TOKYO J. MATH.
VOL. 20, NO. 2, 1997

On Iwasawa λ_p-Invariants of Relative Real Cyclic Extensions of Degree p

Takashi FUKUDA, Keiichi KOMATSU, Manabu OZAKI and Hisao TAYA*

Nihon University, Waseda University and Tohoku University

Dedicated to Professor Fumiyuki Terada on his 70th birthday

Abstract. We give a criterion of the vanishing of λ_p-invariants for relative cyclic extensions of totally real number fields with degree p using Iwasawa's result of Riemann-Hurwitz type which is an analogue to Kida's formula.

1. Introduction.

Let p be a prime number and $\mathbf{Z}_p$ the ring of p-adic integers. Let k be an algebraic number field of finite degree and K a Galois extension of degree p over k. It is considered that properties of the cyclotomic $\mathbf{Z}_p$-extension of k are well reflected on those of K. For example, Iwasawa proved in [4] that if p is odd, then $\mu_p(k)=0$ implies $\mu_p(K)=0$. Here, and in what follows, for a finite algebraic extension k of $\mathbf{Q}$, we denote by k_∞ the cyclotomic $\mathbf{Z}_p$-extension of k, and by $\lambda_p(k)$ and $\mu_p(k)$ the Iwasawa invariants of k_∞/k. In this context, we study a relation between $\lambda_p(K)$ and $\lambda_p(k)$ using the result of Iwasawa which is an analogue to Kida's formula (cf. [5], [7]). Our purpose in this paper is to prove Theorem 3.5 which is a criterion of the vanishing of λ_p-invariants for relative cyclic extensions of totally real number fields with degree p, and apply it for some real cubic fields.

2. Preliminaries.

Throughout the following, let $\mathbf{Z}$ and $\mathbf{Q}$ denote the ring of rational integers and the field of rational numbers, respectively. For an algebraic extension F of $\mathbf{Q}$, let E_F be the unit group of F, I_F the group of ideals of F and P_F the group of principal ideals of F. Let K be a Galois extension of F with Galois group $G(K/F)$. For a finite prime v of F and an extension w of v on K, we denote by $e(w/v)$ the order of the inertia group

Received April 4, 1996
* This research was supported in part by Waseda University Grant for Special Research Projects 95A-286.

$T(w/v)$ in $G(K/F)$. We also denote by $H^n(G(K/F), M)$ the n-th cohomology group for a $G(K/F)$-module M.

In [5], Iwasawa proved the following striking result, which is considered as a "plus-version" analogue to Kida's formula describing a relation between λ_p^--invariants for relative p-extensions of CM-fields.

THEOREM 2.1. *Let p be a prime number, k a totally real number field of finite degree and K a cyclic extension of degree p over k, unramified at every infinite prime of k and not contained in k_∞. Let h_n be the dimension of $H^n(G(K_\infty/k_\infty), E_{K_\infty})$ over the finite field $\mathbf{F}_p=\mathbf{Z}/p\mathbf{Z}$. We assume that $\mu_p(k)=0$. Then we have the following formula for $\lambda_p(K)$ and $\lambda_p(k)$:*

$$\lambda_p(K)=p\lambda_p(k)+\sum_w (e(w/v)-1)+(p-1)(h_2-h_1)\,,$$

where w ranges over all finite primes of K_∞ which are prime to p.

As a straightforward application of this theorem, we see that $\lambda_p(K)\equiv 0 \pmod{p-1}$ for a real cyclic extension K of degree p over a totally real number field k if $\lambda_p(k)=\mu_p(k)=0$. Here we make a remark about $\lambda_p(k)$ and $\mu_p(k)$. It is conjectured that if k is a totally real number field, then $\lambda_p(k)=\mu_p(k)=0$, which is often called Greenberg's conjecture (cf. [2]). In the following, using this theorem, we study cyclotomic $\mathbf{Z}_p$-extensions of relative cyclic extensions of totally real number fields with degree p in connection with Greenberg's conjecture.

