $\lambda_p(k) = \mu_p(k) = 0$. About the conjecture, there are many results for real quadratic fields by Fukuda, Ichimura, Komatsu, Ozaki, Sumida, Taya, etc.. For example, it is known that if $p = 3$ and $k = \boldsymbol{Q}(\sqrt{m})$, $1 < m < 10000$, then $\mu_3(k) = \lambda_3(k) = 0$ (cf. [5] and [8]). For p-extension fields of $\boldsymbol{Q}$, there are results by Greenberg ([4], V), Iwasawa ([6]), Fukuda, Komatsu, Ozaki, and Taya ([3]), etc. On the other hand, Ferrero and Washington have shown that $\mu_p(k) = 0$ for any abelian extension field k of $\boldsymbol{Q}$.

In this paper we shall show $\lambda_p(K) = \mu_p(K) = 0$ for some abelian extension number fields K of $\boldsymbol{Q}$ with $\mathrm{Gal}(K/\boldsymbol{Q}) \simeq (\boldsymbol{Z}/p\boldsymbol{Z})^2$, and the existence of infinitely many such K.

2. Theorem. Let p be a fixed odd prime. Let p_1 and p_2 be distinct primes with $p_1 \equiv p_2 \equiv 1 \pmod{p}$. Then there exists the unique subfield $k(p_i)$ of $\boldsymbol{Q}(\zeta_{p_i})$ which is cyclic over $\boldsymbol{Q}$ of degree p for $i = 1,2$, where ζ_{p_i} is a primitive p_i-th root of unity. We put $K = k(p_1)k(p_2)$. Let K_∞ be the cyclotomic $\boldsymbol{Z}_p$-extension of K and K_n the n-th layer and A_n the p-Sylow subgroup of the ideal class group of K_n. Our main purpose of this section is to prove the following theorem:

Theorem 1. *Let p, p_1, p_2 and K be as above. Assume that p is not a p-th power residue modulo p_1 and p_2 is not a p-th power residue modulo p_2 and $p_2 \not\equiv 1 \pmod{p^2}$. If one of the following conditions* (i)-(iii) *is satisfied, then $\lambda_p(K) = \mu_p(K) = 0$.*

(i) *p is a p-th power residue modulo p_2.*

(ii) *p_2 is a p-th power residue modulo p_1.*

(iii) $p_1 \equiv 1 \pmod{p^2}$.

Let $\boldsymbol{Q}_1$ be the first layer of the cyclotomic $\boldsymbol{Z}_p$-extension of $\boldsymbol{Q}$. For the field $K_1 = K\boldsymbol{Q}_1$, it is easy to see that $K_1/\boldsymbol{Q}$ is Galois and unramified outside p, p_1 and p_2 and $\mathrm{Gal}(K_1/\boldsymbol{Q}) \simeq (\boldsymbol{Z}/p\boldsymbol{Z})^3$. Let G_p, $G_{p_i} (i = 1,2)$ be the decomposition groups for p, p_i in $\mathrm{Gal}(K_1/\boldsymbol{Q})$ and let D_p, D_{p_i} be the fixed field of G_p, G_{p_i}, respectively.

For the field K_1, we have the following result which we shall use as a lemma (The author wishes to thank Dr. Manabu Ozaki for drawing his attention to the result).

Lemma 2 ([1] (G. Cornell and M. Rosen)). *Following statements* (a) *and* (b) *are equivalent*:

(a) *The class number of K_1 is not divisible by p.*

(b) $[D_p : \boldsymbol{Q}] = [D_{P_1} : \boldsymbol{Q}] = [D_{p_2} : \boldsymbol{Q}] = p$ *and* $D_p D_{p_1} D_{p_2} = K_1$.

On the other hand , we have also the following result.