3. Cohomological properties of $\mathbf{Z}_p$-extensions.

Let p be a prime number. From now on, let k be a totally real number field of finite degree and K a real cyclic extension of degree p over k, which satisfies $K\cap k_\infty=k$. Then the degree $[K_\infty : k_\infty]$ is equal to p. Let

$$S_{K_\infty/k_\infty}=\{w : \text{prime ideal of } K_\infty \mid w \text{ is prime to } p \text{ and ramified in } K_\infty/k_\infty\}\,,$$

$$T_{K_\infty/k_\infty}=\{w\in S_{K_\infty/k_\infty} \mid \text{the order of the ideal class of } w \text{ is prime to } p\}$$

and s_∞ (resp. t_∞) be the cardinality of S_{K_∞/k_∞} (resp. T_{K_∞/k_∞}). We note that s_∞ and t_∞ are finite because any prime of K is finitely decomposed in K_∞. Moreover, as mentioned in §2, we let

$$h_i=\dim_{\mathbf{F}_p} H^i(G(K_\infty/k_\infty), E_{K_\infty})$$

for $i=1, 2$.

We first consider h_1. Put $G=G(K_\infty/k_\infty)$ and

$$P_{K_\infty}^G=\{(\alpha)\in P_{K_\infty} \mid (\alpha^\sigma)=(\alpha) \text{ for all } \sigma\in G\}\,.$$

Then the exact sequence

$$1 \to E_{K_\infty} \to K_\infty^\times \to P_{K_\infty} \to 1$$

induces the following exact sequence:

$$1 \to E_{k_\infty} \to k_\infty^\times \to P_{K_\infty}^G \to H^1(G, E_{K_\infty}) \to H^1(G, K_\infty^\times) \to \cdots .$$

Since $H^1(G, K_\infty^\times)=1$, we have $H^1(G, E_{K_\infty}) \simeq P_{K_\infty}^G/P_{k_\infty}$.

Assume that $\lambda_p(k)=\mu_p(k)=0$, namely, the p-primary part of $I_{k_\infty}/P_{k_\infty}$ is trivial. Then $(I_{k_\infty} \cap P_{K_\infty})/P_{k_\infty}=1$ because it is a subgroup of the p-primary part of $I_{k_\infty}/P_{k_\infty}$. Hence

$$H^1(G, E_{K_\infty}) \simeq P_{K_\infty}^G/(I_{k_\infty} \cap P_{K_\infty}) .$$

Let us put

$$I_{K_\infty}^G=\{w \in I_{K_\infty} \mid w^\sigma=w \text{ for all } \sigma \in G\} .$$

Note that $P_{K_\infty}^G=I_{K_\infty}^G \cap P_{K_\infty}$ and $I_{K_\infty}^G=I_{k_\infty}\langle S_{K_\infty/k_\infty}\rangle$ (cf. §1 in [5]). Since

$$1 \to P_{K_\infty}^G/(I_{k_\infty} \cap P_{K_\infty}) \to I_{K_\infty}^G/I_{k_\infty} \to I_{K_\infty}^G/P_{K_\infty}^G I_{k_\infty} \to 1$$

is exact, it follows that

$$h_1+\dim_{\mathbf{F}_p}(I_{K_\infty}^G/P_{K_\infty}^G I_{k_\infty})=\dim_{\mathbf{F}_p}(I_{K_\infty}^G/I_{k_\infty})=s_\infty .$$

In particular, we see that $h_1 \le s_\infty$.

Hence Theorem 2.1 immediately implies the following proposition:

PROPOSITION 3.1. *Assume that* $\lambda_p(k)=\mu_p(k)=0$. *Then* $\lambda_p(K)=0$ *if and only if the following two conditions are satisfied*:

(1) $H^1(G(K_\infty/k_\infty), E_{K_\infty}) \simeq (\mathbf{Z}/p\mathbf{Z})^{\oplus s_\infty}$.

(2) $H^2(G(K_\infty/k_\infty), E_{K_\infty})=1$.

Moreover, since $P_{K_\infty}^G I_{k_\infty}=I_{K_\infty}^G \cap I_{k_\infty}P_{K_\infty}$, we have

$$I_{K_\infty}^G/P_{K_\infty}^G I_{k_\infty} \simeq I_{K_\infty}^G P_{K_\infty}/I_{k_\infty}P_{K_\infty} .$$

This is a p-primary abelian group. Hence, it is seen that $S_{K_\infty/k_\infty}=T_{K_\infty/k_\infty}$ if and only if $I_{K_\infty}^G/P_{K_\infty}^G I_{k_\infty}=1$, so $s_\infty=t_\infty$ if and only if $h_1=s_\infty$.

Now, the following lemma concerning the first cohomology group is an immediate consequence of this argument.

LEMMA 3.2. *Assume that* $\lambda_p(k)=\mu_p(k)=0$. *Then the following two conditions are equivalent*:

(1) $S_{K_\infty/k_\infty}=T_{K_\infty/k_\infty}$.

(2) $H^1(G(K_\infty/k_\infty), E_{K_\infty}) \simeq (\mathbf{Z}/p\mathbf{Z})^{\oplus s_\infty}$.

In the proof of Lemma 3 in [6], Iwasawa noticed the following important property of the second cohomology group. As he, however, omitted the proof, we give it for convenience of readers.

LEMMA 3.3. *Assume that k_∞ has only one prime ideal lying over p and that the class number of k is not divisible by p. Then $H^2(G(K_\infty/k_\infty), E_{K_\infty})=1$.*

PROOF. Note that K_∞/k_∞ is an extension of degree p. Let $G=G(K_\infty/k_\infty)$. Let K_n and k_n be the n-th layer of K_∞/K and k_∞/k, respectively. It follows from the assumption on k_∞/k that the class number of k_n is not divisible by p (cf. [3]). Since k is totally real, from the genus theory for k_n/k_m, we have $N_{k_n/k_m}(E_{k_n})=E_{k_m}$ for $n\geq m$, where N_{k_n/k_m} is the norm mapping of k_n over k_m. This implies the surjective homomorphism

$$(1) \qquad N_{k_n/k_m}\ :\ E_{k_n}/N_{K_n/k_n}(E_{K_n}) \to E_{k_m}/N_{K_m/k_m}(E_{K_m})\ .$$

Also, the genus theory for K_n/k_n shows that the order of $E_{k_n}/N_{K_n/k_n}(E_{K_n})$ is not more than p^{s_∞}. Hence the homomorphism (1) becomes an isomorphism for sufficiently large integers $n\geq m$. For such a sufficiently large m, let n be an integer with $n>m+s_\infty$ and u an element of E_{k_m}. Since the order of $E_{k_n}/N_{K_n/k_n}(E_{K_n})$ is not more than p^{s_∞}, we have $N_{k_n/k_m}(u)=u^{p^{n-m}}\in N_{K_m/k_m}(E_{K_m})$. This shows that a canonical mapping

$$E_{k_m}/N_{K_m/k_m}(E_{K_m}) \to E_{k_n}/N_{K_n/k_n}(E_{K_n})$$

is trivial for sufficiently large integers $n\geq m$. Hence,

$$H^2(G, E_{K_\infty})=\varinjlim H^2(G, E_{K_n})\simeq \varinjlim E_{k_n}/N_{K_n/k_n}(E_{K_n})=1\ .$$

This completes the proof. □

We obtain the next corollary by letting $k=\mathbf{Q}$.

COROLLARY 3.4. *Let K be a real cyclic extension of degree p over $\mathbf{Q}$. Then we have $H^2(G(K_\infty/\mathbf{Q}_\infty), E_{K_\infty})=1$.*

Combining Proposition 3.1 with Lemmas 3.2 and 3.3, we obtain the following theorem.

THEOREM 3.5. *Let p be a prime number, k a totally real number field of finite degree and K a real cyclic extension of degree p over k. Assume that k_∞ has only one prime ideal lying over p and that the class number of k is not divisible by p. Then, the following are equivalent*:

(1) $\lambda_p(K)=0$.

(2) *For any prime ideal w of K_∞ which is prime to p and ramified in K_∞/k_∞, the order of the ideal class of w is prime to p.*

Further, we obtain the next corollary by letting $k=\mathbf{Q}$.

COROLLARY 3.6. *Let K be a real cyclic extension of degree p over $\mathbf{Q}$. Then the following are equivalent*:

(1) $\lambda_p(K)=0$.

(2) *For any prime ideal w of K_∞ which is prime to p and ramified in $K_\infty/\mathbf{Q}_\infty$, the*

order of the ideal class of w is prime to p.

4. Examples in the case $p=3$.

Let K be a cyclic cubic extension of $\mathbf{Q}$. We treat the case that the conductor f of K is a prime number not divisible by 3. Then f is congruent to 1 modulo 3 and such a K is uniquely determined by its conductor (cf. Theorem 6.4.6 of [1]). It follows from genus theory that the class number of such a K is not divisible by 3. If 3 does not decomposed in K, then we conclude that $\lambda_3(K)=0$ by Iwasawa's theorem (cf. [3]). So we consider the case that 3 splits in K. Now, if 9 does not divide $f-1$, then the unique prime ideal of K ramified in $K/\mathbf{Q}$ remains prime in K_∞/K, and hence $s_\infty=t_\infty=1$ because the class number of K is not divisible by 3. Therefore, in such a case, $\lambda_3(K)=0$ from Corollary 3.6. Finally we shall apply Corollary 3.6 for some non-trivial cases.