Lemma 3 ([2] (T. Fukuda)). *Let k_∞/k be a $\boldsymbol{Z}_p$-extention. Let $e \geq 0$ be an integer such that in k_∞/k_e all ramified primes are totally ramified. If $\#A_n = \#A_{n+1}$ for some $n \geq e$, then $\mu_p(k_\infty/k) = \lambda_p(k_\infty/k) = 0$.*

Proof of Theorem 1. First we note that A_0 is trivial because p_1 is not a p-th power residue modulo p_2. We check $[D_p : \boldsymbol{Q}] = [D_{p_1} : \boldsymbol{Q}] = [D_{p_2} : \boldsymbol{Q}] = p$. Since $\mathrm{Gal}(K_1/\boldsymbol{Q}) \simeq (\boldsymbol{Z}/p\boldsymbol{Z})^3$ and $p, p_i (i = 1,2)$ have ramification indices p, it is sufficient for this purpose to show that there exists a subfield of $K_1 (\neq \boldsymbol{Q})$ in which p or p_1 or p_2 remains prime. But from our assumptions for p, p_i, it follows easily that p is inert in $k(p_1)$, p_1 is inert in $k(p_2)$, and p_2 is inert in $\boldsymbol{Q}_1$.

We note that $D_p \subset k(p_1)k(p_2) = K$, $D_{p_1} \subset k(p_2)\boldsymbol{Q}_1$, and $D_{p_2} \subset k(p_1)\boldsymbol{Q}_1$. Next, we consider the composite field $D_p D_{p_1} D_{p_2}$ in each of the cases (i)-(iii).

(i) Since $D_p = k(p_2)$ by (i), and $D_{p_1} \neq k(p_2)$, it follows that $D_p D_{p_1} = k(p_2)\boldsymbol{Q}_1$. Also since $D_{p_2} \subset k(p_1)\boldsymbol{Q}_1$ and $D_{p_2} \neq \boldsymbol{Q}_1$, $D_{p_2} \not\subset k(p_2)\boldsymbol{Q}_1 = D_p D_{p_1}$. Hence we have $D_p D_{p_1} D_{p_2} = K_1$.

(ii) Since $D_{p_2} = k(p_1)$ by (ii), and $D_p \neq k(p_1)$, it follows that $D_p D_{p_2} = k(p_1)k(p_2)$. Also since $D_{p_1} \subset k(p_2)\boldsymbol{Q}_1$ and $D_{p_1} \neq k(p_2)$, $D_{p_1} \not\subset k(p_1)k(p_2) = D_p D_{p_2}$. Hence we have $D_p D_{p_1} D_{p_2} = K_1$.

(iii) Since $D_{p1} = \boldsymbol{Q}_1$ by (iii), and $D_{p_2} \neq \boldsymbol{Q}_1$, it follows that $D_{p_1} D_{p_2} = k(p_1)\boldsymbol{Q}_1$. Also since $D_p \subset k(p_1)k(p_2)$ and $D_p \neq k(p_1)$, $D_p \not\subset k(p_1)\boldsymbol{Q}_1 = D_{p_1} D_{p_2}$. Hence we have $D_p D_{p_1} D_{p_2} = K_1$.

Hence if one of conditions (i)-(iii) is satisfied, then the class number of K_1 is not divisible by p by Lemma 2. This means that A_1 is trivial. Since p does not ramify in $K/\boldsymbol{Q}$ and $\boldsymbol{Z}_p$-extensions are unramified outside p (cf. [9, p. 264]), all ramified primes in K_∞/K are totally ramified. Hence we can apply Lemma 3 and conclude that $\lambda_p(K) = \mu_p(K) = 0$. □

3. Remarks. We note that our theorem 1 (ii) has the following relations with the known result. In [4], Greenberg proved $\lambda_p(k) = \mu_p(k) = 0$ for the fields $k \subseteq K$, where K satisfies the conditions of our theorem 1 (ii) and $k/\boldsymbol{Q}$ is cyclic and p remains prime in k. This follows from our theorem because if $k \subseteq K$ then $\lambda_p(k) \leq \lambda_p(K)$ and $\mu_p(k) \leq \mu_p(K)$.

In [6], Iwasawa proved that if K satisfies the conditions of Theorem 1 (ii) and $p_1 \not\equiv 1 \pmod{p^2}$, then $\lambda_p(K) = \mu_p(K) = 0$, which is contained in our theorem. Iwasawa proved also that there exist infinitely many pairs of primes (p_1, p_2) satisfying these conditions. We shall show that we can prove by the method as in [6], the existence of infinitely many pairs of primes (p_1, p_2) satisfying the conditions of our theorem 1 (i), (ii). We have namely,

Theorem 4. *For any given odd prime p, there exist infinitely many pairs of prime numbers (p_1, p_2) which satisfy the conditions of* Theoerem 1 (i), (ii), *and* (iii), *respectively.*

Proof. Since the case (ii) is proved in [6], we prove (i) and (iii). Let P and P' denote the cyclotomic fields $\boldsymbol{Q}(\zeta_p)$ and $\boldsymbol{Q}(\zeta_{p^2})$, respectively. Then P' and $P(\sqrt[p]{p})$ are independent cyclic extensions of degree p over P.

(i) We can choose a prime ideal $\mathfrak{p}_1$ of P with absolute degree 1 such that $\mathfrak{p}_1$ is undecomposed in $P(\sqrt[p]{p})$. By Tchebotarev density theorem, there exist infinitely many such prime ideals $\mathfrak{p}_1$. Let $p_1 = N_{P/\boldsymbol{Q}}(\mathfrak{p}_1)$, where $N_{P/\boldsymbol{Q}}$ is the norm map from P to $\boldsymbol{Q}$. Then $p_1 \equiv 1 \pmod{p}$ and, by Kummer theory, p is not a p-th power residue modulo p_1. Now P', $P(\sqrt[p]{p})$ and $P(\sqrt[p]{p_1})$ are independent cyclic extensions of degree p over P. Hence there is a prime ideal $\mathfrak{p}_2$ of P with absolute degree 1 such that $\mathfrak{p}_2$ is undecomposed in both P' and $P(\sqrt[p]{p_1})$, but is decomposed in $P(\sqrt[p]{p})$. By Tchebotarev density theorem, there exist infinitely many such prime ideals $\mathfrak{p}_2$. Let $p_2 = N_{P/\boldsymbol{Q}}(\mathfrak{p}_2)$. Then $p_2 \equiv 1 \pmod{p}$, $p_2 \not\equiv 1 \pmod{p^2}$, p_1 is not a p-th power residue modulo p_2 and p is a p-th power residue modulo p_2. Hence p_1 and p_2 satisfy the conditions of Theorem 1 (i) and there exist infinitely many pairs (p_1, p_2).

(iii) We can choose a prime ideal $\mathfrak{p}_1$ of P with absolute degree 1 such that $\mathfrak{p}_1$ is undecomposed in $P(\sqrt[p]{p})$, but is decomposed in P'. Let $p_1 = N_{P/\boldsymbol{Q}}(\mathfrak{p}_1)$. Then $p_1 \equiv 1 \pmod{p^2}$ and p is not a p-th power residue modulo p_1. Now P' and $P(\sqrt[p]{p_1})$ are independent cyclic extensions of degree p over P. Hence there is a prime ideal $\mathfrak{p}_2$ of P with absolute degree 1 such that $\mathfrak{p}_2$ is undecomposed in both P' and $P(\sqrt[p]{p_1})$. Then $p_2 \equiv 1 \pmod{p}$, $p_2 \not\equiv 1 \pmod{p^2}$ and p_1 is not a p-th power residue modulo p_2. Hence p_1 and p_2 satisfy the conditions of Theorem 1 (iii) and there exist infinitely many pairs (p_1, p_2) by Tchebotarev density theorem. □

References

[1] G. Cornell and M. Rosen: The class group of an absolutely abelian l-extension. Illinois J. Math., **32**, 453–461 (1988).

[2] T. Fukuda: Remarks on $\boldsymbol{Z}_p$-extensions of Number

fields. Proc. Japan Acad., **70A**, 264–266 (1994).

[3] T. Fukuda, K. Komatsu, M. Ozaki, and H. Taya: On Iwasawa λ_p-invariants of real cyclic extension of degree p. Tokyo J. Math. (to appear).

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

[5] H. Ichimura and H. Sumida: On the Iwasawa λ-invariants of certain real abelian fields. (preprint).

[6] K. Iwasawa: A note on capitulation problem for number fields. II. Proc. Japan Acad., **65A**, 183–186 (1989).

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

[8] J. Kraft and R. Schoof: Computing Iwasawa modules of real quadratic number fields. Compositio Math., **97**, 135–155 (1995).

[9] L. C. Washington: Introduction to Cyclotomic Fields. Springer-Verlag, New York-Heidelberg-Berlin (1982).