EXAMPLE 4.1. Let K be the cyclic cubic field with conductor 523. Since $523\equiv 1 \pmod 9$ and $523\not\equiv 1 \pmod{27}$, the prime ideal of K lying over 523 splits into $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ in the initial layer K_1 of the cyclotomic $\mathbf{Z}_3$-extension K_∞ and each $\mathfrak{p}_i$ remains prime in K_∞/K_1. Therefore $S_{K_\infty/\mathbf{Q}_\infty}=\{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3\}$. We calculated $E_{\mathbf{Q}_1}$ and E_{K_1} by a computer and verified that $N_{K_1/\mathbf{Q}_1}(E_{K_1})=E_{\mathbf{Q}_1}^3$. From this and genus theory for $K_1/\mathbf{Q}_1$, it follows that each $\mathfrak{p}_i$ is actually principal in K_1. Hence we have $s_\infty=t_\infty=3$. Therefore it follows from Corollary 3.6 that $\lambda_3(K)=0$. The same argument can be applied to the cyclic cubic field of conductor 1531, 4951, 5059, 5851, 6067, 8461 and 9109.

EXAMPLE 4.2. Let K be the cyclic cubic field with conductor $f=73$, 307, 577, 613 or 1009. As in the above example, we see that $S_{K_\infty/\mathbf{Q}_\infty}=\{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3\}$, where $\mathfrak{p}_i$ is a prime ideal of K_1 lying over f. We verified that $(E_{\mathbf{Q}_1}: N_{K_1/\mathbf{Q}_1}(E_{K_1}))=3$ for each case. From this, we see that at least one of ideal classes of $\mathfrak{p}_i$ has order 3 in the ideal class group of K_1. We do not know the values of t_∞ and $\lambda_3(K)$ for these K's.

EXAMPLE 4.3. Let K be the cyclic cubic field with conductor 991, 1117, 1549, 2251 or 2341. Then $S_{K_\infty/\mathbf{Q}_\infty}=\{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3\}$ as in the above example. In each case, we see that $N_{K_1/\mathbf{Q}_1}(E_{K_1})=E_{\mathbf{Q}_1}$ and that every ideal class of $\mathfrak{p}_i$ has order 3 in the ideal class group of K_1. We do not know the values of t_∞ and $\lambda_3(K)$ for these K's.

References

[1] H. COHEN, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Math. **138** (1993), Springer-Verlag.

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

[3] K. IWASAWA, A note on class numbers of algebraic number fields, Abh. Math. Sem. Hamburg **20** (1955), 257–258.

[4] K. IWASAWA, On the μ-invariants of $\mathbf{Z}_l$-extensions, *Number Theory, Algebraic Geometry and Commutative Algebra, in honor of Y. Akizuki*, Kinokuniya (1973), 1–11.

[5] K. Iwasawa, Riemann-Hurwitz formula and p-adic Galois representation for number fields, Tôhoku Math. J. **33** (1981), 263–288.
[6] K. Iwasawa, A note on capitulation problem for number fields II, Proc. Japan Acad. **65** (1989), 183–186.
[7] Y. Kida, l-extensions of CM-fields and cyclotomic invariants, J. Number Theory **12** (1980), 519–528.

Present Addresses:
Takashi Fukuda
Department of Mathematics, College of Industrial Technology, Nihon University,
Shin-ei, Narashino, Chiba, 275 Japan.
e-mail: fukuda@math.cit.nihon-u.ac.jp

Keiichi Komatsu
Department of Information and Computer Sciences, School of Science and Engineering,
Waseda University,
Okubo, Shinjuku-ku, Tokyo, 169–50 Japan.

Manabu Ozaki
Department of Information and Computer Sciences, School of Science and Engineering,
Waseda University,
Okubo, Shinjuku-ku, Tokyo, 169–50, Japan.
e-mail: ozkm@cfi.waseda.ac.jp

Hisao Taya
Graduate School of Information Sciences, Tohoku University,
Katahira, Aoba-ku, Sendai, 980–77, Japan.
e-mail: taya@math.is.tohoku.ac.jp